Περιεχόμενα

1 Βασικές έννοιες **7**

1.1 Σύνολα . . . 7
1.1.1 Σχέσεις συνόλων . . . 7
1.1.2 Πράξεις συνόλων . . . 7
1.1.3 Δυναμοσύνολο . . . 9
1.1.4 Καρτεσιανό γινόμενο . . . 10
1.1.5 Διαμερίσεις . . . 10
1.2 Σχέσεις . . . 11
1.2.1 Ισοδυναμία . . . 12
1.2.2 Διάταξη . . . 13
1.2.3 Πράξεις σχέσεων . . . 14
1.3 Απεικονίσεις . . . 15
1.3.1 Αμφιμονοσήμαντες απεικονίσεις . . . 16
1.3.2 Γραφική παράσταση . . . 17
1.3.3 Σύνθεση απεικονίσεων . . . 17
1.3.4 Αντίστροφη απεικόνιση . . . 18
1.3.5 Εικόνες συνόλων . . . 19
1.4 Ισοδύναμα σύνολα . . . 19
1.4.1 Ιδιότητες πεπερασμένων συνόλων . . . 20
1.4.2 Βασικά αριθμήσιμα σύνολα . . . 21
1.4.3 Βασικά υπεραριθμήσιμα σύνολα . . . 22
1.5 Λυμένες ασκήσεις . . . 23
1.6 Ασκήσεις προς επίλυση . . . 43
1.7 Παράρτημα: Αναπαράσταση συνόλων στον υπολογιστή . . . 49
1.7.1 Η κλάση bitset της *C++* . . . 50
1.8 Παράρτημα: Το παράδοξο του Russell . . . 54

2 Βασικές αρχές **55**

2.1 Μαθηματική επαγωγή . . . 55
2.1.1 Γεωμετρικά προβλήματα απαρίθμησης . . . 72
2.1.2 Ασκήσεις προς επίλυση . . . 75
2.1.3 Παράρτημα: Αναδρομικοί (επαγωγικοί) ορισμοί στο $\mathbb{N}$ . . . 82
2.1.4 Παράρτημα: Επαγωγή και ορθότητα προγραμμάτων . . . 84
2.2 Αρχή εγκλεισμού-αποκλεισμού . . . 86
2.2.1 Έλεγχος συνέπειας δεδομένων και εκτίμηση φραγμάτων . . . 97
2.2.2 Ασκήσεις προς επίλυση . . . 99
2.2.3 Παράρτημα: Απαρίθμηση απεικονίσεων επί . . . 103
2.3 Αρχή του περιστερεώνα . . . 104

2.3.1 Ασκήσεις προς επίλυση . . . 117
2.4 Αρχή της διαγωνιοποίησης . . . 121
2.4.1 Ασκήσεις προς επίλυση . . . 122
2.5 Παράρτημα: Αρχή της αρτιότητας . . . 123
2.5.1 Ασκήσεις προς επίλυση . . . 126

3 Διατάξεις, Συνδυασμοί 127
3.1 Πολλαπλασιαστική αρχή ή κανόνας γινομένου . . . 127
3.2 Διατάξεις . . . 127
3.3 Συνδυασμοί . . . 131
3.4 Συνδυαστικά μοντέλα και συνδυαστικές αποδείξεις . . . 140
3.4.1 Το συνδυαστικό μοντέλο των επιτροπών . . . 141
3.4.2 Το συνδυαστικό μοντέλο των λέξεων . . . 143
3.5 Λυμένες ασκήσεις . . . 146
3.6 Ασκήσεις προς επίλυση . . . 164
3.7 Παράρτημα: Οικογένειες Sperner . . . 172

4 Διαφορές, παραγοντικά πολυώνυμα, διώνυμο του Νεύτωνα 175
4.1 Διαφορές . . . 175
4.2 Παραγοντικά πολυώνυμα . . . 177
4.3 Ο τύπος του Gregory . . . 180
4.4 Ο τύπος του Vandermonde . . . 182
4.5 Ο τύπος του διωνύμου του Νεύτωνα . . . 182
4.6 Λυμένες ασκήσεις . . . 188
4.7 Ασκήσεις προς επίλυση . . . 197

5 Στοιχεία θεωρίας αριθμών 201
5.1 Διαιρετότητα . . . 201
5.1.1 Ο αλγόριθμος της διαίρεσης . . . 201
5.1.2 Μέγιστος κοινός διαιρέτης . . . 204
5.1.3 Λυμένες ασκήσεις . . . 205
5.1.4 Ασκήσεις προς επίλυση . . . 208
5.1.5 Ο αλγόριθμος του Ευκλείδη . . . 208
5.1.6 Ο επεκτεταμένος αλγόριθμος του Ευκλείδη . . . 212
5.1.7 Λυμένες ασκήσεις . . . 214
5.1.8 Ασκήσεις προς επίλυση . . . 215
5.1.9 Γραμμικές διοφαντικές εξισώσεις . . . 215
5.1.10 Λυμένες ασκήσεις . . . 221
5.1.11 Ασκήσεις προς επίλυση . . . 223
5.1.12 Ελάχιστο κοινό πολλαπλάσιο . . . 224
5.1.13 Πρώτοι αριθμοί . . . 226
5.1.14 Ασκήσεις προς επίλυση . . . 229
5.1.15 Παράρτημα: Πόσους διαιρέτες έχει ένας αριθμός; . . . 230
5.1.16 Παράρτημα: Πως ελέγχουμε αν ένας αριθμός είναι πρώτος; . . . 232
5.1.17 Παράρτημα: Πως βρίσκουμε τους πρώτους αριθμούς; . . . 234
5.1.18 Παράρτημα: Πόσοι είναι οι πρώτοι αριθμοί μέχρι το n; . . . 236
5.2 Ισοτιμίες . . . 240
5.2.1 Η συνάρτηση ϕ του Euler . . . 248

5.2.2 Θεώρημα Euler-Fermat . . . 250
5.2.3 Ασκήσεις προς επίλυση . . . 253
5.2.4 Παράρτημα: Κριτήρια διαιρετότητας . . . 255
5.2.5 Αντιστροφή modulo n . . . 258
5.2.6 Παράρτημα: Το σύστημα κρυπτογράφησης RSA . . . 262
5.2.7 Το κινέζικο θεώρημα υπολοίπων . . . 264
5.2.8 Παράρτημα: Αναπαράσταση αριθμών modulo $n_1, n_2, \ldots, n_k$ . . . 267
5.2.9 Παράρτημα: RSA και κινέζικο θεώρημα υπολοίπων . . . 269
5.2.10 Παράρτημα: Ψηφιακό κορώνα ή γράμματα . . . 270
5.2.11 Παράρτημα: Το τεστ του Fermat . . . 272
5.2.12 Παράρτημα: Το πρόβλημα του κύκλου του Gauss . . . 274

6 Στοιχεία μαθηματικής λογικής 279
6.1 Εισαγωγή . . . 279
6.2 Γλώσσα του προτασιακού λογισμού . . . 281
6.2.1 Λυμένες ασκήσεις . . . 289
6.2.2 Ασκήσεις προς επίλυση . . . 290
6.3 Τιμές αληθείας, εκτίμηση, λογικό συμπέρασμα . . . 291
6.3.1 Λυμένες ασκήσεις . . . 296
6.3.2 Ασκήσεις προς επίλυση . . . 304
6.4 Προβλήματα ικανοποιησιμότητας . . . 307
6.4.1 Ασκήσεις προς επίλυση . . . 313
6.4.2 Κανονικές μορφές - Επάρκεια συνδέσμων . . . 315
6.4.3 Λυμένες ασκήσεις . . . 320
6.4.4 Ασκήσεις προς επίλυση . . . 322
6.4.5 Το πρόβλημα CNF-SAT . . . 324
6.4.6 Λυμένες ασκήσεις . . . 326
6.4.7 Ικανοποιησιμότητα τύπων Horn . . . 327
6.4.8 Ασκήσεις προς επίλυση . . . 328
6.5 Αξιωματικοποίηση του προτασιακού λογισμού - Πληρότητα . . . 329
6.5.1 Ανεξαρτησία των αξιωμάτων . . . 334
6.5.2 Λυμένες ασκήσεις . . . 334
6.5.3 Ασκήσεις προς επίλυση . . . 335
6.6 Δένδρα αληθείας . . . 336
6.6.1 Ασκήσεις προς επίλυση . . . 340
6.7 Αρχή της απόφασης . . . 341
6.7.1 Ασκήσεις προς επίλυση . . . 345
6.8 Κατηγορηματικός Λογισμός . . . 346
6.8.1 Εισαγωγή . . . 346
6.8.2 Πρωτοβάθμια γλώσσα . . . 348
6.8.3 Ελεύθερες και δεσμευμένες μεταβλητές . . . 350
6.8.4 Επαγωγικός ορισμός . . . 351
6.8.5 Αντικατάσταση . . . 352
6.8.6 Επαγωγική απόδειξη . . . 353
6.8.7 Ασκήσεις προς επίλυση . . . 354
6.9 Παράρτημα: Λογικοί γρίφοι και προβλήματα . . . 355
6.9.1 Ασκήσεις προς επίλυση . . . 359

7 Άλγεβρα Boole **365**
7.1 Δικτυωτά . . . 365
7.2 Δυαδική Άλγεβρα Boole . . . 367
7.2.1 Ορισμός . . . 367
7.2.2 Ιδιότητες . . . 368
7.2.3 Εξισώσεις . . . 370
7.2.4 Συστήματα . . . 371
7.2.5 Συναρτήσεις Boole . . . 372
7.2.6 Εφαρμογές . . . 373
7.3 Ασκήσεις προς επίλυση . . . 377

Βιβλιογραφία **380**

Κεφάλαιο 1

Βασικές έννοιες

1.1 Σύνολα

Το σύνολο είναι μια συλλογή αντικειμένων σαφώς καθορισμένων τα οποία θεωρούμε ως μια ολότητα. Τα αντικείμενα που απαρτίζουν ένα σύνολο ονομάζονται **στοιχεία** του συνόλου. Όταν θέλουμε να δηλώσουμε ότι το αντικείμενο x ανήκει (αντίστοιχα δεν ανήκει) στο σύνολο A, τότε σημειώνουμε $x \in A$ (αντίστοιχα $x \notin A$). Το **κενό σύνολο** είναι το σύνολο που δεν περιέχει κανένα στοιχείο και σημειώνεται με $\emptyset$.

Μερικά βασικά σύνολα είναι τα παρακάτω:
$\mathbb{N}$ το σύνολο των **φυσικών αριθμών**,
$\mathbb{Z}$ το σύνολο των **ακεραίων αριθμών**,
$\mathbb{Q}$ το σύνολο των **ρητών αριθμών**,
$\mathbb{R}$ το σύνολο των **πραγματικών αριθμών**,
$\mathbb{C}$ το σύνολο των **μιγαδικών αριθμών**.

Αν A είναι ένα από τα παραπάνω σύνολα, με A^* σημειώνουμε το σύνολο που αποτελείται από όλα τα μη μηδενικά στοιχεία του A.

1.1.1 Σχέσεις συνόλων

Εγκλεισμός: Ένα σύνολο A είναι **υποσύνολο** ενός συνόλου B (συμβολισμός $A \subseteq B$) αν και μόνο αν για κάθε $x \in A$ συνεπάγεται ότι $x \in B$[1]. Στην περίπτωση αυτή το B ονομάζεται **υπερσύνολο** του A. Όταν $A \subseteq B$ και υπάρχει ένα τουλάχιστο στοιχείο του B που δεν ανήκει στο A τότε το A ονομάζεται **γνήσιο υποσύνολο** του B (συμβολισμός $A \subset B$).

Το κενό σύνολο $\emptyset$ είναι υποσύνολο κάθε συνόλου A.

Ισότητα: Δύο σύνολα ονομάζονται ίσα (συμβολισμός $A = B$) όταν κάθε στοιχείο του ενός συνόλου ανήκει στο άλλο και αντιστρόφως. Προφανώς, ισχύει

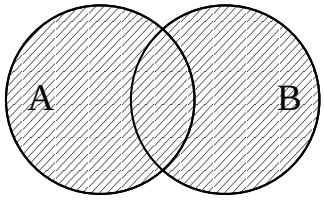
$$A = B \iff (A \subseteq B \text{ και } B \subseteq A).$$

1.1.2 Πράξεις συνόλων

(i) Αν A, B είναι δύο σύνολα, τότε η **ένωση** των A, B (συμβολισμός $A \cup B$) είναι το σύνολο που αποτελείται από τα στοιχεία που ανήκουν στο A ή στο B, δηλαδή

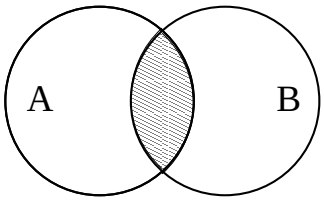
$$A \cup B = \{x : x \in A \text{ ή } x \in B\}.$$

[1] Ισοδύναμα, με αντιθετοαναστροφή, αν για κάθε $x \notin B$ συνεπάγεται ότι $x \notin A$.



(ii) Αν A, B είναι δύο σύνολα, τότε η **τομή** (συμβολισμός $A \cap B$) των A, B είναι το σύνολο που αποτελείται από τα κοινά στοιχεία των A, B, δηλαδή

$$A \cap B = \{x : x \in A \text{ και } x \in B\}.$$



Η ένωση και η τομή των συνόλων ορίζεται για περισσότερα από δύο σύνολα, δηλαδή

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i = \{x : \text{ Υπάρχει } i \in [n] \text{ με } x \in A_i\},$$

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i = \{x : x \in A_i \text{ για κάθε } i \in [n]\}$$

(όπου $[n] = \{1, 2, \ldots, n\}$).

Επίσης σημειώνουμε

$$\bigcup_{i=1}^{\infty} A_i = \{x : \text{ Υπάρχει } i \in \mathbb{N}^* \text{ με } x \in A_i\},$$

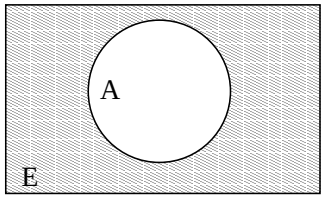
$$\bigcap_{i=1}^{\infty} A_i = \{x : x \in A_i \text{ για κάθε } i \in \mathbb{N}^*\}.$$

Γενικότερα, αν $(A_i)_{i \in I}$ είναι μια οικογένεια συνόλων ορίζεται η ένωση και η τομή τους ως εξής:

$$\bigcup_{i \in I} A_i = \{x : \text{ Υπάρχει } i \in I \text{ με } x \in A_i\},$$

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ για κάθε } i \in I\}.$$

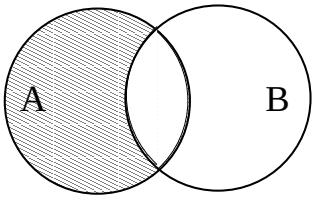
(iii) Έστω ένα σύνολο E (το οποίο πολλές φορές θα συμβολίζει το βασικό σύνολο) και $A \subseteq E$. Το **συμπλήρωμα** του συνόλου A (συμβολισμός $\overline{A}$) είναι το σύνολο όλων των στοιχείων του E που δεν ανήκουν στο A.



Άλλοι συμβολισμοί για το συμπλήρωμα είναι: A^c, CA και A'.

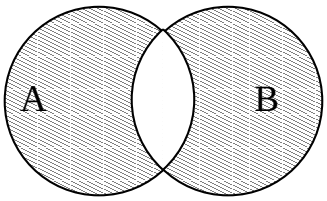
(iv) Αν A, B είναι δύο σύνολα, τότε η **διαφορά** του B από το A (συμβολισμός $A \setminus B$) είναι το σύνολο που αποτελείται από τα στοιχεία του A που δεν ανήκουν στο B, δηλαδή

$$A \setminus B = \{x : x \in A \text{ και } x \notin B\}.$$



(v) Αν A, B είναι δύο σύνολα, τότε η **συμμετρική διαφορά** των A και B (συμβολισμός $A \triangle B$) είναι το σύνολο όλων των στοιχείων του A που δεν ανήκουν στο B και όλων των στοιχείων του B που δεν ανήκουν στο A, δηλαδή

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$



Ιδιότητες πράξεων συνόλων

(i) $A \cup B = B \cup A$, $A \cap B = B \cap A$.

(ii) $A \cup (B \cup \Gamma) = (A \cup B) \cup \Gamma$, $A \cap (B \cap \Gamma) = (A \cap B) \cap \Gamma$.

(iii) $A \cap (B \cup \Gamma) = (A \cap B) \cup (A \cap \Gamma)$, $A \cup (B \cap \Gamma) = (A \cup B) \cap (A \cup \Gamma)$.

(iv) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (Κανόνες De Morgan).

Παράδειγμα. Έστω $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{1, 2, 3, 4, 5, 6\}$ και $B = \{2, 3, 5, 7, 9\}$. Τότε $A, B \subseteq E$ και $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 9\}$, $A \cap B = \{2, 3, 5\}$, $A^c = \{7, 8, 9, 10\}$, $B^c = \{1, 4, 6, 8, 10\}$, $A \setminus B = \{1, 4, 6\}$, $B \setminus A = \{7, 9\}$, $A \triangle B = \{1, 4, 6, 7, 9\}$

1.1.3 Δυναμοσύνολο

Το σύνολο όλων των υποσυνόλων ενός συνόλου E ονομάζεται **δυναμοσύνολο** του E και συμβολίζεται με $\mathcal{P}(E)$.

Παράδειγμα. Αν $E = \{\alpha, \beta, \gamma\}$ τότε

$$\mathcal{P}(E) = \{\emptyset, \{\alpha\}, \{\beta\}, \{\gamma\}, \{\alpha, \beta\}, \{\alpha, \gamma\}, \{\beta, \gamma\}, E\}.$$

1.1.4 Καρτεσιανό γινόμενο

Έστω A, B δυο μη κενά σύνολα, τότε **καρτεσιανό γινόμενο**, με πρώτο παράγοντα το A και δεύτερο παράγοντα το B, ονομάζεται το σύνολο όλων των διατεταγμένων ζευγών [2] (α, β) με $\alpha \in A$, $\beta \in B$ (συμβολισμός $A \times B$), δηλαδή

$$A \times B = \{(\alpha, \beta) : \alpha \in A \text{ και } \beta \in B\}.$$

Όταν το ένα (τουλάχιστον) από τα σύνολα A, B είναι το κενό σύνολο τότε ως καρτεσιανό γινόμενό τους ορίζεται το κενό σύνολο.

Παραδείγματα

1. Αν $A = \{1, 2, 3\}$ και $B = \{x, y\}$, τότε

$$\begin{aligned} A \times B &= \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}, \\ B \times A &= \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}, \\ A \times A &= \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}, \\ B \times B &= \{(x, x), (x, y), (y, x), (y, y)\}. \end{aligned}$$

2. Αν $A = \{2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A\}$ και $B = \{\clubsuit, \diamond, \heartsuit, \spadesuit\}$ τότε το καρτεσιανό γινόμενο $A \times B$ είναι το σύνολο των ενδείξεων των 52 χαρτιών της τράπουλας.

Η έννοια του καρτεσιανού γινομένου γενικεύεται για περισσότερους από δύο παράγοντες ως εξής:

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i \text{ για κάθε } i \in [n]\}.$$

Εξάλλου, αν $A_1 = A_2 = \cdots = A_n = A$ τότε το καρτεσιανό γινόμενο $\underbrace{A \times A \times \cdots \times A}_{n \text{ φορές}}$ σημειώνεται με A^n.

Ο συμβολισμός αυτός χρησιμοποιείται συχνά τόσο στη Μαθηματική Ανάλυση όσο και στη Γραμμική Άλγεβρα για τους χώρους $\mathbb{R}^2, \mathbb{R}^3, \ldots, \mathbb{R}^n$ των δύο, τριών, ..., n διαστάσεων.

1.1.5 Διαμερίσεις

Κάθε οικογένεια $(A_i)_{i \in I}$ μη κενών υποσυνόλων ενός συνόλου E, ορίζει μια **διαμέριση** του όταν τα σύνολα A_i είναι ανά δύο ξένα και η ένωσή τους είναι το E, δηλαδή

$$(A_i)_{i \in I} \text{ διαμέριση του } E \iff \left(\begin{array}{c} \emptyset \neq A_i \subseteq E \text{ για κάθε } i \in I \\ A_i \cap A_j = \emptyset \text{ για κάθε } i, j \in I \text{ με } i \neq j \\ \bigcup_{i \in I} A_i = E. \end{array} \right).$$

Παραδείγματα

[2] Στα διατεταγμένα ζεύγη, αντίθετα με τα σύνολα, έχει σημασία η σειρά (διάταξη) και έχουμε ότι αν $a \neq b$ τότε $(a, b) \neq (b, a)$ (ενώ στα σύνολα ισχύει ότι $\{a, b\} = \{b, a\}$). Τα διατεταγμένα ζεύγη μπορούν να ορισθούν χρησιμοποιώντας σύνολα. Ο πιο διαδεδομένος ορισμός είναι ο εξής:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

και οφείλεται στον Πολωνό μαθηματικό Kazimierz Kuratowski. Ένας τέτοιος ορισμός ονομάζεται *συνολοθεωρητικός* ορισμός.

1. Η οικογένεια $\{\{1,2,5\},\{3,4\},\{6,8\},\{7\}\}$ αποτελεί μια διαμέριση του συνόλου $[8] = \{1,2,3,4,5,6,7,8\}$.

2. Αν E είναι το σύνολο όλων των περιττών φυσικών αριθμών και A_i, $i \in I = \{1,3,5,7,9\}$, είναι το σύνολο όλων των φυσικών αριθμών που λήγουν σε i, τότε η οικογένεια $(A_i)_{i\in I}$ αποτελεί μια διαμέριση του E.

3. Έστω $E = \mathbb{R}$ και $A_i = [i, i+1)$, όπου $i \in \mathbb{Z}$, τότε η οικογένεια $(A_i)_{i\in\mathbb{Z}}$ αποτελεί μια διαμέριση του $\mathbb{R}$.

1.2 Σχέσεις

Έστω A, B δύο μη κενά σύνολα. Τότε κάθε μη κενό υποσύνολο R του $A \times B$ ορίζει μια **διμελή σχέση** (ή απλά **σχέση**) μεταξύ των στοιχείων των A και B. Συγκεκριμένα, αν για τα στοιχεία $\alpha \in A$ και $\beta \in B$ ισχύει $(\alpha,\beta) \in R$, τότε τα στοιχεία α, β *σχετίζονται μέσω της σχέσης* R και σημειώνουμε ότι $\alpha R \beta$, δηλαδή

$$\alpha R \beta \Longleftrightarrow (\alpha,\beta) \in R.$$

Αν $(a,b) \notin R$ λέμε ότι τα a, b *δεν σχετίζονται* μέσω της σχέσης R και σημειώνουμε $a \not R b$.

Στην περίπτωση όπου $A = B$ λέμε ότι η R είναι μια σχέση στο A (ή στο B).

Παραδείγματα

1. Αν E είναι το σύνολο όλων των φοιτητών του Τμήματος, τότε ορίζεται μια σχέση R των στοιχείων του E ως εξής:

$$aRb \Leftrightarrow \text{ οι } a, b \text{ είναι φίλοι.}$$

2. Αν E είναι το σύνολο των σπουδαστών ενός έτους, τότε ο προτασιακός τύπος "ο σπουδαστής α έχει την ίδια επίδοση με το σπουδαστή β" ορίζει μια σχέση των στοιχείων του E.

3. Αν E είναι το σύνολο των ευθειών του επιπέδου, τότε η καθετότητα ορίζει μια σχέση (την οποία συμβολίζουμε με $\perp$) μεταξύ των στοιχείων του E, με $\epsilon_1 \perp \epsilon_2$ όταν η ευθεία ϵ_1 είναι κάθετη στην ευθεία ϵ_2.

4. Αν E είναι το σύνολο των ανθρώπων, τότε ορίζεται μια σχέση R των στοιχείων του E ως εξής: aRb αν οι a, b είναι συγγενείς.

5. Αν A είναι το σύνολο όλων των άρτιων αριθμών τότε ορίζεται μια σχέση S των στοιχείων του $A \times A \times A$ ως εξής:

$$(a,b,c)S(x,y,z) \Leftrightarrow abc = x + y + z.$$

Η σχέση S είναι μια διμελής σχέση! Συσχετίζει ή όχι δύο στοιχεία του $A \times A \times A$.

Τρόποι ορισμού μιας διμελούς σχέσης

1. Με παράθεση των στοιχείων της.

Για παράδειγμα, αν $A = \{1,2,3\}$, $B = \{a,b,c,d\}$, τότε μια σχέση σ αποτελείται από τα ζεύγη

$$\sigma = \{(1,a),(1,b),(2,a),(2,b),(2,c)\}.$$

2. Με αντιστοιχία ανάμεσα στα δύο σύνολα (όχι απαραίτητα απεικόνιση[3]).

   Για παράδειγμα, η προηγούμενη σχέση σ μπορεί να ορισθεί από την αντιστοιχία $\Gamma : A \to B$ με

   $$\Gamma(1) = \{a, b\},\ \Gamma(2) = \{a, b, c\},\ \Gamma(3) = \varnothing,$$

   με την οποία δηλώνουμε οτι το 1 σχετίζεται με τα a, b, το 2 με τα a, b, c και το 3 δεν σχετίζεται με κανένα στοιχείο του B.

3. Με προτασιακό τύπο, ή ιδιότητα.

   Για παράδειγμα, έστω $A = \{1, 2, 3, 4, 5, 6, 7, 9\}$, $B = \{0, 1, 2, 3\}$.

   Ο προτασιακός τύπος (ιδιότητα): "το υπόλοιπο της διαίρεσης του $a \in A$ με το 3 είναι $b \in B$" ορίζει τη σχέση

   $$\{(1, 1), (2, 2), (3, 0), (4, 1), (5, 2), (6, 0), (7, 1), (8, 2), (9, 0)\}.$$

1.2.1 Ισοδυναμία

Μια σχέση R στο E ονομάζεται **ισοδυναμία** όταν ικανοποιεί τις ιδιότητες:

(i) $\alpha R \alpha$, για κάθε $a \in E$ (**ανακλαστική**).

(ii) $\alpha R \beta \Leftrightarrow \beta R \alpha$, για κάθε $\alpha, \beta \in E$ (**συμμετρική**).

(iii) $\alpha R \beta$ και $\beta R \gamma \Longrightarrow \alpha R \gamma$, για κάθε $\alpha, \beta, \gamma \in E$ (**μεταβατική**).

Συνήθως η σχέση ισοδυναμίας σημειώνεται με $\sim$ αντί R.

Παραδείγματα

1. Αν E είναι το σύνολο των ευθειών ενός επιπέδου, τότε η παραλληλία (με την ευρεία έννοια) ορίζει μια σχέση ισοδυναμίας, με $\epsilon_1 \sim \epsilon_2$ όταν οι ευθείες ϵ_1, ϵ_2 είναι παράλληλες.

2. Αν $E = \mathbb{N}^*$ τότε το σύνολο $R = \{(x, y) : |x-y| \text{ πολλαπλάσιο του } 2\}$ ορίζει μια σχέση ισοδυναμίας, με $n_1 \sim n_2$ όταν $\frac{n_1 - n_2}{2}$ είναι ακέραιος αριθμός.

Αν $\sim$ είναι μια σχέση ισοδυναμίας στο σύνολο E και $\alpha \in E$ τότε το σύνολο

$$C_\alpha = \{\beta \in E : \beta \sim \alpha\}$$

ονομάζεται **κλάση ισοδυναμίας** του στοιχείου α.

Οι κλάσεις ισοδυναμίας μπορεί να συμπίπτουν για ορισμένα $\alpha \in E$. Συγκεκριμένα ισχύουν οι παρακάτω ιδιότητες:

1. $\alpha \in C_\alpha$, για κάθε $\alpha \in E$.
2. $\alpha \sim \beta \Longrightarrow C_\alpha = C_\beta$.
3. $\alpha \nsim \beta \Longrightarrow C_\alpha \cap C_\beta = \emptyset$.

[3] βλέπε ενότητα 1.3.

Η πρώτη ιδιότητα ισχύει διότι η σχέση $\sim$ είναι ανακλαστική. Για την απόδειξη της δεύτερης ιδιότητας θεωρούμε $\alpha \sim \beta$ και $x \in C_\alpha$· τότε $x \sim \alpha$, οπότε από τη μεταβατική ιδιότητα προκύπτει ότι $x \sim \beta$ και επομένως $x \in C_\beta$. Άρα $C_\alpha \subseteq C_\beta$. Ανάλογα αποδεικνύεται ότι $C_\beta \subseteq C_\alpha$, οπότε τελικά $C_\alpha = C_\beta$. Τέλος, για την απόδειξη της τρίτης ιδιότητας, θεωρούμε ότι $C_\alpha \cap C_\beta \neq \emptyset$ και έστω $x \in C_\alpha \cap C_\beta$, τότε $x \sim \alpha$ και $x \sim \beta$ οπότε από τη συμμετρική και από τη μεταβατική ιδιότητα προκύπτει ότι $\alpha \sim \beta$ το οποίο είναι άτοπο. Άρα $C_\alpha \cap C_\beta = \emptyset$.

Από τις τρεις ιδιότητες αυτές προκύπτει ότι:

Κάθε σχέση ισοδυναμίας στο E ορίζει μια διαμέριση του E.

Ισχύει και το **αντίστροφο**, δηλαδή αν (A_i) είναι μια διαμέριση του E, τότε ορίζουμε τη σχέση R στο E ως εξής:

$$xRy \Leftrightarrow \text{ Υπάρχει } i \in I \text{ με } x, y \in A_i.$$

Εύκολα προκύπτει ότι η σχέση αυτή ικανοποιεί τις ιδιότητες (i), (ii) και (iii) οπότε είναι μια σχέση ισοδυναμίας με κλάσεις ισοδυναμίας τα σύνολα A_i.

Το σύνολο $\{C_\alpha : \alpha \in E\}$ ονομάζεται **σύνολο πηλίκο** του E για τη σχέση $\sim$ και συμβολίζεται με $E/\sim$.

1.2.2 Διάταξη

Μια σχέση R στο E ονομάζεται (**μερική**) **διάταξη** όταν ικανοποιεί τις ιδιότητες:

(i) $\alpha R \alpha$, για κάθε $\alpha \in E$ (**ανακλαστική**).

(ii) $\alpha R \beta$ και $\beta R \alpha \Longrightarrow \alpha = \beta$, για κάθε $\alpha, \beta \in E$ (**αντισυμμετρική**).

(iii) $\alpha R \beta$ και $\beta R \gamma \Longrightarrow \alpha R \gamma$, για κάθε $\alpha, \beta, \gamma \in E$ (**μεταβατική**).

Συνήθως η σχέση διάταξης σημειώνεται με $\leq$.
Η διάταξη ονομάζεται **ολική** αν ικανοποιεί την ιδιότητα

$$\alpha \leq \beta \text{ ή } \beta \leq \alpha, \text{ για κάθε } \alpha, \beta \in E.$$

Παραδείγματα

1. Η σχέση $\leq$ στο $\mathbb{R}$ είναι ολική διάταξη, ενώ η σχέση $<$ στο $\mathbb{R}$ δεν είναι διάταξη.

2. Η σχέση διαιρετότητας I στο $\mathbb{N}^*$ είναι μερική διάταξη.

3. Η σχέση εγκλεισμού στο $\mathcal{P}(E)$ είναι μερική διάταξη.

Ένα σύνολο E εφοδιασμένο με μια μερική (αντίστοιχα ολική) διάταξη ονομάζεται **μερικά** (αντίστοιχα **ολικά**) **διατεταγμένο** σύνολο και σημειώνεται με $(E, \leq)$.

Αν $(E, \leq)$ είναι ένα διατεταγμένο σύνολο και A είναι ένα μη κενό υποσύνολό του, τότε ένα στοιχείο $\alpha \in E$ (αντίστοιχα $\beta \in E$) ονομάζεται **άνω** (αντίστοιχα **κάτω**) **φράγμα** του A όταν $x \leq \alpha$ (αντίστοιχα $\beta \leq x$) για κάθε $x \in A$. Όταν υπάρχει ένα τουλάχιστον άνω (αντίστοιχα κάτω) φράγμα ενός συνόλου A, τότε το σύνολο αυτό ονομάζεται **άνω** (αντίστοιχα **κάτω**) **φραγμένο** σύνολο.

Αν A είναι ένα άνω (αντίστοιχα κάτω) φραγμένο υποσύνολο του $(E, \leq)$ τότε ένα στοιχείο $s \in E$ (αντίστοιχα $i \in E$) που ικανοποιεί τις ιδιότητες:

(i) s είναι άνω φράγμα (αντίστοιχα i είναι κάτω φράγμα),

(ii) $s \leq \alpha$ (αντίστοιχα $\beta \leq i$) για κάθε άνω φράγμα α (αντίστοιχα κάτω φράγμα β) του A

ονομάζεται **supremum** ή **άνω πέρας** (αντίστοιχα **infimum** ή **κάτω πέρας**) του A και σημειώνεται με $\sup A$ (αντίστοιχα $\inf A$).

Πρέπει να τονισθεί ότι τα $\sup A$ και $\inf A$ δεν υπάρχουν πάντα για ένα σύνολο. Όταν όμως υπάρχουν είναι μοναδικά. Γενικά το $\sup A$ (αντίστοιχα $\inf A$) δεν ανήκει υποχρεωτικά στο σύνολο A. Όμως, στην περίπτωση που ανήκει, ονομάζεται **μέγιστο** (αντίστοιχα **ελάχιστο**) **στοιχείο** του A και σημειώνεται με $\max A$ (αντίστοιχα $\min A$).

Παραδείγματα

1. Για το ολικά διατεταγμένο σύνολο $(\mathbb{R}, \leq)$ είναι:
   α) Αν $A = \{\frac{1}{n} : n \in \mathbb{N}^*\}$ τότε $\sup A = 1$ και $\inf A = 0$.
   β) Αν $A = (\alpha, \beta)$ τότε $\sup A = \beta$ και $\inf A = \alpha$.

2. Για το μερικά διατεταγμένο σύνολο $(\mathbb{N}^*, |)$, όπου $|$ είναι η σχέση διαιρετότητας και $A = \{4, 16, 28, 40\}$ είναι $\sup A = \text{ΕΚΠ}(4, 16, 28, 40) = 560$ και $\inf A = \text{ΜΚΔ}(4, 16, 28, 40) = 4$.

3. Για το μερικά διατεταγμένο σύνολο $(\mathcal{P}(E), \subseteq)$ και για $A = \{B_i : i \in I\}$ είναι
$$\sup A = \bigcup_{i \in I} B_i \text{ και } \inf A = \bigcap_{i \in I} B_i.$$

1.2.3 Πράξεις σχέσεων

Οι πράξεις μεταξύ σχέσεων ορίζονται όπως στα σύνολα. Συγκεκριμένα, έστω R, R_1, R_2 σχέσεις στο $A \times B$.

(i) Η ένωση των R_1, R_2 (συμβολισμός $R_1 \cup R_2$) ορίζεται ως εξής:
$$R_1 \cup R_2 = \{(x, y) \in A \times B : (x, y) \in R_1 \text{ ή/και } (x, y) \in R_2\}.$$

(ii) Η τομή των R_1, R_2 (συμβολισμός $R_1 \cap R_2$) ορίζεται ως εξής:
$$R_1 \cap R_2 = \{(x, y) \in A \times B : (x, y) \in R_1 \text{ και } (x, y) \in R_2)\}.$$

(iii) Το συμπλήρωμα της R (συμβολισμός $\overline{R}$) ορίζεται ως εξής:
$$\overline{R} = \{(x, y) \in A \times B : (x, y) \notin R\}.$$

(iv) Η διαφορά της R_2 από την R_1 (συμβολισμός $R_1 \setminus R_2$) ορίζεται ως εξής:
$$R_1 \setminus R_2 = \{(x, y) \in A \times B : (x, y) \in R_1 \text{ και } (x, y) \notin R_2\}.$$

(v) Η αντίστροφη σχέση της R (συμβολισμός R^{-1}) ορίζεται ως εξής:
$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}.$$

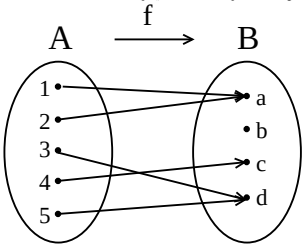
Επιπλέον ορίζονται οι παρακάτω πράξεις:

(vi) Η σύνθεση των R_1, R_2 (συμβολισμός $R_2 \circ R_1$) ορίζεται ως εξής:
$$R_2 \circ R_1 = \{(x, y) \in A \times B : \text{ Υπάρχει } z \in A \cap B \text{ για το οποίο } (x, z) \in R_1 \text{ και } (z, y) \in R_2\}$$

(vii) Η πρώτη και δεύτερη προβολή της R (συμβολισμός $\text{proj}_1 R$ και $\text{proj}_2 R$) ορίζονται ως εξής:
$$\text{proj}_1 R = \{x \in A : \text{ Υπάρχει } y \in B \text{ με } (x, y) \in R\},$$
$$\text{proj}_2 R = \{y \in B : \text{ Υπάρχει } x \in A \text{ με } (x, y) \in R\}.$$

1.3 Απεικονίσεις

Δίνονται δύο μη κενά σύνολα A, B και ένας κανόνας (που συνήθως μπορεί να περιγραφεί από ένα τύπο) με τον οποίο αντιστοιχίζουμε σε κάθε στοιχείο του A ένα και μόνο ένα στοιχείο του B. Τότε ορίζεται μια απεικόνιση f του A στο B (συμβολισμός $f : A \to B$).



Το σύνολο A ονομάζεται **πεδίο ορισμού** της f και συμβολίζεται με $D(f)$ ή D_f τα δε στοιχεία του ονομάζονται **πρότυπα**. Αν το πρότυπο α αντιστοιχίζεται μέσω της f στο στοιχείο β, τότε σημειώνουμε $f(\alpha) = \beta$. Στην περίπτωση αυτή το β ονομάζεται **εικόνα** του στοιχείου α.

Το υποσύνολο του B που αποτελείται από όλες τις εικόνες ονομάζεται **σύνολο τιμών** της f και συμβολίζεται με $R(f)$ ή R_f, δηλαδή

$$R(f) = \{\beta \in B : \text{ Υπάρχει } \alpha \in A \text{ με } f(\alpha) = \beta\}.$$

Μια απεικόνιση $f : A \to \mathbb{R}$ με $A \subseteq \mathbb{R}$ ονομάζεται **πραγματική συνάρτηση μιας μεταβλητής** (ή απλά **συνάρτηση**). Στην περίπτωση αυτή το τυχαίο στοιχείο του A συμβολίζεται συνήθως με x και ονομάζεται **ανεξάρτητη μεταβλητή** ενώ η εικόνα του $y = f(x)$ ονομάζεται **τιμή** της ανεξάρτητης μεταβλητής. Το τυχαίο στοιχείο $y \in R(f)$ ονομάζεται **εξαρτημένη μεταβλητή**.

Γενικότερα, αν $A \subseteq \mathbb{R}^n$ η απεικόνιση $f : A \to R$ ονομάζεται πραγματική συνάρτηση n μεταβλητών. Εδώ έχουμε n το πλήθος ανεξάρτητες μεταβλητές και μια εξαρτημένη $y = f(x_1, x_2, \ldots, x_n)$.

Η απεικόνιση $f : A \to A$ με $f(x) = x$ για κάθε $x \in A$ ονομάζεται **ταυτοτική απεικόνιση** του A και σημειώνεται με 1_A.

Μια απεικόνιση f ονομάζεται **σταθερή** αν το σύνολο τιμών της είναι μονοσύνολο, δηλαδή $R(f) = \{\beta\}$.

Αν A είναι ένα μη κενό υποσύνολο ενός συνόλου E τότε η απεικόνιση $f : E \to \{0, 1\}$ με

$$f(x) = \begin{cases} 1, & \text{αν } x \in A \\ 0, & \text{αν } x \notin A \end{cases}$$

ονομάζεται **χαρακτηριστική συνάρτηση του** A και συμβολίζεται με μ_A (ή χ_A). Η χαρακτηριστική συνάρτηση χρησιμεύει για τον καθορισμό των σχέσεων και πράξεων των συνόλων όπως φαίνεται και από τις επόμενες ιδιότητες.

(i) $A = B$ αν και μόνο αν $\mu_A(x) = \mu_B(x)$, για κάθε $x \in E$.

(ii) $A \subseteq B$ αν και μόνο αν $\mu_A(x) \leq \mu_B(x)$, για κάθε $x \in E$.

(iii) $\mu_{A\cup B}(x) = \max\{\mu_A(x), \mu_B(x)\} = \mu_A(x) + \mu_B(x) - \mu_{A\cap B}(x)$, για κάθε $x \in E$.

(iv) $\mu_{A\cap B}(x) = \min\{\mu_A(x), \mu_B(x)\} = \mu_A(x) \cdot \mu_B(x)$, για κάθε $x \in E$.

1.3.1 Αμφιμονοσήμαντες απεικονίσεις

(i) Μια απεικόνιση $f : A \to B$ ονομάζεται $1-1$ όταν δύο οποιαδήποτε διαφορετικά πρότυπα έχουν διαφορετικές εικόνες, δηλαδή:

$$\text{Για κάθε } x_1, x_2 \in A \text{ με } x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2).$$

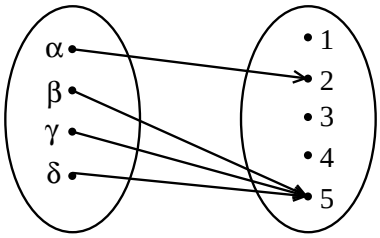
Ισοδύναμα για κάθε $x_1, x_2 \in A$ με $f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$.

(ii) Μια απεικόνιση $f : A \to B$ ονομάζεται **επί** όταν κάθε στοιχείο του B είναι εικόνα κάποιου στοιχείου του A, δηλαδή όταν $B = R(f)$.

(iii) Μια απεικόνιση $f : A \to B$ ονομάζεται **αμφιμονοσήμαντη** όταν είναι $1-1$ και επί.

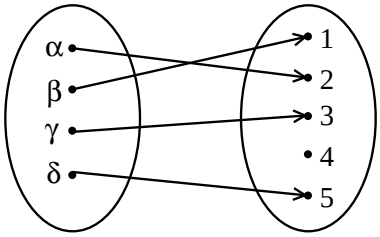
Παραδείγματα

1.



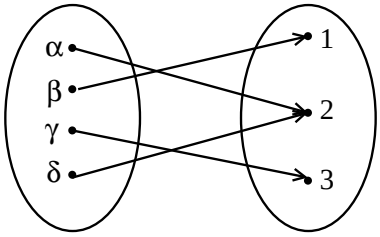
Δεν είναι ούτε 1-1 ούτε επί.

2.



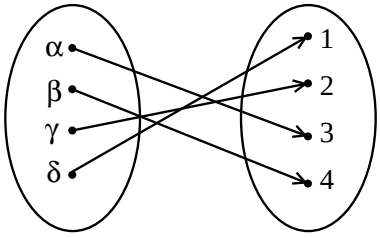
Είναι 1-1, αλλά όχι επί.

3.



Είναι επί, αλλά όχι 1-1.

4.



Είναι αμφιμονοσήμαντη.

1.3.2 Γραφική παράσταση

Έστω η απεικόνιση $f : A \to B$, τότε το σύνολο

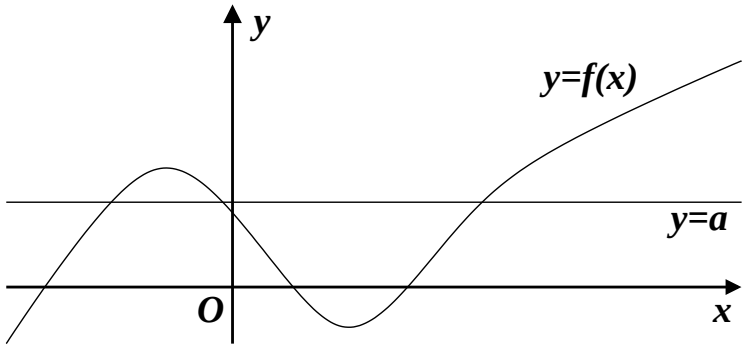
$$\{(x, y) \in A \times B : y = f(x)\}$$

ονομάζεται **γραφική παράσταση** ή (**διάγραμμα**) της απεικόνισης f και συμβολίζεται με $G(f)$ (ή G_f).

Η γραφική παράσταση μιας πραγματικής συνάρτησης μιας μεταβλητής συνήθως είναι δυνατό να σχεδιασθεί στο Καρτεσιανό επίπεδο και έχει την ιδιότητα ότι κάθε παράλληλη ευθεία προς τον άξονα Oy την τέμνει σε ένα το πολύ σημείο.

Αν η συνάρτηση είναι $1-1$, τότε και κάθε παράλληλη ευθεία προς τον άξονα Ox πρέπει να την τέμνει σε ένα το πολύ σημείο.

Παράδειγμα.



Η συνάρτηση $y = f(x)$ δεν είναι $1-1$ διότι τέμνεται από την ευθεία $y = a$ σε τρία σημεία.

Υπάρχουν συναρτήσεις των οποίων δεν είναι δυνατό να σχεδιασθεί η γραφική παράσταση. Ένα τέτοιο παράδειγμα είναι **η συνάρτηση του Dirichlet** που ορίζεται ως εξής:

$$f(x) = \begin{cases} 1, & \text{αν } x \in \mathbb{Q} \\ 0, & \text{αν } x \notin \mathbb{Q}. \end{cases}$$

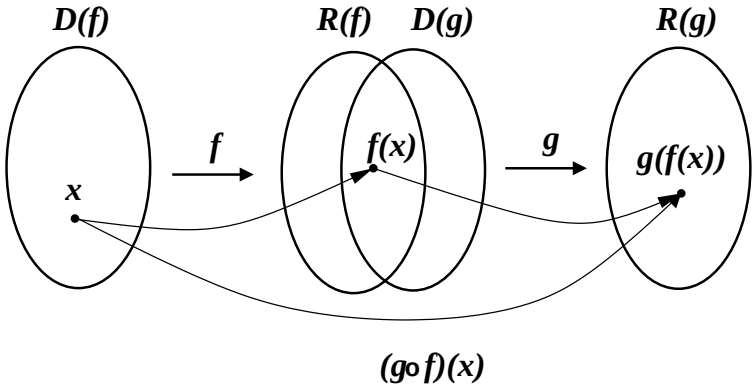
1.3.3 Σύνθεση απεικονίσεων

Δίνονται δύο απεικονίσεις f, g με $R(f) \cap D(g) \neq \emptyset$.

Τότε ορίζεται μια καινούρια απεικόνιση που ονομάζεται **σύνθεση** της g με την f, και συμβολίζεται με $g \circ f$, ως εξής:

$$D(g \circ f) = \{x \in D(f) : f(x) \in D(g)\},$$

$$(g \circ f)(x) = g(f(x)).$$



Παράδειγμα. Δίνονται οι συναρτήσεις f, g με τύπους $f(x) = x^2 + 2$ και $g(x) = \sqrt{x-6}$.

Τότε $D(f) = \mathbb{R}$, $R(f) = [2, +\infty)$, $D(g) = [6, +\infty)$ και $R(g) = [0, +\infty)$.

Είναι

$$D(g \circ f) = \{x \in D(f) : f(x) \in D(g)\} = \{x \in \mathbb{R} : x^2 + 2 \geq 6\} = (-\infty, -2] \cup [2, +\infty)$$

και $(g \circ f)(x) = g(f(x)) = \sqrt{f(x) - 6} = \sqrt{x^2 - 4}$.

Επιπλέον,

$$D(f \circ g) = \{x \in D(g) : g(x) \in D(f)\} = \{x \in [6, +\infty) : \sqrt{x - 6} \in \mathbb{R}\} = [6, +\infty)$$

και $(f \circ g)(x) = f(g(x)) = (g(x))^2 + 2 = x - 4$.

Όπως προκύπτει και από το προηγούμενο παράδειγμα οι συναρτήσεις $g \circ f$ και $f \circ g$ είναι εν γένει διαφορετικές.

1.3.4 Αντίστροφη απεικόνιση

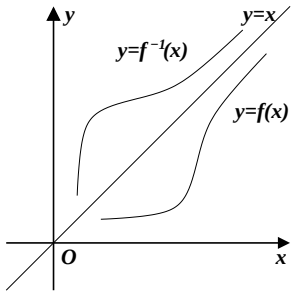
Έστω $f : A \to B$ μια αμφιμονοσήμαντη απεικόνιση. Τότε η **αντίστροφη απεικόνιση** της f, που συμβολίζεται με f^{-1}, είναι η απεικόνιση που σε κάθε $y \in B$ αντιστοιχεί το μοναδικό $x \in A$ με $f(x) = y$, δηλαδή ισχύει :

$$f^{-1} : B \to A \text{ με } f^{-1}(y) = x \Leftrightarrow f(x) = y.$$

Εύκολα προκύπτει ότι $f^{-1} \circ f = 1_A$ και $f \circ f^{-1} = 1_B$.

Προκειμένου να ορίσουμε την αντίστροφη απεικόνιση μιας $1 - 1$ αλλά όχι επί απεικόνισης $f : A \to B$ θεωρούμε αντί του συνόλου B το σύνολο $R(f)$ και ορίζουμε την $f^{-1} : R(f) \to A$.

Η γραφική παράσταση της αντίστροφης μιας αμφιμονοσήμαντης συνάρτησης μιας μεταβλητής f στο Καρτεσιανό επίπεδο είναι συμμετρική της γραφικής παράστασης της f ως προς την ευθεία $y = x$.



1.3.5 Εικόνες συνόλων

Αν $f : A \to B$ είναι μια απεικόνιση και $\Gamma \subseteq A$, $\Delta \subseteq B$, τότε τα σύνολα

$$f(\Gamma) = \{y \in B : \text{ Υπάρχει } x \in \Gamma \text{ με } y = f(x)\}$$

και

$$f^{-1}(\Delta) = \{x \in A : f(x) \in \Delta\}$$

ονομάζονται αντίστοιχα **εικόνα** του Γ και **αντίστροφη εικόνα** του Δ.

Εύκολα αποδεικνύονται οι παρακάτω ιδιότητες:

1. $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$.
2. $f(f^{-1}(\Delta)) \subseteq \Delta$ και $f^{-1}(f(\Gamma)) \supseteq \Gamma$.
3. (i) $f(\Gamma_1) \subseteq f(\Gamma_2)$, όταν $\Gamma_1 \subseteq \Gamma_2 \subseteq A$.
   (ii) $f^{-1}(\Delta_1) \subseteq f^{-1}(\Delta_2)$, όταν $\Delta_1 \subseteq \Delta_2 \subseteq B$.
4. (i) $f(\Gamma_1 \cup \Gamma_2) = f(\Gamma_1) \cup f(\Gamma_2)$, όταν $\Gamma_1, \Gamma_2 \subseteq A$.
   (ii) $f^{-1}(\Delta_1 \cup \Delta_2) = f^{-1}(\Delta_1) \cup f^{-1}(\Delta_2)$, όταν $\Delta_1, \Delta_2 \subseteq B$.
5. (i) $f(\Gamma_1 \cap \Gamma_2) \subseteq f(\Gamma_1) \cap f(\Gamma_2)$, όταν $\Gamma_1, \Gamma_2 \subseteq A$.
   (ii) $f^{-1}(\Delta_1 \cap \Delta_2) = f^{-1}(\Delta_1) \cap f^{-1}(\Delta_2)$, όταν $\Delta_1, \Delta_2 \subseteq B$.

1.4 Ισοδύναμα σύνολα

Δυο μη κενά σύνολα ονομάζονται **ισοδύναμα** (συμβολισμός $A \sim B$) όταν υπάρχει αμφιμονοσήμαντη απεικόνιση μεταξύ τους.

Ένα μη κενό σύνολο A ονομάζεται **πεπερασμένο** όταν είναι ισοδύναμο με ένα **τμήμα** του $\mathbb{N}^*$, δηλαδή υπάρχει $n \in \mathbb{N}^*$ με $A \sim [n]$.

Ισχύς (ή **πληθάριθμος**, ή **πληθικός αριθμός**) ενός πεπερασμένου συνόλου A ονομάζεται ο αριθμός των στοιχείων του και σημειώνεται με $|A|$ (ή card(A)). Έτσι, είναι

$$|A| = n \Leftrightarrow A \sim [n].$$

Το κενό σύνολο θεωρείται επίσης πεπερασμένο και η ισχύς του είναι ίση με 0.

Ένα σύνολο ονομάζεται **άπειρο** όταν δεν είναι πεπερασμένο. Τα άπειρα σύνολα διακρίνονται σε **αριθμήσιμα** και **υπεραριθμήσιμα**. Ένα άπειρο σύνολο ονομάζεται **αριθμήσιμο** (αντίστοιχα **υπεραριθμήσιμο**) όταν είναι (αντίστοιχα δεν είναι) ισοδύναμο προς το $\mathbb{N}^*$. Ένα σύνολο ονομάζεται **το πολύ αριθμήσιμο** αν είναι πεπερασμένο ή αριθμήσιμο.

Αποδεικνύεται ότι κάθε υποσύνολο ενός αριθμήσιμου συνόλου είναι το πολύ αριθμήσιμο.

Παραδείγματα

1. Το σύνολο $A = \{3, 9, -7, 1/2, -12, 3/4\}$ είναι πεπερασμένο με $|A| = 6$.
2. Το συνολο A των αρτίων φυσικών αριθμών είναι αριθμήσιμο, διότι η απεικόνιση $f : A \to \mathbb{N}^*$ με $f(x) = \frac{1}{2}x$ είναι αμφιμονοσήμαντη, οπότε $A \sim \mathbb{N}^*$.

3. Το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών είναι αριθμήσιμο, διότι η απεικόνιση $f : \mathbb{Z} \to \mathbb{N}^*$ με

$$f(x) = \begin{cases} 2x, & \text{αν } x > 0 \\ -2x + 1, & \text{αν } x \leq 0 \end{cases}$$

είναι αμφιμονοσήμαντη, οπότε $\mathbb{Z} \sim \mathbb{N}^*$.

Αν A, B είναι δύο μη κενά σύνολα τότε θα σημειώνουμε με B^A το σύνολο όλων των απεικονίσεων από το A στο B.

Πρόταση 1.1. *Αν E είναι μη κενό σύνολο τότε $\mathcal{P}(E) \sim \{0,1\}^E$.*

Απόδειξη. Προκύπτει άμεσα από το γεγονός ότι η απεικόνιση $f : \mathcal{P}(E) \to \{0,1\}^E$ με $f(A) = \mu_A$ είναι αμφιμονοσήμαντη. □

1.4.1 Ιδιότητες πεπερασμένων συνόλων

Αν A, B είναι δύο πεπερασμένα μη κενά σύνολα τότε τα σύνολα $A \cup B$, B^A και $\mathcal{P}(A)$ είναι πεπερασμένα και ισχύουν οι ισότητες :

(i) $|A \cup B| = |A| + |B| - |A \cap B|$.

(ii) $|A \times B| = |A||B|$.

(iii) $|B^A| = |B|^{|A|}$.

(iv) $|\mathcal{P}(A)| = 2^{|A|}$.

Η απόδειξη της (i) αρχικά γίνεται όταν A, B είναι ξένα σύνολα. Αν $|A| = n$ και $|B| = m$ τότε θα υπάρχουν αμφιμονοσήμαντες απεικονίσεις $f : A \to [n]$ και $g : B \to \{n+1, n+2, \ldots, n+m\}$. Επειδή $A \cap B = \emptyset$ ορίζεται η απεικόνιση $h : A \cup B \to [m+n]$ με

$$h(x) = \begin{cases} f(x), & \text{αν } x \in A \\ g(x), & \text{αν } x \in B. \end{cases}$$

Εύκολα αποδεικνύεται ότι η απεικόνιση αυτή είναι αμφιμονοσήμαντη, οπότε $A \cup B \sim [n+m]$ και $|A \cup B| = n + m = |A| + |B|$.

Στη συνέχεια θεωρούμε τη γενική περίπτωση (όπου δηλαδή τα A, B δεν είναι κατ΄ ανάγκη ξένα). Επειδή τα σύνολα $A, B \setminus A$ είναι ξένα, σύμφωνα με τα προηγούμενα προκύπτει ότι

$$|A \cup B| = |A \cup (B \setminus A)| = |A| + |B \setminus A|.$$

Επιπλέον τα σύνολα $B \setminus A$ και $A \cap B$ είναι επίσης ξένα, οπότε θα ισχύει ότι

$$|B| = |(B \setminus A) \cup (A \cap B)| = |B \setminus A| + |A \cap B|.$$

Από τις παραπάνω δύο ισότητες προκύπτει ότι

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Σημειώνουμε ότι στην ειδική περίπτωση των ξένων συνόλων η προηγούμενη ιδιότητα επεκτείνεται επαγωγικά για περισσότερα από δύο σύνολα, δηλαδή ισχύει ότι

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

όταν $A_i \cap A_j \neq \emptyset$, για κάθε $i \neq j$.

Η παραπάνω ισότητα χρησιμοποιείται για την απόδειξη της ιδιότητας (ii).

Πραγματικά αν $A = \{x_1, x_2, \ldots, x_n\}$ και $A_i = \{x_i\} \times B$, $i \in [n]$, τα σύνολα A_i είναι ξένα ανά δύο μεταξύ τους και ισχύει ότι $A_i \sim B$ για κάθε $i \in [n]$. Οπότε προκύπτει ότι

$$|A \times B| = |\bigcup_{i=1}^{n} A_i| = |A_1| + |A_2| + \cdots + |A_n| = \underbrace{|B| + |B| + \cdots + |B|}_{n \text{ φορές}} = n|B| = |A||B|.$$

Σημειώνουμε ότι η ιδιότητα (ii) επεκτείνεται επαγωγικά για περισσότερους από δύο παράγοντες, δηλαδή ισχύει ότι

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1||A_2| \cdots |A_n|.$$

Για την απόδειξη της ιδιότητας (iii) αν $A = \{x_1, x_2, \ldots, x_n\}$ θεωρούμε την απεικόνιση $f : B^A \to B^n$ με

$$f(g) = (g(x_1), g(x_2), \ldots, g(x_n))$$

για κάθε $g \in B^A$. Αποδεικνύεται ότι η απεικόνιση αυτή είναι αμφιμονοσήμαντη και επομένως $B^A \sim B^n$. Άρα ισχύει,

$$|B^A| = |B^n| = |B \times B \times \cdots \times B| = \underbrace{|B||B| \cdots |B|}_{n \text{ φορές}} = |B|^n = |B|^{|A|}.$$

Τέλος για την απόδειξη της ιδιότητας (iv) επειδή $\mathcal{P}(A) \sim \{0,1\}^A$ χρησιμοποιούμε την ιδιότητα (iii) και προκύπτει ότι

$$|\mathcal{P}(A)| = |\{0,1\}^A| = |\{0,1\}|^{|A|} = 2^{|A|}.$$

1.4.2 Βασικά αριθμήσιμα σύνολα

(i) *Το σύνολο $\mathbb{N}^* \times \mathbb{N}^*$ είναι αριθμήσιμο.*

Πραγματικά αν θεωρήσουμε την απεικόνιση $f : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$ με $f(m,n) = 2^m 3^n$ εύκολα προκύπτει ότι είναι $1-1$, οπότε $\mathbb{N}^* \times \mathbb{N}^* \sim R(f)$. Επειδή το σύνολο $R(f)$ είναι το πολύ αριθμήσιμο και άπειρο (αφού είναι ισοδύναμο με το $\mathbb{N}^* \times \mathbb{N}^*$) θα είναι αριθμήσιμο, οπότε και το $\mathbb{N}^* \times \mathbb{N}^*$ που είναι ισοδύναμό του θα είναι αριθμήσιμο.

(ii) *Το σύνολο $\mathbb{Q}$ των ρητών αριθμών είναι αριθμήσιμο.*

Θεωρούμε το σύνολο $A = \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* : \text{ΜΚΔ}(m,n) = 1\}$ και $\mathbb{Q}^+$ το σύνολο των θετικών ρητών αριθμών, δηλαδή

$$\mathbb{Q}^+ = \{x \in \mathbb{R} : x = \frac{m}{n} \text{ όπου } n, m \in \mathbb{N}^*\}.$$

Εύκολα αποδεικνύεται ότι η απεικόνιση $f : A \to \mathbb{Q}^+$ με $f(m,n) = \frac{m}{n}$ είναι αμφιμονοσήμαντη οπότε $A \sim \mathbb{Q}^+$. Επειδή το σύνολο A είναι άπειρο υποσύνολο του αριθμήσιμου συνόλου $\mathbb{N}^* \times \mathbb{N}^*$ θα είναι και αυτό αριθμήσιμο. Άρα το σύνολο $\mathbb{Q}^+$ είναι αριθμήσιμο.

Θεωρώντας την αμφιμονοσήμαντη απεικόνιση $g : \mathbb{Q}^+ \to \mathbb{Q}^-$ με $g(x) = -x$ προκύπτει ότι και το σύνολο $\mathbb{Q}^-$ των αρνητικών ρητών αριθμών θα είναι αριθμήσιμο. Έτσι και το σύνολο $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ θα είναι επίσης αριθμήσιμο.

Σημειώνουμε ότι αποδεικνύεται ότι η ένωση, το πολύ αριθμήσιμων το πλήθος, αριθμήσιμων συνόλων είναι αριθμήσιμο σύνολο (Άσκηση).

1.4.3 Βασικά υπεραριθμήσιμα σύνολα

(i) *Το διάστημα* $[0,1]$ *είναι υπεραριθμήσιμο.*

Απόδειξη. Η απόδειξη θα γίνει με τη μέθοδο της εις άτοπον απαγωγής.

Έστω ότι το διάστημα $[0,1]$ είναι αριθμήσιμο και έστω $x_1, x_2, \ldots, x_n, \ldots$ μια αρίθμηση των στοιχείων του. Χρησιμοποιώντας τη δεκαδική μορφή των x_i έχουμε,

$$\begin{aligned} x_1 &= 0, a_1^1 a_2^1 a_3^1 \cdots a_n^1 \cdots \\ x_2 &= 0, a_1^2 a_2^2 a_3^2 \cdots a_n^2 \cdots \\ &\vdots \\ x_n &= 0, a_1^n a_2^n a_3^n \cdots a_n^n \cdots \\ &\vdots \end{aligned}$$

όπου $a_i^j \in \{0, 1, \ldots, 9\}$ για κάθε $i, j \in \mathbb{N}^*$.

Αν επιλεγεί μια ακολουθία (β_n) με $(\beta_n) \in \{1, \ldots, 8\}$ και $\beta_n \neq a_n^n$, τότε ο αριθμός

$$x = 0, \beta_1 \beta_2 \cdots \beta_n \cdots$$

ενώ ανήκει στο $[0,1]$ είναι διαφορετικός από όλα τα x_n, $n \in \mathbb{N}^*$, το οποίο είναι άτοπο. □

(ii) *Κάθε διάστημα είναι υπεραριθμήσιμο.*

Απόδειξη. Προκύπτει άμεσα από το γεγονός ότι $[\alpha, \beta] \sim [0,1]$. (Βλέπε άλυτη άσκηση 44)). □

(iii) *Το σύνολο* $\mathbb{R}$ *των πραγματικών αριθμών είναι υπεραριθμήσιμο.*

Απόδειξη. Προκύπτει άμεσα από το γεγονός ότι $[0,1] \subseteq \mathbb{R}$. □

1.5 Λυμένες ασκήσεις

Άσκηση 1.1 (Ταυτότητες συνόλων). *Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να δειχθεί ότι*

i) $A \setminus B = A \cap \overline{B}$. *(Τύπος διαφοράς συνόλων.)*

ii) $\overline{A \cup B} = \overline{A} \cap \overline{B}$. *(Κανόνας Δε Μοργαν για το συμπλήρωμα της ένωσης.)*

iii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. *(Επιμεριστική ιδιότητα της τομής ως προς την ένωση.)*

iv) $A = (A \cap B) \cup (A \cap \overline{B})$. *(Διαμέριση του A ως προς την τομή του με τα B και $\overline{B}$.)*

v) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$. *(Επιμεριστική ιδιότητα της τομής ως προς την διαφορά.)*

Λύση της (i) με τη χρήση ισοδυναμιών. Θέλουμε να δείξουμε ότι $A \setminus B = A \cap \overline{B}$.

Για κάθε $x \in A \setminus B$ ισχύει ότι

$$\begin{aligned} x \in A \setminus B &\Leftrightarrow x \in A \text{ και } x \notin B \\ &\Leftrightarrow x \in A \text{ και } x \in \overline{B} \\ &\Leftrightarrow x \in A \cap \overline{B}, \end{aligned}$$

οπότε, επειδή χρησιμοποιήθηκαν παντού ισοδυναμίες,

$$A \setminus B = A \cap \overline{B}.$$ □

Λύση της (ii) με τη χρήση ισοδυναμιών. Θέλουμε να δείξουμε ότι $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

$$\begin{aligned} x \in \overline{A \cup B} &\Leftrightarrow x \notin A \cup B \\ &\Leftrightarrow x \notin A \text{ και } x \notin B \\ &\Leftrightarrow x \in \overline{A} \text{ και } x \in \overline{B} \\ &\Leftrightarrow x \in \overline{A} \cap \overline{B} \end{aligned}$$

οπότε, επειδή χρησιμοποιήθηκαν παντού ισοδυναμίες,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$ □

Λύση της (iii) με τη χρήση πινάκων. Θέλουμε να δείξουμε ότι $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Τα A, B, C είναι υποσύνολα του E.

Πού μπορεί να ανήκει κάποιο στοιχείο $x \in E$·

Σημειώνουμε 1 αν το x ανήκει στο σύνολο και 0 αλλιώς.

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Οι στήλες $A \cap (B \cup C)$ και $(A \cap B) \cup (A \cap C)$ είναι ίδιες. Άρα, τα σύνολα αυτά έχουν τα ίδια στοιχεία του E, δηλαδή είναι ίσα. □

Παρατήρηση Αν σε ένα τύπο εμφανίζονται:
2 διαφορετικά σύνολα, ο πίνακας έχει $2^2 = 4$ γραμμές (περιπτώσεις),
3 διαφορετικά σύνολα, ο πίνακας έχει $2^3 = 8$ γραμμές (περιπτώσεις),
n διαφορετικά σύνολα, ο πίνακας έχει 2^n γραμμές (περιπτώσεις).
Η μέθοδος των πινάκων είναι πρακτική όταν σε ένα τύπο εμφανίζονται το πολύ 4 διαφορετικά σύνολα.

Λύση της (iv) με τη χρήση πινάκων. Θέλουμε να δείξουμε ότι $A = (A \cap B) \cup (A \cap \overline{B})$.

A	B	$\overline{B}$	$A \cap B$	$A \cap \overline{B}$	$(A \cap B) \cup (A \cap \overline{B})$
1	1	0	1	0	1
1	0	1	0	1	1
0	1	0	0	0	0
0	0	1	0	0	0

Οι στήλες των A και $(A \cap B) \cup (A \cap \overline{B})$ είναι ίδιες.
Άρα, τα σύνολα A και $(A \cap B) \cup (A \cap \overline{B})$ περιέχουν τα ίδια στοιχεία του E, δηλαδή είναι ίσα. □

Λύση της (v) με τη χρήση ιδιοτήτων. Θέλουμε να δείξουμε ότι $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.
Χρησιμοποιώντας τις βασικές ιδιότητες των πράξεων συνόλων, έχουμε τις επόμενες ισότητες:

$$\begin{aligned}
(A \cap B) \setminus (A \cap C) &= (A \cap B) \cap (\overline{A \cap C}) \\
&= (A \cap B) \cap (\overline{A} \cup \overline{C}) \\
&= ((A \cap B) \cap \overline{A}) \cup ((A \cap B) \cap \overline{C}) \\
&= \varnothing \cup (A \cap B \cap \overline{C}) \\
&= A \cap (B \cap \overline{C}) \\
&= A \cap (B \setminus C).
\end{aligned}$$

□

Λύση της (v) με τη μέθοδο διπλού εγκλεισμού. Για να δείξουμε ότι δύο σύνολα A, B είναι ίσα, αρκεί να δείξουμε ότι $A \subseteq B$ και $B \subseteq A$.
Θέλουμε να δείξουμε ότι $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.
Έστω $x \in A \cap (B \setminus C)$. Τότε,

$$\begin{aligned}
x \in A \cap (B \setminus C) &\Leftrightarrow x \in A \text{ και } x \in B \setminus C \\
&\Leftrightarrow x \in A \text{ και } x \in B \text{ και } x \notin C \\
&\Leftrightarrow x \in A \cap B \text{ και } x \notin C \\
&\overset{4}{\Rightarrow} x \in A \cap B \text{ και } x \notin A \cap C \\
&\Rightarrow x \in (A \cap B) \setminus (A \cap C).
\end{aligned}$$

Άρα, $A \cap (B \setminus C) \subseteq (A \cap B) \setminus (A \cap C)$.

[4] Αν $x \notin C$, τότε $x \notin A \cap C$. (Το αντίστροφο, γενικά, δεν ισχύει.)

Έστω $x \in (A \cap B) \setminus (A \cap C)$. Τότε

$$\begin{aligned} x \in (A \cap B) \setminus (A \cap C) &\Leftrightarrow x \in A \cap B \text{ και } x \notin A \cap C \\ &\Leftrightarrow x \in B \text{ και } x \in A \text{ και } x \notin A \cap C \\ &\overset{5}{\Rightarrow} x \in B \text{ και } x \in A \text{ και } x \notin C \\ &\Leftrightarrow x \in A \text{ και } x \in B \text{ και } x \notin C \\ &\Leftrightarrow x \in A \text{ και } x \in B \setminus C \\ &\Leftrightarrow x \in A \cap (B \setminus C) \end{aligned}$$

Άρα, $(A \cap B) \setminus (A \cap C) \subseteq A \cap (B \setminus C)$.

Επομένως,

$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C). \qquad \square$$

Άσκηση 1.2 (Δυναμοσύνολο τομής συνόλων). *Έστω A, B μη κενά σύνολα. Να δειχθεί ότι $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.*

Λύση. Για κάθε $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ ισχύει ότι

$$\begin{aligned} X \in \mathcal{P}(A) \cap \mathcal{P}(B) &\Leftrightarrow \\ X \in \mathcal{P}(A) \text{ και } X \in \mathcal{P}(B) &\Leftrightarrow \\ X \subseteq A \text{ και } X \subseteq B &\Leftrightarrow \\ X \subseteq A \cap B &\Leftrightarrow \\ X \in \mathcal{P}(A \cap B), & \end{aligned}$$

οπότε, επειδή χρησιμοποιήθηκαν παντού ισοδυναμίες

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B). \qquad \square$$

Άσκηση 1.3 (Δυναμοσύνολο ένωσης συνόλων). *Έστω A, B μη κενά σύνολα. Να εξετασθεί αν ισχύει η ισότητα $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$.*

Λύση. Θα δείξουμε ότι η ισότητα αυτή δεν ισχύει πάντα, με ένα αντιπαράδειγμα. Θεωρούμε τα σύνολα $A = \{1\}$ και $B = \{2\}$, οπότε

$$\mathcal{P}(A) = \{\emptyset, \{1\}\} \qquad \text{και} \qquad \mathcal{P}(B) = \{\emptyset, \{2\}\}.$$

Επομένως, είναι $\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}\}$.

Επιπλέον, είναι $A \cup B = \{1, 2\}$, οπότε

$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\},$$

δηλαδή, $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$. $\square$

[5] Αν $x \in A$ και $x \notin A \cap C$, τότε $x \in A$ και $x \notin C$.

Άσκηση 1.4 (Ταυτότητες συνόλων). *Έστω E ένα μη κενό σύνολο και $A, B \subseteq E$. Να δειχθεί ότι*

i) $A \triangle B = (A \cap \overline{B}) \cup (B \cap \overline{A})$.

ii) $A \setminus B = \emptyset \Leftrightarrow A \subseteq B$.

iii) $A \cup B = \emptyset \Leftrightarrow A = B = \emptyset$.

iv) $A = B \Leftrightarrow A \triangle B = \emptyset$.

Λύση. i) Ισχύει ότι

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cap \overline{B}) \cup (B \cap \overline{A}).$$

ii) Αν $A \subseteq B$ τότε

$$x \in A \setminus B \Leftrightarrow x \in A \text{ και } x \notin B$$

Αλλά, επειδή $A \subseteq B$, αν $x \in A$ τότε $x \in B$ οπότε

$$x \in A \setminus B \Leftrightarrow x \in B \text{ και } x \notin B$$

Άρα, το σύνολο $A \setminus B$ είναι κενό.

Αντίστροφα, έστω $A \setminus B = \emptyset$.

Αν $A \not\subseteq B$ τότε υπάρχει $x \in A$ ώστε $x \notin B$, τότε όμως $x \in A \setminus B$, το οποίο είναι άτοπο. Άρα, $A \subseteq B$.

iii) Αν $A \neq \emptyset$ (αντ. $B \neq \emptyset$ τότε $A \cup B \neq \emptyset$. Άρα, $A = B = \emptyset$.

iv) Έστω $A = B$, τότε

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = \emptyset \cup \emptyset = \emptyset.$$

Αντίστροφα, έστω $A \triangle B = \emptyset$, τότε

$$\begin{aligned} A \triangle B = \emptyset &\Leftrightarrow \\ (A \setminus B) \cup (B \setminus A) = \emptyset &\Leftrightarrow \\ A \setminus B = \emptyset \text{ και } B \setminus A = \emptyset &\Leftrightarrow \\ A \subseteq B \text{ και } B \subseteq A &\Leftrightarrow \\ A = B. & \end{aligned}$$

□

Άσκηση 1.5 (Εξισώσεις συνόλων). *Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να λυθούν οι παρακάτω εξισώσεις, όπου X, Y είναι τα άγνωστα σύνολα.*

i) $A \cap X = X$.

ii) $A \cup X = X$.

iii) $A \cap X = A \cup X$.

iv) $A \cap X = \emptyset$.

v) $(A \cap X) \cup (B \cap \overline{X}) = \emptyset$.

vi) $A \setminus X = B$.

Λύση. Στις εξισώσεις συνόλων συνήθως η λύση περιγράφεται με τη μορφή εγκλεισμών. Για την επίλυσή τους είναι χρήσιμες οι παρακάτω ιδιότητες:

Έστω P, Q δύο σύνολα τότε ισχύουν οι παρακάτω σχέσεις εγκλεισμού

$$P \cap Q \subseteq P \subseteq P \cup Q.$$

Επίσης, ισχύει η παρακάτω συνεπαγωγή

$$P \subseteq Q \subseteq P \Rightarrow P = Q.$$

Επιπλέον, ισχύουν οι παρακάτω ιδιότητες:

$$P = Q \Leftrightarrow P \triangle Q = \emptyset.$$

$$P \triangle Q = (A \cap \overline{B}) \cup (B \cap \overline{A}).$$

$$P \cup Q = \emptyset \Leftrightarrow P = Q = \emptyset.$$

i) (1ος τρόπος) Για κάθε σύνολο X ισχύει ότι $A \cap X \subseteq A$. Αντικαθιστώντας την έκφραση $A \cap X$ με X έχουμε ότι

$$A \cap X \subseteq A \Leftrightarrow X \subseteq A.$$

Άρα, η λύση της εξίσωσης είναι κάθε X που είναι υποσύνολο του A.

(2ος τρόπος) Ισχύει ότι

$$\begin{aligned}
A \cap X = X \Leftrightarrow \\
(A \cap X) \triangle X = \emptyset \Leftrightarrow \\
((A \cap X) \cap \overline{X}) \cup (X \cap \overline{(A \cap X)}) = \emptyset \Leftrightarrow \\
(A \cap X) \cap \overline{X} = \emptyset \text{ και } (X \cap \overline{(A \cap X)} = \emptyset \Leftrightarrow \\
\emptyset = \emptyset \text{ και } (X \cap (\overline{A} \cup \overline{X}) = \emptyset \Leftrightarrow \\
(X \cap \overline{A}) \cup (X \cap \overline{X}) = \emptyset \Leftrightarrow \\
X \cap \overline{A} = \emptyset \Leftrightarrow \\
X \setminus A = \emptyset \Leftrightarrow \\
X \subseteq A.
\end{aligned}$$

Άρα, η λύση της εξίσωσης είναι κάθε X που είναι υποσύνολο του A.

ii) Για κάθε σύνολο X ισχύει ότι $A \subseteq A \cup X$. Αντικαθιστώντας την έκφραση $A \cup X$ με X έχουμε ότι

$$A \subseteq A \cup X \Leftrightarrow A \subseteq X.$$

Άρα, η λύση της εξίσωσης είναι κάθε X που είναι υπερσύνολο του A.

iii) (1ος τρόπος) Ισχύει ότι

$$A \cap X \subseteq X \subseteq A \cup X = A \cap X.$$

Άρα, παντού ισχύει η ισότητα, δηλαδή

$$A \cap X = X = A \cup X.$$

Άρα, το X είναι υποσύνολο και υπερσύνολο του A, δηλαδή $X = A$.

(2ος τρόπος) Ισχύει ότι

$$\begin{aligned}
A \cap X = A \cup X \Leftrightarrow \\
(A \cap X) \triangle (A \cup X) = \emptyset \Leftrightarrow \\
((A \cap X) \cap \overline{(A \cup X)}) \cup ((A \cup X) \cap \overline{(A \cap X)}) = \emptyset \Leftrightarrow \\
((A \cap X) \cap \overline{A} \cap \overline{X}) \cup ((A \cup X) \cap (\overline{A} \cup \overline{X})) = \emptyset \Leftrightarrow \\
\emptyset \cup (A \cap (\overline{A} \cup \overline{X})) \cup (X \cap (\overline{A} \cup \overline{X})) = \emptyset \Leftrightarrow \\
(A \cap \overline{X}) \cup (X \cap \overline{A}) = \emptyset \Leftrightarrow \\
(A \setminus X) \cup (X \setminus A) = \emptyset \Leftrightarrow \\
A \setminus X = \emptyset \text{ και } X \setminus A = \emptyset \Leftrightarrow \\
A \subseteq X \text{ και } X \subseteq A \Leftrightarrow \\
X = A.
\end{aligned}$$

iv) Αφού $A \cap X = \emptyset$, έπεται ότι $X \subseteq \overline{A}$ και αντιστρόφως. Άρα, η λύση της εξίσωσης είναι κάθε υποσύνολο X του $\overline{A}$.

v) Η εξίσωση $(A \cap X) \cup (B \cap \overline{X}) = \emptyset$ είναι ισοδύναμη με τις εξισώσεις $A \cap X = \emptyset$ και $B \cap \overline{X} = \emptyset$. Από την εξίσωση $A \cap X$ έπεται ότι $X \subseteq \overline{A}$ και από την εξίσωση $B \cap \overline{X} = \emptyset$ έπεται ότι $B \subseteq \overline{\overline{X}} = X$, δηλαδή

$$B \subseteq X \subseteq \overline{A}.$$

Επομένως, η εξίσωση έχει λύση αν και μόνο αν $B \subseteq \overline{A}$.

vi) Ισχύει ότι

$$\begin{aligned}
A \setminus X = B \Leftrightarrow \\
(A \setminus X) \triangle B = \emptyset \\
((A \setminus X) \cap \overline{B}) \cup (B \cap \overline{(A \setminus X)}) = \emptyset \\
(A \cap \overline{X} \cap \overline{B}) = \emptyset \text{ και } (B \cap \overline{(A \cap \overline{X})}) = \emptyset \\
(A \cap \overline{B}) \cap \overline{X} = \emptyset \text{ και } B \cap (\overline{A} \cup X) = \emptyset \\
(A \cap \overline{B}) \setminus X = \emptyset \text{ και } (B \cap \overline{A}) \cup (B \cap X) = \emptyset \\
A \cap \overline{B} \subseteq X \text{ και } (B \setminus A) = \emptyset \text{ και } (X \setminus \overline{B}) = \emptyset \\
A \cap \overline{B} \subseteq X \text{ και } B \subseteq A \text{ και } X \subseteq \overline{B} \\
A \cap \overline{B} \subseteq X \subseteq \overline{B} \text{ και } \overline{A} \subseteq \overline{B}
\end{aligned}$$

Επομένως, η εξίσωση έχει λύση αν και μόνο αν $\overline{A} \subseteq \overline{B}$ και οι λύσεις της είναι όλα τα X για τα οποία $A \cap \overline{B} \subseteq X \subseteq \overline{B}$ □

Άσκηση 1.6 (Σωστό ή λάθος). *Να εξετασθεί αν κάθε μια από τις παρακάτω προτάσεις είναι σωστή ή λάθος:*

1. $|A \cup B| = |A| + |B|$.

   Λάθος. Ισχύει μόνο όταν $A \cap B = \varnothing$. Για παράδειγμα, $A = \{1, 2\}$ και $B = \{2, 3\}$, τότε το πρώτο μέλος ισούται με 3 ενώ το δεύτερο με 4.

2. $|A \triangle B| = |A \setminus B| + |B \setminus A|$.

   Σωστό. Είναι $A \triangle B = A \setminus B \cup B \setminus A$ και τα σύνολα $A \setminus B$ και $B \setminus A$ είναι ξένα.

3. $|\{\{\varnothing, \{\varnothing, \{\varnothing\}\}\}, \varnothing, \{\varnothing, \{\varnothing\}\}\}| = 6$.

   Λάθος. Το σύνολο περιέχει 3 στοιχεία, τα $\{\varnothing, \{\varnothing, \{\varnothing\}\}\}$, $\varnothing$ και $\{\varnothing, \{\varnothing\}\}$.

Άσκηση 1.7 (Σωστό ή λάθος). *Να εξετασθεί αν κάθε μια από τις παρακάτω προτάσεις είναι σωστή ή λάθος:*

1. *Αν $|A| = 5$, $|B| = 7$ και $|A \cup B| = 12$, τα σύνολα A, B είναι ξένα.*

   Σωστό. Είναι $|A \cap B| = |A| + |B| - |A \cup B| = 5 + 7 - 12 = 0$.

2. $|[n + 2]| = |[n]| + 2$.

   Σωστό. Είναι $[n] = \{1, 2, \ldots, n\}$, οπότε $|[n]| = n$ και $|[n + 2]| = n + 2$.

Άσκηση 1.8 (Εξισώσεις πληθαρίθμων). *Για δύο σύνολα A, B δίνονται*

$$|B| = 6, \quad |B \setminus A| = 4 \quad \textit{και} \quad |A \cup B| = 11.$$

Να υπολογισθούν οι πληθάριθμοι $|A|$ και $|A \cap B|$.

Λύση. Είναι

$$|B| = |B \setminus A| + |A \cap B| \Rightarrow |A \cap B| = |B| - |B \setminus A| = 6 - 4 = 2.$$

και

$$11 = |A \cup B| = |A| + |B| - |A \cap B| = |A| + 6 - 2,$$

επομένως, $|A| = 11 - 4 = 7$. □

Άσκηση 1.9 (Παράδειγμα σχέσης ισοδυναμίας). *Στο σύνολο $\mathbb{N}$ ορίζουμε μια σχέση R ως εξής:*

$$xRy \Leftrightarrow \textit{ Υπάρχει } k \in Z \textit{ ώστε } y - x = 3k.$$

i) Να δειχθεί ότι η σχέση R είναι σχέση ισοδυναμίας στο $\mathbb{N}$.

ii) Να βρεθεί η κλάση ισοδυναμίας του αριθμού 2.

iii) Να βρεθεί το σύνολο πηλίκο της σχέσης R.

Για παράδειγμα,

$$2R5, \text{ διότι } 5-2=3\cdot 1$$

$$2R8, \text{ διότι } 8-2=3\cdot 2$$

$$8R2, \text{ διότι } 2-8=3\cdot(-2)$$

$$3\not R7, \text{ διότι δεν υπάρχει } k\in\mathbb{Z} \text{ ώστε } 7-3=4=3k.$$

Λύση.

i) Ισχύει η ανακλαστική ιδιότητα. Πράγματι, για κάθε $x\in\mathbb{N}$, ισχύει ότι $x-x=0=3\cdot 0$, άρα ικανοποιείται ο ορισμός με $k=0$, δηλαδή xRx.

Ισχύει η συμμετρική ιδιότητα. Πράγματι, αν $x,y\in\mathbb{N}$ με xRy, τότε υπάρχει $k\in\mathbb{Z}$ ώστε $y-x=3k$. Επομένως, $x-y=3(-k)$, και επειδή, $-k\in\mathbb{Z}$, έπεται ότι yRx.

Ισχύει η μεταβατική ιδιότητα. Πράγματι, αν $x,y,z\in\mathbb{N}$ με xRy και yRz, τότε υπάρχουν $k_1,k_2\in\mathbb{Z}$ ώστε

$$y-x=3k_1 \qquad \text{και} \qquad z-y=3k_2.$$

Προσθέτοντας κατά μέλη προκύπτει ότι $z-x=3(k_1+k_2)$ και επειδή $k_1+k_2\in\mathbb{Z}$, έπεται ότι xRz.

Από τα προηγούμενα προκύπτει ότι η R είναι σχέση ισοδυναμίας.

ii) Η κλάση ισοδυναμίας του 2 είναι εξ ορισμού το σύνολο

$$\begin{aligned} C_2 &= \{x\in\mathbb{N} : 2Rx\} \\ &= \{x\in\mathbb{N} : x-2=3k, k\in\mathbb{Z}\} \\ &= \{3k+2\in\mathbb{N} : k\in\mathbb{Z}\} \\ &= \{3k+2\in\mathbb{N} : k\in\mathbb{N}\} \\ &= \{2,5,8,11,14,\ldots\}. \end{aligned}$$

Παρατηρήστε ότι η κλάση C_5 του 5 ταυτίζεται με την C_2. Πράγματι,

$$\begin{aligned} C_5 &= \{x\in\mathbb{N} : 5Rx\} = \{x\in\mathbb{N} : x-5=3k, k\in\mathbb{Z}\} \\ &= \{x\in\mathbb{N} : x-2=3(k+1), k\in\mathbb{Z}\} = C_2 \end{aligned}$$

Το ίδιο συμβαίνει και για τις κλάσεις των στοιχείων $5,8,11,\ldots$ που ανήκουν στην C_2, δηλαδή $C_2=C_5=C_8=C_{11}=\cdots$.

iii) Το σύνολο C_2 αποτελεί μια κλάση του συνόλου πηλίκου $\mathbb{N}/_R$. Επειδή $C_2\neq\mathbb{N}$, υπάρχουν και άλλες κλάσεις.

Διαλέγουμε ένα στοιχείο που δεν ανήκει στο C_2. Για παράδειγμα, το 1.

$$\begin{aligned} C_1 &= \{x\in\mathbb{N} : 1Rx\} = \{x\in\mathbb{N} : x-1=3k, k\in\mathbb{Z}\} \\ &= \{3k+1\in\mathbb{N} : k\in\mathbb{Z}\} = \{1,4,7,10,13,\ldots\} \end{aligned}$$

Επειδή $C_1 \cup C_2 \neq \mathbb{N}$, υπάρχει και άλλη κλάση στην σχέση R. Διαλέγουμε ένα στοιχείο που δεν ανήκει στο $C_1 \cup C_2$. Για παράδειγμα, το 3.

$$\begin{aligned} C_3 &= \{x \in \mathbb{N} : 3Rx\} = \{x \in \mathbb{N} : x - 3 = 3k, k \in \mathbb{Z}\} \\ &= \{3k + 3 \in \mathbb{N} : k \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, \ldots\} \end{aligned}$$

Επειδή $C_1 \cup C_2 \cup C_3 = \mathbb{N}$, δεν υπάρχουν άλλες κλάσεις, οπότε $\mathbb{N}/_R = \{C_1, C_2, C_3\}$. □

Παρατήρηση Το σύνολο πηλίκο $\mathbb{N}/_R$ της προηγούμενης άσκησης μπορεί να προσδιορισθεί πιο απλά, βάσει των επόμενων παρατηρήσεων:

Ο ορισμός της σχέσης R:

$$xRy \Leftrightarrow y - x = 3k, k \in \mathbb{Z},$$

υπονοεί ότι τα x και y σχετίζονται (μέσω της R) ανν η (απόλυτη) διαφορά τους είναι πολλαπλάσιο του 3. Εφόσον τα x και y είναι φυσικοί, αυτό μπορεί να συμβεί μόνο στις εξής 3 περιπτώσεις:

- $x = 3n$ και $y = 3m$, για κάποια $n, m \in \mathbb{N}$.
- $x = 3n + 1$ και $y = 3m + 1$, για κάποια $n, m \in \mathbb{N}$.
- $x = 3n + 2$ και $y = 3m + 2$, για κάποια $n, m \in \mathbb{N}$.

Οι τρεις αυτές περιπτώσεις αντιστοιχούν στις 3 κλάσεις $C_0 = C_3$, C_1 και C_2, διότι αν τα x και y δεν ανήκουν στην ίδια περίπτωση, τότε δεν σχετίζονται και επιπλέον δεν υπάρχουν άλλες περιπτώσεις για έναν φυσικό αριθμό.

Άσκηση 1.10 (Παράδειγμα σχέσης ισοδυναμίας). *Έστω R μια σχέση στο $\mathbb{Z}$ με $xRy \Leftrightarrow x^2 - y^2 = 5k$ για κάποιο $k \in \mathbb{Z}$. Να δειχθεί ότι η σχέση R είναι σχέση ισοδυναμίας.*

Λύση. Για κάθε $a \in \mathbb{Z}$ ισχύει $a^2 - a^2 = 0 = 5 \cdot 0$, όπου $0 \in \mathbb{Z}$, άρα aRa, δηλαδή η R είναι ανακλαστική.

Έστω $a, b \in \mathbb{Z}$ με aRb. Τότε υπάρχει $k \in \mathbb{Z}$ ώστε $a^2 - b^2 = 5k$, οπότε $b^2 - a^2 = 5(-k)$, όπου $-k \in \mathbb{Z}$, άρα bRa, δηλαδή η σχέση R είναι συμμετρική.

Έστω $a, b, c \in \mathbb{Z}$ με aRb και bRc. Τότε υπάρχουν $k_1, k_2 \in \mathbb{Z}$ με $a^2 - b^2 = 5k_1$ και $b^2 - c^2 = 5k_2$. Προσθέτοντας κατά μέλη προκύπτει ότι $a^2 - c^2 = 5(k_1 + k_2)$, όπου $k_1 + k_2 \in \mathbb{Z}$, άρα aRc, δηλαδή η σχέση R είναι μεταβατική.

Επομένως, η σχέση R είναι σχέση ισοδυναμίας στο $\mathbb{Z}$. □

Άσκηση 1.11 (Μερική διάταξη διαιρετότητας). *Στο σύνολο $\mathbb{N}^*$, ορίζουμε την σχέση διαιρετότητας $|$ ως εξής*

$$\begin{aligned} x \mid y &\Leftrightarrow x \text{ διαιρεί τον } y \\ &\Leftrightarrow \text{υπάρχει } k \in \mathbb{N}^* \text{ ώστε } y = kx. \end{aligned}$$

i) Να δειχθεί ότι η σχέση διαιρετότητας $|$ είναι σχέση μερικής διάταξης στο $\mathbb{N}^*$.

ii) Είναι η σχέση διαιρετότητας $|$ σχέση ολικής διάταξης στο $\mathbb{N}^*$;

Λύση.

i) (Ανακλαστική ιδιότητα.) Για κάθε $x \in \mathbb{N}^*$ ισχύει ότι $x = 1 \cdot x$, άρα $x \mid x$.

(Αντισυμμετρική ιδιότητα.) Θεωρούμε $x, y \in \mathbb{N}^*$ με $x \mid y$ και $y \mid x$. Τότε, υπάρχουν $k_1, k_2 \in \mathbb{N}^*$ ώστε $y = k_1 x$ και $x = k_2 y$, οπότε $y = k_1 k_2 y$ και

$$y = k_1 k_2 y \Rightarrow k_1 k_2 = 1 \Rightarrow k_1 = k_2 = 1 \Rightarrow x = y.$$

(Μεταβατική ιδιότητα.) Θεωρούμε $x, y, z \in \mathbb{N}^*$ με $x \mid y$ και $y \mid z$. Τότε, υπάρχουν $k_1, k_2 \in \mathbb{N}^*$ ώστε $y = k_1 x$ και $z = k_2 y$, οπότε $z = k_2 k_1 x$. Επειδή $k_2 k_1 \in \mathbb{N}^*$ έπεται ότι $x \mid z$.

Κατόπιν τούτων, η σχέση $\mid$ είναι σχέση μερικής διάταξης στο $\mathbb{N}^*$.

ii) Δεν είναι ολική διάταξη στο $\mathbb{N}^*$, διότι υπάρχουν αριθμοί στο $\mathbb{N}^*$ που δεν συγκρίνονται. Για παράδειγμα,

$$3 \nmid 5 \text{ και } 5 \nmid 3.$$ □

Διάγραμμα Hasse Τα διαγράμματα Hasse αναπαριστούν γεωμετρικά μια μερική διάταξη $\leq$ που ορίζεται σε ένα σύνολο A.

- Τα στοιχεία του A αναπαρίστανται από σημεία.
- Αν $x < y$ και δεν υπάρχει $z \in A$ ώστε $x < z < y$, τότε τα σημεία x και y ενώνονται με μια γραμμή, έτσι ώστε το σημείο x να βρίσκεται χαμηλότερα από το σημείο y.

Άσκηση 1.12. *Έστω A το σύνολο των θετικών διαιρετών του 24, δηλαδή*

$$A = \{1, 2, 3, 4, 6, 8, 12, 24\},$$

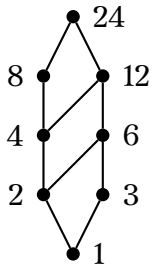
εφοδιασμένο με την σχέση διαιρετότητας $\mid$.

i) Να σχεδιασθεί το διάγραμμα Hασσε του $(A, \mid)$

ii) Να βρεθούν τα $\inf A$ και $\sup A$.

iii) Να βρεθούν τα $\sup B$ και $\inf B$, όπου $B = \{2, 4, 6\}$.

Λύση. i) Ένα διάγραμμα Hασσε για το $A = \{1, 2, 3, 4, 6, 8, 12, 24\}$ είναι το επόμενο



ii) Για το supremum του A, ψάχνουμε φυσικό αριθμό x ώστε

$$1 \mid x, \qquad 2 \mid x, \qquad 3 \mid x, \qquad \ldots, \qquad 24 \mid x$$

και το x να είναι το ελάχιστο δυνατό. Επομένως,

$$\sup A = \text{εκπ των στοιχείων του } A = 24.$$

Ανάλογα, βρίσκουμε ότι

$$\inf A = \text{μκδ των στοιχείων του } A = 1.$$

Παρατηρήστε ότι από το διάγραμμα Hasse, εντοπίζουμε άμεσα το μέγιστο και το ελάχιστο στοιχείο του A, τα οποία είναι τα 24 και 1 αντίστοιχα, οπότε έχουμε ότι

$$\sup A = \max A = 24 \qquad \text{και} \qquad \inf A = \min A = 1.$$

iii) Ψάχνουμε τα supremum και infimum του συνόλου $B = \{2, 4, 6\}$.

Το $\sup B$ θα πρέπει να είναι ένα στοιχείο του $\mathbb{N}^*$ (όχι απαραίτητα στο A) που να είναι άνω φράγμα για τα $2, 4, 6$, δηλαδή να είναι πολλαπλάσιο αυτών, και μάλιστα να είναι το ελάχιστο δυνατό, άρα

$$\sup B = \text{εκπ των } 2, 4, 6 = 12.$$

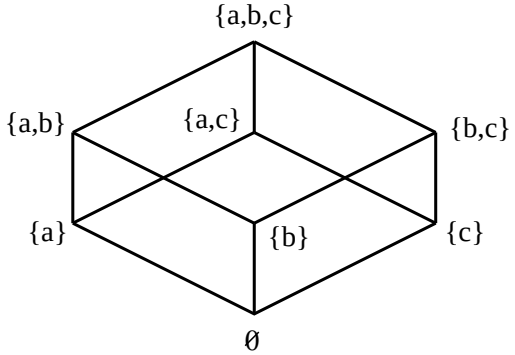
Ομοίως, το $\inf A$ θα πρέπει να διαιρεί τα $2, 4, 6$ και να είναι το μέγιστο δυνατό, οπότε

$$\inf B = \text{μκδ των } 2, 4, 6 = 2.$$

□

Άσκηση 1.13 (Διάγραμμα Hasse του δυναμοσυνόλου). *Να σχεδιασθεί το διάγραμμα Hasse του δυναμοσυνόλου του $A = \{a, b, c\}$ ως προς τη μερική διάταξη του εγκλεισμού $\subseteq$.*

Λύση.



□

Άσκηση 1.14 (Μερική διάταξη από ύψωση σε δύναμη). *Έστω R μια σχέση στο $\mathbb{N}$ με $xRy \Leftrightarrow x = y^k$ για κάποιο $k \in \mathbb{N}^*$. Να δειχθεί ότι η σχέση R είναι σχέση μερικής διάταξης. Είναι η R σχέση ολικής διάταξης;*

Λύση. Για κάθε $a \in \mathbb{N}$ ισχύει ότι $a = a^1$, όπου $1 \in \mathbb{N}^*$, άρα aRa, δηλαδή η σχέση R είναι ανακλαστική.

Έστω $a, b \in \mathbb{N}$ με aRb και bRa. Τότε υπάρχουν $k_1, k_2 \in \mathbb{N}^*$ ώστε $a = b^{k_1}$ και $b = a^{k_2}$. Αντικαθιστώντας το b έχουμε ότι $a = a^{k_1 k_2}$. Επομένως, $k_1 k_2 = 1$, οπότε $k_1 = k_2 = 1$, άρα $a = b$. Δηλαδή, η σχέση R είναι αντισυμμετρική.

Έστω $a, b \in \mathbb{N}$ με aRb και bRc. Τότε υπάρχουν $k_1, k_2 \in \mathbb{N}^*$ ώστε $a = b^{k_1}$ και $b = c^{k_2}$. Αντικαθιστώντας το b προκύπτει ότι $a = c^{k_1 k_2}$, όπου $k_1 k_2 \in \mathbb{N}^*$, άρα aRc, δηλαδή η σχέση R είναι μεταβατική.

Επομένως, η σχέση R είναι σχέση μερικής διάταξης.

Η σχέση R δεν είναι σχέση ολικής διάταξης διότι ούτε $2R3$, ούτε $3R2$. □

Άσκηση 1.15 (Κυκλικές σχέσεις). *Μια σχέση R σε ένα σύνολο A, ονομάζεται **κυκλική** αν για κάθε $a, b, c \in A$ με aRb και bRc έπεται ότι cRa.*

Να δειχθεί ότι μια σχέση R είναι σχέση ισοδυναμίας αν και μόνο αν είναι ανακλαστική και κυκλική.

Λύση. Έστω ότι η σχέση R είναι σχέση ισοδυναμίας. Θα δείξουμε ότι είναι ανακλαστική και κυκλική.

Η R είναι ανακλαστική (αφού είναι σχέση ισοδυναμίας).

Θα δείξουμε ότι η R είναι και κυκλική.

Πράγματι, έστω $a, b, c \in A$ με aRb και bRc. Επειδή η R είναι συμμετρική έπεται ότι bRa και cRb. Επειδή η R είναι μεταβατική έπεται ότι cRa. Άρα, η σχέση R είναι κυκλική.

Αντίστροφα, έστω ότι η σχέση R είναι ανακλαστική και κυκλική. Θα δείξουμε ότι η R είναι σχέση ισοδυναμίας.

Αρκεί να δείξουμε ότι είναι συμμετρική και μεταβατική.

Πράγματι, έστω $a, b \in R$ με aRb. Επειδή η R είναι ανακλαστική έπεται ότι bRb. Επειδή η R είναι κυκλική έπεται ότι bRa. Άρα, η R είναι συμμετρική.

Έστω $a, b, c \in R$ με aRb και bRc. Επειδή η R είναι κυκλική έπεται ότι cRa. Επειδή (όπως αποδείξαμε) η R είναι συμμετρική έπεται ότι aRc. Άρα, η R είναι μεταβατική. Άρα, η σχέση R είναι σχέση ισοδυναμίας. □

Τοπολογική διάταξη Δίδεται ένα σύνολο V, στο οποίο έχουμε ορίσει μια μερική διάταξη $\leq$. Μια ολική διάταξη $\lhd$ στο V ονομάζεται **γραμμική επέκταση** ή **τοπολογική διάταξη** της διάταξης $\leq$ στο V ανν για κάθε $a, b \in V$ ισχύει

$$a \leq b \Rightarrow a \lhd b.$$

Δηλαδή η διάταξη $\lhd$ είναι 'συμβατή' με την $\leq$ και την επεκτείνει σε όλα τα ζεύγη στοιχείων.

Για παράδειγμα, ας υποθέσουμε ότι δίνεται το σύνολο $V = \{a, b, c, d, e, f\}$ με την μερική διάταξη $\leq$, για την οποία $x \leq x$ για κάθε $x \in V$ και επιπλέον

$$d \leq b,\ d \leq c,\ d \leq a,\ d \leq e,\ d \leq f,\ b \leq e,\ c \leq e,\ a \leq f$$

Μια τοπολογική διάταξη $\lhd$ για την σχέση $\leq$ είναι η ολική διάταξη

$$d \lhd b \lhd c \lhd a \lhd e \lhd f$$

Μια άλλη τοπολογική διάταξη $\lhd$ είναι η ολική διάταξη

$$d \lhd b \lhd c \lhd e \lhd a \lhd f.$$

Αποδεικνύεται ότι κάθε μερική διάταξη μπορεί να επεκταθεί σε μια τοπολογική διάταξη. Μερικές φορές μπορεί να υπάρχουν πολλές τοπολογικές διατάξεις.

Για την εύρεση της τοπολογικής διάταξης μπορεί να χρησιμοποιηθεί ο επόμενος αλγόριθμος:

Αλγόριθμος εύρεσης τοπολογικής διάταξης

- Είσοδος: Ένα σύνολο U διατεταγμένων ζευγών (x, y) που αναπαριστούν την μερική διάταξη $\leq$ στο σύνολο V
- Έξοδος: Μια (διατεταγμένη) λίστα L των στοιχείων του V, η οποία αναπαριστά την τοπολογική διάταξη $\lhd$.
- Όσο υπάρχουν στοιχεία του V που δεν έχουν προστεθεί στην L
  - Επιλέγουμε ένα στοιχείο $x \in V$ που δεν έχει μικρότερο στοιχείο μεταξύ των στοιχείων που δεν έχουν προστεθεί στην λίστα L (Δηλαδή το x δεν εμφανίζεται στην δεύτερη θέση κανενός ζεύγους του U.)
  - Προσθέτουμε το x στο τέλος της λίστας L.
  - Σβήνουμε όλα τα ζεύγη (x, y) του U που περιέχουν το x.

Το πρόβλημα της επέκτασης μιας μερικής διάταξης σε ολική είναι πολύ συνηθισμένο στις εφαρμογές, όπως φαίνεται και στην επόμενη άσκηση.

Άσκηση 1.16 (Βάζοντας τα πράγματα σε σειρά). *Για την ολοκλήρωση ενός έργου, πρέπει να εκτελεστούν 9 δραστηριότητες $1, 2, \ldots, 9$. Κάποιες από αυτές χρειάζονται τα αποτελέσματα μερικών άλλων, των οποίων η εκτέλεση πρέπει να προηγηθεί. Οι απαιτήσεις κάθε μιας δίδονται στον επόμενο πίνακα:*

	απαιτήσεις		*απαιτήσεις*		*απαιτήσεις*
1	3, 4	4		7	3, 4
2	1, 5	5		8	5, 7
3		6	1, 2	9	6, 8

Να βρεθεί με ποια σειρά πρέπει να εκτελεστούν οι $1, 2, \ldots, 9$ ώστε να ολοκληρωθεί το έργο.

Λύση. Οι απαιτήσεις του προβλήματος ορίζουν μια μερική διάταξη στο σύνολο 1, 2, ..., 9. Συγκεκριμένα, $j < i$ αν η δραστηριότητα i απαιτεί την ολοκλήρωση της δραστηριότητας j. Επομένως, η ολοκλήρωση του έργου απαιτεί την ικανοποίηση των παρακάτω ζευγών περιορισμών:

$$U = \{(1,2), (1,6), (2,6), (3,1), (3,7), (3,8),\\ (4,1), (4,7), (5,2), (5,8), (6,9), (8,9)\}$$

Η εύρεση της σειράς εκτέλεσης αντιστοιχεί στην εύρεση μια τοπολογικής διάταξης για την μερική διάταξη των απαιτήσεων.

Θα εφαρμόσουμε τον αλγόριθμο της τοπολογικής διάταξης. Θα φτιάξουμε μια λίστα L που τελικά θα περιέχει τους αριθμούς $1, 2, 3, \ldots, 9$ με την σειρά της τοπολογικής διάταξης. Κάθε φορά, επιλέγουμε μια δραστηριότητα i που δεν απαιτεί τις υπόλοιπες που απομένουν, την προσθέτουμε στο τέλος της L και σβήνουμε από το U τα ζεύγη που την περιέχουν. Επαναλαμβάνουμε μέχρι να εξαντληθούν οι δραστηριότητες.

0. Αρχικά, έχουμε $V = [1, 2, 3, 4, 5, 6, 7, 8, 9]$, $L = []$ και

$$U = \{(1, 2), (1, 6), (2, 6), (3, 1), (3, 7), (3, 8), (4, 1), (4, 7), (5, 2), (5, 8), (6, 9), (8, 9)\}$$

1. Επιλέγουμε την 5 οπότε έχουμε $V = [1, 2, 3, 4, 6, 7, 8, 9]$, $L = [5]$ και

$$U = \{(1, 2), (1, 6), (2, 6), (3, 1), (3, 7), (3, 8), (4, 1), (4, 7), (6, 9), (8, 9)\}$$

2. Επιλέγουμε την 3 οπότε έχουμε $V = [1, 2, 4, 6, 7, 8, 9]$, $L = [5, 3]$ και

$$U = \{(1, 2), (1, 6), (2, 6), (4, 1), (4, 7), (6, 9), (8, 9)\}$$

3. Επιλέγουμε την 4 οπότε έχουμε $V = [1, 2, 6, 7, 8, 9]$, $L = [5, 3, 4]$ και

$$U = \{(1, 2), (1, 6), (2, 6), (6, 9), (8, 9)\}$$

4. Επιλέγουμε την 1 οπότε έχουμε $V = [2, 6, 7, 8, 9]$, $L = [5, 3, 4, 1]$ και

$$U = \{(2, 6), (6, 9), (8, 9)\}$$

5. Επιλέγουμε την 7 οπότε έχουμε $V = [2, 6, 8, 9]$, $L = [5, 3, 4, 1, 7]$ και

$$U = \{(2, 6), (6, 9), (8, 9)\}$$

6. Επιλέγουμε την 8 οπότε έχουμε $V = [2, 6, 9]$, $L = [5, 3, 4, 1, 7, 8]$ και

$$U = \{(2, 6), (6, 9)\}$$

7. Επιλέγουμε την 2 οπότε έχουμε $V = [6, 9]$, $L = [5, 3, 4, 1, 7, 8, 2]$ και

$$U = \{(6, 9)\}$$

8. Επιλέγουμε την 6 οπότε έχουμε: $V = [9]$, $L = [5, 3, 4, 1, 7, 8, 2, 6]$ και

$$U = \{\}$$

9. Επιλέγουμε την 9 οπότε έχουμε $V = []$, $L = [5, 3, 4, 1, 7, 8, 2, 6, 9]$ και

$$U = \{\}$$

Επομένως, μια τοπολογική διάταξη των δραστηριοτήτων 1, 2, ..., 9, και άρα μια πιθανή σειρά εκτέλεσης των δραστηριοτήτων, είναι η σειρά $L = [5, 3, 4, 1, 7, 8, 2, 6, 9]$.

Παρακάτω δίδεται μια υλοποίηση του παραπάνω αλγορίθμου στην γλώσσα Python

```
V = [1,2,3,4,5,6,7,8,9] #elements
U = [(1,2),(1,6),(2,6),(3,1),(3,7),(4,1),(4,7),(5,2),(5,8),(6,9),(3,8),(8,9)] #
    partial order
Vc = V.copy()
n = len(V)
pre = [[] for i in range(n+1)] #u in pre[v] <==> (u,v) in U
succ = [[] for i in range(n+1)] #u in succ[v] <==> (v,u) in U
for t in U: #for each tuple t in U
    pre[t[1]].append(t[0]) #populate pre
    succ[t[0]].append(t[1]) #populate succ

L = [] #result is stored in L
while(len(Vc) > 0):
    l = len(Vc)
    for v in Vc: #for each element v
        if len(pre[v]) == 0: #if v has no predecessor
            L.append(v) #append it in L
            for u in succ[v]: #for each successor u of v
                pre[u].remove(v) #delete v from list of predecessors of u
            #succ[v].clear()
            Vc.remove(v) #delete v
            break #reset for v loop
    if l == len(Vc): break #no progress => no possible solution

if (len(Vc)==0): print("result:", L)
else: print("no result found")
```

Output:

```
result: [3, 4, 1, 5, 2, 6, 7, 8, 9]
```

□

Άσκηση 1.17 (Πράξεις σχέσεων). *Έστω* $A = \{1,2\}$, $B = \{2,4,6,8\}$. *Στο σύνολο* $A \times B$ *ορίζονται δύο σχέσεις* R_1, R_2 *όπου*

$$R_1 = \{(1,2),(1,4),(2,4),(2,8)\}$$

$$R_2 = \{(1,2),(2,2),(2,4),(2,6)\}$$

Να βρεθούν οι σχέσεις $R_1 \cup R_2$, $R_1 \cap R_2$, $\overline{R_1}$, $\overline{R_2}$, $R_1 \setminus R_2$, $R_2 \setminus R_1$, R_1^{-1}, R_2^{-1}, $R_2 \circ R_1$, $R_1 \circ R_2$, $\mathrm{proj}_1 R_1$, $\mathrm{proj}_2 R_1$.

Λύση. Ισχύει ότι

$$R_1 \cup R_2 = \{(1,2),(1,4),(2,2),(2,4),(2,6),(2,8)\}, \qquad R_1 \cap R_2 = \{(1,2),(2,4)$$

$$\overline{R_1} = \{(1,8),(1,6),(2,2),(2,6)\}, \qquad \overline{R_2} = \{(1,8),(1,4),(1,6),(2,8)\}$$

$$R_1 \setminus R_2 = \{(1,4),(2,8)\}, \qquad R_2 \setminus R_1 = \{(2,2),(2,6)$$

$$R_1^{-1} = \{(2,1),(4,1),(4,2),(8,2), \qquad R_2^{-1} = \{(2,1),(2,2),(4,2),(6,2)\}$$

$$R_2 \circ R_1 = \{(1,2),(1,4),(1,6)\}, \qquad R_1 \circ R_2 = \{(1,4),(1,8),(2,4),(2,8)\}$$

$$\mathrm{proj}_1 R_1 = \{1,2\}, \qquad \mathrm{proj}_2 R_1 = \{2,4,8\}.$$

□

Άσκηση 1.18 (Συλλογικές κατατάξεις). *Ζητήθηκε από 17 κριτικούς ταινιών να κατατάξουν 4 ταινίες a, b, c, d. Στον επόμενο πίνακα παρουσιάζονται συγκεντρωτικά οι αξιολογήσεις τους.*

Κατάταξη:	*1*	*2*	*3*	*4*
5	*a*	*d*	*c*	*b*
3	*a*	*d*	*b*	*c*
5	*b*	*c*	*d*	*a*
4	*c*	*d*	*b*	*a*
Βαθμοί:	3	2	1	0

Για παράδειγμα, 5 κριτικοί επέλεξαν την ταξινόμηση $a > d > c > b$. Ποια κατά την γνώμη σας είναι η καλύτερη ταινία με βάση τις κατατάξεις των κριτικών·

Λύση. Υπάρχουν αρκετοί τρόποι (κανόνες) να επιλέξουμε την καλύτερη ταινία. Μερικοί από τους πιο δημοφιλείς είναι οι επόμενοι:

Ο κανόνας της σχετικής πλειοψηφίας. Κάθε κριτικός δίνει μια μόνο ψήφο (στην καλύτερη ταινία που επιλέγει). Κερδίζει η ταινία με τον μεγαλύτερο αριθμό ψήφων.

Κατάταξη:	1	2	3	4
5	*a*	*d*	*c*	*b*
3	*a*	*d*	*b*	*c*
5	*b*	*c*	*d*	*a*
4	*c*	*d*	*b*	*a*
Βαθμοί:	3	2	1	0

(Νικήτρια: *a*)

Ο κανόνας της απόλυτης πλειοψηφίας. Κάθε κριτικός δίνει μια μόνο ψήφο (στην καλύτερη ταινία που επιλέγει). Αλλά για να κερδίσει μια ταινία, πρέπει να συγκεντρώσει περισσότερες από τις μισές ψήφους. Αν δεν συμβεί αυτό, διεξάγεται δεύτερος γύρος ψηφοφορίας, στον οποίο συμμετέχουν οι δύο ταινίες που είχαν τις περισσότερες ψήφους. Στο δεύτερο γύρο, νικήτρια είναι εκείνη η ταινία που πλειοψηφεί.

(1ος γύρος)

Κατάταξη:	1	2	3	4
5	*a*	*d*	*c*	*b*
3	*a*	*d*	*b*	*c*
5	*b*	*c*	*d*	*a*
4	*c*	*d*	*b*	*a*

(2ος γύρος)

Κατάταξη:	1	2
5	*a*	*b*
3	*a*	*b*
5	*b*	*a*
4	*b*	*a*

Στον πρώτο γύρο, δεν υπάρχει νικητής. Στον δεύτερο γύρο, περνάνε οι ταινίες *a* και *b*. (Νικήτρια: *b*)

Ο κανόνας της υψηλότερης βαθμολογίας. Κάθε κριτικός παρουσιάζει ολόκληρο το σύστημα προτίμησής του. Μια ταινία παίρνει 0 βαθμούς για την τελευταία θέση, 1 βαθμό για την προτελευταία, 2 βαθμούς για την αμέσως επόμενη, και ούτω καθεξής. Κερδίζει η ταινία που συγκεντρώνει την υψηλότερη βαθμολογία.

Κατάταξη:	1	2	3	4
5	a	d	c	b
3	a	d	b	c
5	b	c	d	a
4	c	d	b	a
Βαθμοί:	3	2	1	0

$a: 5\cdot 3+3\cdot 3+5\cdot 0+4\cdot 0=24$. $b: 4\cdot 0+3\cdot 1+5\cdot 3+4\cdot 1=22$.
$c: 5\cdot 1+3\cdot 0+5\cdot 2+4\cdot 3=27$. $d: 5\cdot 2+3\cdot 2+5\cdot 1+4\cdot 2=29$.

(Νικήτρια: d)

Ο κανόνας του Condorcet. Συγκρίνουμε ανά δύο τις ταινίες. Η ταινία x κερδίζει στην μονομαχία με την y αν είναι περισσότεροι αυτοί που θεωρούν ότι $x > y$ παρά αυτοί που θεωρούν ότι $x < y$. Η ταινία που υπερισχύει σε όλες τις μονομαχίες κερδίζει.

Κατάταξη:	1	2	3	4
5	a	d	c	b
3	a	d	b	c
5	b	c	d	a
4	c	d	b	a

Μονομαχίες **(νίκες:ήττες)**

	a	b	c	d
a	-	8:9	8:9	8:9
b	9:8	-	8:9	5:12
c	9:8	9:8	-	9:8
d	9:8	12:5	8:9	-

(Νικήτρια: c)

Παρατηρήστε ότι στο παράδειγμα κάθε κανόνας οδηγεί σε διαφορετική απάντηση. Ποιός από αυτούς είναι πιο δίκαιος;

Ο Kenneth Arrow (βραβείο Νόμπελ Οικονομίας το 1972) εξέπληξε την επιστημονική κοινότητα αποδεικνύοντας ότι στην περίπτωση που υπάρχουν τουλάχιστον 3 υποψήφιοι δεν μπορεί να υπάρξει δίκαιος κανόνας για όλες τις πιθανές περιπτώσεις. Συγκεκριμένα:

Θεώρημα του Arrow. Ο μόνος κανόνας συλλογικής κατάταξης τριών ή περισσοτέρων υποψηφίων με βάση τις ατομικές κατατάξεις για τον οποίο ικανοποιούνται οι συνθήκες

- (Αξίωμα της ομοφωνίας) Αν όλοι οι ψηφοφόροι προτιμούν τον a από τον b τότε στην συλλογική κατάταξη πρέπει να προηγείται ο a από τον b.
- (Αξίωμα της ανεξαρτησίας) Η συλλογική κατάταξη δύο υποψηφίων a και b δεν πρέπει να επηρεάζεται από τις αλλαγές κατάταξης άλλων υποψηφίων.

είναι ο κανόνας του δικτάτορα (δηλαδή επιλέγεται ως συλλογική κατάταξη η ατομική κατάταξη κάποιου ψηφοφόρου).

Για περισσότερες πληροφορίες, βλέπε την ενότητα 10.1 Rankings and Social Choice στο βιβλίο A. Blum, J. Hopcroft, R. Kannan, *Foundations of data science*, March 2019. Λήψη □

Άσκηση 1.19. *Να εξετασθεί αν η απεικόνιση* $f(x)=x^2+x+1/\mathbb{R}$ *είναι ένα προς ένα.*

Λύση. Ο ισχυρισμός είναι λάθος. Είναι

$$\begin{aligned} f(x) = f(y) &\Leftrightarrow x^2 + x + 1 = y^2 + y + 1 \Leftrightarrow x^2 - y^2 + x - y = 0 \\ &\Leftrightarrow (x-y)(x+y) + x - y = 0 \\ &\Leftrightarrow (x-y)(x+y+1) = 0 \end{aligned}$$

Αν λοιπόν επιλέξουμε x, y τέτοια ώστε $x \neq y$ και $x + y = -1$, π.χ. $x = 0$ και $y = -1$, τότε $f(-1) = (-1)^2 + (-1) + 1 = 1 = f(0)$. □

Άσκηση 1.20. *Να εξετασθεί αν η απεικόνιση $f : A \to B$, με $A = [1, 2]$ και $B = [7, 10]$ και τύπο $f(x) = 2x + 5$ είναι επί.*

Λύση. Ο ισχυρισμός είναι λάθος. Είναι

$$x \in A \Rightarrow 1 \leq x \leq 2 \Rightarrow 2 \leq 2x \leq 4 \Rightarrow 7 \leq 2x + 5 \leq 9 \Rightarrow 7 \leq f(x) \leq 9$$

Άρα, αν $y \in B$, με $y > 9$, τότε δεν υπάρχει $x \in A$ τέτοιο ώστε $f(x) = y$. □

Άσκηση 1.21 (Εικόνες συνόλων). *Έστω $A = \{1, 2, 4, 5, 6, 7\}$, $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ και $f : A \to B$ με $f(x) = (x - 5)(x - 4)$. Να βρεθούν τα σύνολα $f(A)$, $f(\{3, 4\})$, $f(\emptyset)$, $f(\{1, 2, 6\})$, $f^{-1}(B)$, $f^{-1}(\{2\})$, $f^{-1}(\{0\})$, $f^{-1}(\{0, 2\})$, $f^{-1}(\{12\})$, $f^{-1}(\{9\})$, $f^{-1}(\{4, 5, 6\})$.*

Λύση. Ισχύει ότι

$f(A) = \{f(1), f(2), f(3), f(4), f(5), f(6), f(7)\} = \{12, 6, 2, 0, 0, 2, 6\} = \{0, 2, 6, 12\}$.
$f(\{3, 4\}) = \{f(3), f(4)\} = \{2, 0\}$.
$f(\emptyset) = \emptyset$.
$f(\{1, 2, 6\}) = \{f(1), f(2), f(6)\} = \{12, 6, 2\}$.
$f^{-1}(B) = A$.
$f^{-1}(\{2\}) = \{3, 6\}$, διότι $f(3) = f(6) = 2$ και $f(x) \neq 2$ για κάθε $x \in A$ με $x \neq 3, 6$.
$f^{-1}(\{0\}) = \{4, 5\}$, διότι $f(4) = f(5) = 0$ και $f(x) \neq 0$ για κάθε $x \in A$ με $x \neq 4, 5$.
$f^{-1}(\{0, 2\}) = f^{-1}(\{0\}) \cup f^{-1}(\{2\}) = \{3, 6\} \cup \{4, 5\} = \{3, 4, 5, 6\}$.
$f^{-1}(\{12\}) = \{1\}$, διότι $f(1) = 12$ και $f(x) \neq 12$ για κάθε $x \in A$ με $x \neq 1$.
$f^{-1}(\{9\}) = \emptyset$, διότι $f(x) \neq 9$ για κάθε $x \in A$.
$f^{-1}(\{4, 5, 6\}) = f^{-1}(\{4\}) \cup f^{-1}(\{5\}) \cup f^{-1}(\{6\}) = \emptyset \cup \emptyset \cup \{2, 7\} = \{2, 7\}$. □

Άσκηση 1.22 (Εικόνες 1–1 συναρτήσεων). *Έστω $f : A \to B$. Να δειχθεί ότι η f είναι $1-1$ αν και μόνο αν $f^{-1}(f(\Gamma)) = \Gamma$, για κάθε $\Gamma \subseteq A$.*

Λύση. Έστω ότι η απεικόνιση f είναι $1-1$· θα δειχθεί ότι $f^{-1}(f(\Gamma)) = \Gamma$.

Επειδή για κάθε απεικόνιση f ισχύει ότι $\Gamma \subseteq f^{-1}(f(\Gamma))$, αρκεί να δειχθεί ότι $f^{-1}(f(\Gamma)) \subseteq \Gamma$. Πράγματι, αν $x \in f^{-1}(f(\Gamma))$, τότε $f(x) \in f(\Gamma)$ οπότε θα υπάρχει $\xi \in \Gamma$ με $f(x) = f(\xi)$. Επειδή η συνάρτηση f είναι $1-1$ έπεται ότι $x = \xi$, οπότε $x \in \Gamma$.

Αντίστροφα, αν $f^{-1}(f(\Gamma)) = \Gamma$ για κάθε $\Gamma \subseteq A$, θα δειχθεί ότι η f είναι $1-1$. Πραγματικά, αν $x_1, x_2 \in A$ με $f(x_1) = f(x_2)$, εφαρμόζουμε τη δοσμένη ισότητα για $\Gamma = \{x_1\}$, οπότε προκύπτει ότι $x_2 \in f^{-1}(f(\{x_1\})) = \{x_1\}$ και επομένως $x_1 = x_2$. □

Άσκηση 1.23 (Ισοδύναμα σύνολα). *Δίνονται τα σύνολα* $A = \{2^3, 2^4, 2^5, \ldots\}$ *και* $B = \{4^6, 4^8, 4^{10}, \ldots\}$. *Να δοθεί μια αμφιμονοσήμαντη απεικόνιση* $f : A \to B$.

Λύση. Απεικονίζουμε το τυχαίο στοιχείο 2^n, $n \in \mathbb{N}^*$, του A στο 4^{2n}, δηλαδή ορίζουμε $f(2^n) = 4^{2n}$.

Επειδή $4^{2n} = (2^2)^{2n} = 2^{4n} = (2^n)^4$, η f ορίζεται ισοδύναμα από τον τύπο $f(x) = x^4$.

Το τυχαίο στοιχείο y του B είναι της μορφής $y = 4^{2n}$. Το στοιχείο αυτό είναι εικόνα του $x = 2^n \in A$, άρα η f είναι επί. Επιπλέον, η f είναι και ένα προς ένα, διότι το x είναι το μοναδικό πρότυπο για το y. Πράγματι, αν υπάρχει και άλλο πρότυπο $x' = 2^m$ με $f(x') = y$, τότε

$$y = 4^{2n} = f(x') = f(2^m) = 4^{2m} \Rightarrow 2n = 2m \Rightarrow n = m \Rightarrow x = x'.$$ □

Άσκηση 1.24. *Έστω* $\sim$ *μια σχέση ισοδυναμίας στο πεπερασμένο σύνολο* A. *Να δειχθεί για τον πληθάριθμο του σύνολου πηλίκου* $A/\sim$ *ισχύει η ισότητα*

$$|A/\sim| = \sum_{a \in A} \frac{1}{|C_a|},$$

όπου C_a *είναι η κλάση ισοδυναμίας στην οποία ανήκει το* a.

Λύση. Για κάθε κλάση ισοδυναμίας C της σχέσης $\sim$ ισχύει ότι

$$\sum_{x \in C} \frac{1}{|C|} = 1$$

αφού κάθε ένα από τα $|C|$ στοιχεία της κλάσης συνεισφέρει $\frac{1}{|C|}$ στο άθροισμα.

Κάθε στοιχείο a του A ανήκει ακριβώς σε μια κλάση ισοδυναμίας C, επομένως όλα τα στοιχεία μιας κλάσης συνεισφέρουν στο άθροισμα

$$\sum_{a \in A} \frac{1}{|C_a|}$$

ακριβώς μια μονάδα, και όλες οι κλάσεις συνεισφέρουν τόσες μονάδες όσες και το πλήθος τους.

Άρα, ο πληθάριθμος του συνόλου πηλίκου $A/\sim$ που είναι το σύνολο όλων των ξένων κλάσεων ισοδυναμίας C_a, $a \in C$ είναι ίσος με το προηγούμενο άθροισμα, δηλαδή

$$|A/\sim| = \sum_{a \in A} \frac{1}{|C_a|}.$$ □

Άσκηση 1.25. *Σε μια νομοτεχνική επιτροπή των Ηνωμένων Εθνών συμμετέχουν ομάδες εργασίας πολλών χωρών. Τα ζητήματα όπου υπάρχουν διαφορές τίθενται υπό ψηφοφορία στην οποία κάθε μέλος (και όχι κάθε ομάδα) ψηφίζει ανεξάρτητα. Να βρεθεί μια δίκαιη βαρύτητα για τις ψήφους των μελών της επιτροπής, έτσι ώστε όλες οι χώρες να έχουν την ίδια δύναμη ψήφου.*

Λύση. Μια απλή λύση είναι να δοθεί σε κάθε μέλος μιας χώρας βαρύτητα ψήφου ίση με το αντίστροφο του αριθμού των μελών από τα οποία αποτελείται η ομάδα της χώρας του. Π.χ. αν η ομάδα της χώρας του έχει 4 μέλη, τότε η ψήφος κάθε μέλους να έχει βαρύτητα $\frac{1}{4}$ και επομένως τα 4 μέλη, όταν συμφωνούν, να έχουν βαρύτητα ψήφου 1. Έτσι, κάθε χώρα έχει συνολική βαρύτητα ψήφου 1. (Η ιδέα για το συγκεκριμένο σύστημα ψηφοφορίας προέρχεται από τον τύπο της προηγούμενης άσκησης.) □

Άσκηση 1.26. *Σε μια πολιτιστική διοργάνωση συμμετέχουν αντιπροσωπείες από διαφόρους συλλόγους. Κάθε αντιπροσωπεία έχει 2 ή 3 ή 4 μέλη. Τα μέλη των 2/μελών αντιπροσωπειών φορούν μπλε διακριτικά, τα μέλη των 3/μελών αντιπροσωπειών φορούν κόκκινα διακριτικά και τα μέλη των 4/μελών αντιπροσωπειών φορούν πράσινα διακριτικά. Να βρεθεί ο αριθμός των αντιπροσωπειών που συμμετέχουν στην διοργάνωση όταν είναι γνωστό ότι υπάρχουν* 170 *άτομα με μπλε διακριτικά,* 153 *με κόκκινα διακριτικά και* 128 *με πράσινα διακριτικά.*

Λύση. Οι αντιπροσωπείες είναι οι κλάσεις ισοδυναμίας της σχέσης ισοδυναμίας $\sim$ που σχετίζει δύο άτομα της διοργάνωσης αν και μόνο αν ανήκουν στην ίδια αντιπροσωπεία. Το σύνολο πηλίκο της σχέσης είναι το σύνολο όλων αντιπροσωπειών που συμμετέχουν στην διοργάνωση.

Οπότε, σύμφωνα με προηγούμενη άσκηση, ο ζητούμενος αριθμός ισούται με το άθροισμα

$$\sum_{a\in A}\frac{1}{C_a} = 170\cdot\frac{1}{2} + 153\cdot\frac{1}{3} + 128\cdot\frac{1}{4} = 85 + 51 + 32 = 168. \qquad \square$$

1.6 Ασκήσεις προς επίλυση

1) Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να δειχθούν οι παρακάτω ισότητες:

(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(iii) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
(iv) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
(v) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
(vi) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
(vii) $A \setminus (A \setminus B) = A \cap B$.
(viii) $(A \cap B) \cup (A \cap \overline{B}) \cup (\overline{A} \cap B) = A \cup B$.
(ix) $(A \setminus B) \setminus (A \setminus C) = A \cap \overline{B} \cap C$.

2) Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να δειχθούν οι παρακάτω προτάσεις:

(i) $A\triangle(B\triangle C) = (A\triangle B)\triangle C$.
(ii) $A\triangle\emptyset = A$.
(iii) $A\triangle A = \emptyset$.
(iv) $(A\triangle B)\triangle B = A$.
(v) Αν $A\triangle C = B\triangle C$, τότε $A = B$.
(vi) $A\triangle E = \overline{A}$.
(vii) $A\triangle\overline{A} = E$.
(viii) $\overline{A}\triangle\overline{B} = A\triangle B$.
(ix) $A\triangle(B \setminus A) = A \cup B$.

3) Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να δειχθούν οι παρακάτω προτάσεις:

(i) $A \cap B = A \Leftrightarrow A \subseteq B$.
(ii) $A \cup B = B \Leftrightarrow A \subseteq B$.
(iii) $A \setminus B = \emptyset \Leftrightarrow A \subseteq B$.
(iv) $A \setminus B = A \Leftrightarrow A \cap B = \emptyset$.
(v) $A \setminus B = A \setminus C \Leftrightarrow A \cap B = A \cap C$.
(vi) $A \subseteq B \Rightarrow \overline{B} \subseteq \overline{A}$.

4) Έστω E ένα μη κενό σύνολο και $A, B \subseteq E$. Να λυθούν οι παρακάτω εξισώσεις, όπου X είναι το άγνωστο σύνολο.

i) $A \cap X = B$.
ii) $A \cup X = B$.
iii) $A \cup X = B \cap X$.
iv) $(B \cap X) \cup (A \cap X) = \emptyset$
v) $(A \cap X) \cup (B \setminus X) = \emptyset$.
vi) $(A \setminus X) \cap (B \cup X) = \emptyset$.

5) Έστω E ένα μη κενό σύνολο και $A_1, A_2, \ldots, A_n \subseteq E$, όπου $n \geq 2$. Να δειχθεί ότι

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq A_1 \Leftrightarrow A_1 = A_2 = \cdots = A_n.$$

6) Να βρεθεί το δυναμοσύνολο $\mathcal{P}(A)$ όταν

i) $A = \{1\}$.
ii) $A = \emptyset$.
iii) $A = \{\emptyset\}$.
iv) $A = \{\{\emptyset\}\}$.
v) $A = \{1, 2\}$.
vi) $A = \{a, b, c, d\}$.
vii) $A = \{1, \{1\}\}$.
viii) $A = \{1, \{1\}, \{1, \{1\}\}\}$.
ix) $A = \{1, \{1, 2\}, 2\}$.
x) $A = \mathcal{P}(\{0, 1\})$.

7) Να βρεθούν τρία σύνολα A, B, C για τα οποία ισχύει ότι

i) $A \in B$, $B \in C$ και $A \notin C$.

ii) $A \in B$, $B \in C$ και $A \in C$.

8) Έστω, E ένα μη κενό σύνολο και $A, B, C, D \subseteq E$. Να απλοποιηθούν οι παρακάτω εκφράσεις συνόλων

i) $\overline{(A \cap B)} \cup B$.

ii) $(A \cap B \cap C) \cup (\overline{A} \cap B \cap C) \cup (\overline{B} \cap \overline{C})$.

iii) $(A \cap B \cap C \cap \overline{D}) \cup (\overline{A} \cap C) \cup (\overline{B} \cap C) \cup (C \cap D)$.

9) Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να δειχθεί ότι οι επόμενες προτάσεις είναι όλες ψευδείς:

(i) Για κάθε A, B, C, αν $A \nsubseteq B$ και $B \nsubseteq C$ τότε $A \subset C$.

(ii) Για κάθε A, B, C ισχύει ότι $(A \cup B) \cap C = A \cup (B \cap C)$.

(iii) Για κάθε A, B, C ισχύει ότι $(A \setminus B) \cap (C \setminus B) = A \setminus (B \cup C)$.

(iv) Για κάθε A, B, C, αν $A \cap C \subseteq B \cap C$ και $A \cup C \subseteq B \cup C$, τότε $A = B$.

(v) Για κάθε A, B, C αν $A \cup C = B \cup C$ τότε $A = B$.

(vi) Για κάθε A, B, C ισχύει ότι $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.

10) Έστω E ένα μη κενό σύνολο και $A, B, C \subseteq E$. Να εξετασθεί αν ισχύουν οι παρακάτω προτάσεις:

(i) Για κάθε A, B, C ισχύει ότι $(A \setminus C) \cap (B \setminus C) \cap (A \setminus B) = \emptyset$.

(ii) Για κάθε A, B, αν $A \subseteq B$ τότε $A \cap (E \setminus B) = \emptyset$.

(iii) Για κάθε A, B, C, αν $A \subseteq B$ τότε $A \cap (E \setminus (B \cap C)) = \emptyset$.

(iv) Για κάθε A, B, C, αν $(B \cap C) \subseteq A$ τότε $(A \setminus B) \cap (A \setminus C) = \emptyset$.

(v) Για κάθε A, B, C ισχύει ότι $(A \setminus B) \cap (B \setminus C) = \emptyset$.

(vi) Για κάθε A, B, C ισχύει ότι $(A \setminus B) \cap (C \setminus B) = \emptyset$.

(vii) Για κάθε A, B, C ισχύει ότι $(A \setminus (B \cup C)) \cap (B \setminus (A \cup C)) = \emptyset$.

(viii) Για κάθε A, B, C ισχύει ότι $(A \setminus (B \cap C)) \cap (B \setminus (A \cap C)) = \emptyset$.

Αν κάποια από αυτές ισχύει να δοθεί η απόδειξή της, αν όχι να δοθεί ένα αντιπαράδειγμα.

11) Για κάθε δύο σύνολα A, B ορίζουμε $A \mid B = \overline{(A \cap B)}$. Να δειχθεί ότι οι πράξεις $\cup$, $\cap$, $\bar{}$, $\setminus$, $\triangle$ μπορούν να ορισθούν χρησιμοποιώντας μόνο με την πράξη $|$.

12) Για κάθε δύο σύνολα A, B ορίζουμε $A \downarrow B = \overline{(A \cup B)}$. Να δειχθεί ότι οι πράξεις $\cup$, $\cap$, $\bar{}$, $\setminus$, $\triangle$ μπορούν να ορισθούν χρησιμοποιώντας μόνο με την πράξη $\downarrow$.

13) Δίδονται τα σύνολα $A = [9]$, $B = \{\alpha, \beta, \gamma\}$, $\Gamma = \{\alpha, \delta, \varepsilon, \zeta, \eta\}$.

(i) Να βρεθεί το πλήθος των στοιχείων των συνόλων

$$A \times B, \quad B \times \Gamma, \quad A \times B \times \Gamma, \quad \Gamma^2.$$

(ii) Να γραφούν τα σύνολα $\Gamma \times A$ και B^2.

14) Έστω $A, B \subseteq E$. Να αποδειχθούν οι παρακάτω ιδιότητες:

i) $A = B$ αν και μόνο αν $\mu_A(x) = \mu_B(x)$, για κάθε $x \in E$.

ii) $A \subseteq B$ αν και μόνο αν $\mu_A(x) \leq \mu_B(x)$, για κάθε $x \in E$.

iii) $\mu_{A\cup B}(x) = \max\{\mu_A(x), \mu_B(x)\} = \mu_A(x) + \mu_B(x) - \mu_{A\cap B}(x)$, για κάθε $x \in E$.

iv) $\mu_{A\cap B}(x) = \min\{\mu_A(x), \mu_B(x)\} = \mu_A(x) \cdot \mu_B(x)$, για κάθε $x \in E$.

15) Σε ποιές από τις παρακάτω περιπτώσεις η συνάρτηση $f : A \to B$ είναι $1-1$, επί, ή αμφιμονοσήμαντη;

i) $A = [0, 1]$, $B = [5, 9]$ και $f(x) = 3x + 5$.

ii) $A = [-2, 2]$, $B = [0, 4]$ και $f(x) = x^2$.

iii) $A = [0, 2]$, $B = [\frac{1}{3}, 1]$ και $f(x) = \frac{1}{x+1}$.

16) Δίνονται οι συναρτήσεις $f : A \to B$ και $g : B \to \Gamma$. Να δειχθεί ότι αν f, g είναι $1-1$ (αντίστοιχα επί) τότε και η σύνθεση τους $g \circ f$ είναι $1-1$ (αντίστοιχα επί).

17) Να δειχθεί ότι αν $f : A \to B$ και $g : B \to \Gamma$ είναι δυο αμφιμονοσήμαντες απεικονίσεις τότε $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

18) Έστω $A = \{1, 2, 3, 4, 5\}$, $B = \{0, 2, 4, 6, 8, 10, 12\}$ και $f : A \to B$ με $f(x) = (x-1)(x-2)(x-3)$. Να βρεθούν τα σύνολα $f(A)$, $f(\{2, 3\})$, $f^{-1}(B)$, $f^{-1}(\{0\})$, $f^{-1}(\{4\})$, $f^{-1}(\{2, 4, 10\})$.

19) Έστω $f : A \to B$ μια απεικόνιση. Να δειχθεί ότι

(i) $f(f^{-1}(\Delta)) \subseteq \Delta$ και $f^{-1}(f(\Gamma)) \supseteq \Gamma$ για κάθε $\Gamma \subseteq A$, $\Delta \subseteq B$.

(ii) $f(\Gamma_1) \subseteq f(\Gamma_2)$, όταν $\Gamma_1 \subseteq \Gamma_2 \subseteq A$.

(iii) $f^{-1}(\Delta_1) \subseteq f^{-1}(\Delta_2)$, όταν $\Delta_1 \subseteq \Delta_2 \subseteq B$.

(iv) $f(\Gamma_1 \cup \Gamma_2) = f(\Gamma_1) \cup f(\Gamma_2)$, όταν $\Gamma_1, \Gamma_2 \subseteq A$.

(v) $f^{-1}(\Delta_1 \cup \Delta_2) = f^{-1}(\Delta_1) \cup f^{-1}(\Delta_2)$, όταν $\Delta_1, \Delta_2 \subseteq B$.

(vi) $f(\Gamma_1 \cap \Gamma_2) \subseteq f(\Gamma_1) \cap f(\Gamma_2)$, όταν $\Gamma_1, \Gamma_2 \subseteq A$.

(vii) $f^{-1}(\Delta_1 \cap \Delta_2) = f^{-1}(\Delta_1) \cap f^{-1}(\Delta_2)$, όταν $\Delta_1, \Delta_2 \subseteq B$.

(viii) $f(\Gamma_2) \setminus f(\Gamma_1) \subseteq f(\Gamma_2 \setminus \Gamma_1)$ για κάθε $\Gamma_1, \Gamma_2 \subseteq A$.

(ix) Η f είναι επί αν και μόνο αν $f(f^{-1}(\Delta)) = \Delta$, για κάθε $\Delta \subseteq B$.

(x) Η f είναι $1-1$ αν και μόνο αν $f(\Gamma_1 \cap \Gamma_2) = f(\Gamma_1) \cap f(\Gamma_2)$ για κάθε $\Gamma_1, \Gamma_2 \subseteq A$.

20) Έστω $A = \{1, 2, 3, 4\}$ και $B = \{2, 4, 6\}$.

Ορίζουμε $R_1 = \{(x, y) \in A \times B : x = y\}$, $R_2 = \{(x, y) \in A \times B : y - x \in A\}$, $R_3 = \{(x, y) \in A \times A : x + y \in B\}$.

(i) Να εξετασθεί ποιές από τις παραπάνω σχέσεις είναι σχέσεις ανακλαστικές, συμμετρικές, αντισυμμετρικές, μεταβατικές, σχέσεις ισοδυναμίας, σχέσεις διάταξης.

(ii) Να βρεθούν οι σχέσεις $R_1^{-1}, R_2^{-1}, R_3^{-1}$, $R_1 \cup R_2$, $R_2 \cup R_3$, $R_1 \cap R_2^{-1}$, $R_1 \circ R_3$, $R_3 \circ R_2$, $R_1 \cup (R_2 \cap R_3)$, $R_1 \circ R_1$, $R_2 \circ R_2$, $R_3 \circ R_3$, $R_3 \circ R_3 \circ R_3$.

21) Να βρεθούν όλες οι διαμερίσεις των συνόλων $A = \{1, 2, 3\}$ και $B = \{a, b, c, d\}$.

22) Να δοθούν παραδείγματα σχέσεων οι οποίες:

(i) είναι ανακλαστικές αλλά όχι συμμετρικές και μεταβατικές.
(ii) είναι συμμετρικές αλλά όχι ανακλαστικές και μεταβατικές.
(iii) είναι μεταβατικές αλλά όχι ανακλαστικές και συμμετρικές.
(iv) είναι ανακλαστικές και συμμετρικές αλλά όχι μεταβατικές.
(v) είναι ανακλαστικές και μεταβατικές αλλά όχι συμμετρικές.
(vi) είναι συμμετρικές και μεταβατικές αλλά όχι ανακλαστικές.

Τα ίδια ερωτήματα αντικαθιστώντας παντού την ιδιότητα συμμετρική με την αντισυμμετρική.

23) Να εξετασθεί ποιές από τις παρακάτω σχέσεις R_i, $i \in [8]$, οι οποίες ορίζονται στο σύνολο όλων των ανθρώπων, είναι σχέσεις ανακλαστικές, συμμετρικές, αντισυμμετρικές, μεταβατικές.

(i) $(x, y) \in R_1$ ανν οι x, y είναι αδέλφια.
(ii) $(x, y) \in R_3$ ανν ο x έχει μεγαλύτερη ηλικία από τον y.
(iii) $(x, y) \in R_4$ ανν οι x, y έχουν γεννηθεί την ίδια μέρα.
(iv) $(x, y) \in R_5$ ανν οι x, y έχουν ταξιδέψει με την ίδια πτήση.
(v) $(x, y) \in R_6$ ανν οι x, y δεν κατάγονται από την ίδια πόλη.
(vi) $(x, y) \in R_7$ ανν ο x είναι πατέρας.
(vii) $(x, y) \in R_8$ ανν ο x είναι πρόγονος του y.

24) Στο σύνολο $\mathbb{N} \times \mathbb{N}$ ορίζουμε τη σχέση R ως εξής:

$$(x, y)R(z, w) \Leftrightarrow x + w = y + z.$$

Να δειχθεί ότι η σχέση R είναι σχέση ισοδυναμίας.

25) Έστω R μια συμμετρική και μεταβατική σχέση σε ένα σύνολο A. Αν για κάθε $a \in A$ υπάρχει $b \in A$ ώστε aRb, τότε να δειχθεί ότι η R είναι σχέση ισοδυναμίας.

26) Να δειχθεί ότι αν R είναι σχέση ισοδυναμίας στο A, τότε και R^{-1} είναι επίσης σχέση ισοδυναμίας στο A.

27) Έστω R_1, R_2 σχέσεις ισοδυναμίας στο σύνολο A. Να δειχθεί ότι η σχέση $R_1 \cap R_2$ είναι σχέση ισοδυναμίας, ενώ η σχέση $R_1 \cup R_2$ δεν είναι, γενικά, σχέση ισοδυναμίας.

28) Έστω R μια σχέση ισοδυναμίας στο σύνολο A. Ορίζουμε τη σχέση $\widehat{R}$ στο A ως εξής:

$$x\widehat{R}y \Leftrightarrow \text{ υπάρχει } z \in A \text{ με } xRz \text{ και } zRy.$$

Να δειχθεί ότι η σχέση $\widehat{R}$ είναι σχέση ισοδυναμίας.

29) Έστω $R = \{(x, y) \in \mathbb{N}^* \times \mathbb{N}^* : |x - y| \text{ πολλαπλάσιο του } 2\}$. Το σύνολο R ορίζει μια σχέση ισοδυναμίας, με $n_1 \sim n_2$ όταν $\frac{n_1 - n_2}{2}$ είναι ακέραιος αριθμός. Να δειχθεί ότι το σύνολο πηλίκο της σχέσης $\sim$ είναι

$$\mathbb{N}^*/\sim = \{A_1, A_2\}$$

όπου A_1, A_2 είναι αντίστοιχα τα σύνολα των περιττών και άρτιων αριθμών.

30) Στο σύνολο $\mathbb{R}$ ορίζουμε τη σχέση σ ως εξής: $x\sigma y$ αν και μόνο αν $x - y \in \mathbb{Z}$. Να δειχθεί ότι η σχέση σ είναι σχέση ισοδυναμίας και να βρεθούν οι κλάσεις της.

31) Έστω E ένα μη κενό σύνολο. Για κάθε $X, Y \subseteq E$ ορίζουμε τη σχέση $\lhd$ ως εξής: $X \lhd Y \Leftrightarrow X \subseteq Y$. Να δειχθεί ότι η σχέση $\lhd$ είναι σχέση μερικής διάταξης. Είναι σχέση ολικής διάταξης;

32) Στο σύνολο $A = \{0, 1, 2, \ldots, n\}$ ορίζουμε τη σχέση R ως εξής:

$$aRb \Leftrightarrow b - a \in A.$$

Να δειχθεί ότι η σχέση R είναι σχέση μερικής διάταξης. Είναι σχέση ολικής διάταξης;

33) Έστω $(E_1, \leq_1)$, $(E_2, \leq_2)$ δύο διατεταγμένα σύνολα. Αν "$\leq$" είναι μια σχέση στο $E_1 \times E_2$ που ορίζεται ως εξής:

$$(\alpha_1, \alpha_2) \leq (\beta_1, \beta_2) \Leftrightarrow \alpha_1 \leq_1 \beta_1 \text{ και } \alpha_2 \leq_2 \beta_2,$$

να αποδειχθεί ότι η σχέση αυτή είναι μια διάταξη. Αν οι διατάξεις "$\leq_1$", "$\leq_2$" είναι ολικές, θα είναι και η διάταξη "$\leq$" ολική;

34) Έστω $(E_1, \leq_1)$, $(E_2, \leq_2)$ δύο διατεταγμένα σύνολα. Αν "$\prec$" είναι μια σχέση στο $E_1 \times E_2$ που ορίζεται ως εξής:

$$\begin{aligned}&(\alpha_1, \alpha_2) \prec (\beta_1, \beta_2) \Leftrightarrow \\ &(\alpha_1 \leq_1 \beta_1 \text{ και } \alpha_1 \neq \beta_1) \text{ ή } (\alpha_1 = \beta_1 \text{ και } \alpha_2 \leq_2 \beta_2),\end{aligned}$$

να αποδειχθεί ότι η σχέση αυτή είναι μια διάταξη. Αν οι διατάξεις "$\leq_1$", "$\leq_2$" είναι ολικές, θα είναι και η διάταξη "$\prec$" ολική;

35) Να δειχθεί ότι τα υποσύνολα A, Π του $\mathbb{N}$ που αποτελούνται από τους άρτιους και τους περιττούς φυσικούς αντίστοιχα, είναι ισοδύναμα.

36) Να δειχθεί ότι τα σύνολα $\mathbb{N}$ και $\mathbb{N}^*$ είναι ισοδύναμα.

37) Να δειχθεί ότι η απεικόνιση $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ με $f(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x$ είναι αμφιμονοσήμαντη.

38) Να δειχθεί ότι το σύνολο όλων των *πεπερασμένων* υποσυνόλων του $\mathbb{N}$ είναι αριθμήσιμο.

39) Να αποδειχθεί ότι το σύνολο

$$A = \{x \in \mathbb{R} : x = n + mt \text{ με } m, n \in \mathbb{N}^* \text{ και } t \in \mathbb{Q},\}$$

είναι αριθμήσιμο.

40) Έστω X, Y δύο μη κενά σύνολα και μια απεικόνιση f του X επί του Y. Αν το σύνολο Y είναι αριθμήσιμο και κάθε σύνολο της μορφής $f^{-1}(\{y\})$, $y \in Y$ είναι αριθμήσιμο, να αποδειχθεί ότι το σύνολο X είναι επίσης αριθμήσιμο.

41) Να δειχθεί ότι δεν υπάρχει απεικόνιση f του $\mathbb{N}^*$ επί του $\mathbb{R}$.

42) i) Δεδομένου ότι το σύνολο $\mathbb{Q}$ είναι αριθμήσιμο, να δειχθεί ότι κάθε σύνολο, ξένων ανά δύο διαστημάτων του $\mathbb{R}$, είναι επίσης αριθμήσιμο. (Υπόδειξη: Κάθε διάστημα περιέχει τουλάχιστον ένα ρητό αριθμό.)

ii) Δεδομένου ότι το σύνολο $\mathbb{Q}\times\mathbb{Q}$ είναι αριθμήσιμο, να δειχθεί ότι κάθε σύνολο, ξένων ανά δύο, κυκλικών δίσκων στο επίπεδο $\mathbb{R}\times\mathbb{R}$ είναι επίσης αριθμήσιμο.

∗iii) Να δειχθεί ότι γενικά δεν ισχύει το ίδιο για κάθε σύνολο, ξένων ανά δύο κύκλων στο επίπεδο $\mathbb{R}\times\mathbb{R}$. (Υπόδειξη. Οι μη αλγεβρικοί αριθμοί[6] είναι υπεραριθμήσιμοι).

43) Να δειχθεί ότι το σύνολο των άρρητων αριθμών είναι υπεραριθμήσιμο. (Υπόδειξη. Το σύνολο $\mathbb{R}$ είναι υπεραριθμήσιμο.)

44) Να δειχθεί ότι κάθε διάστημα $[\alpha,\beta]$ είναι ισοδύναμο με το $[0,1]$. (Υπόδειξη: Να δειχθεί ότι η απεικόνιση $f:[0,1]\to[\alpha,\beta]$ με $f(x)=(1-x)\alpha+x\beta$ είναι αμφιμονοσήμαντη.)

45) Να δειχθεί ότι τα σύνολα (a,b) και $\mathbb{R}$ είναι ισοδύναμα.

46) Να δειχθεί ότι το σύνολο $[0,+\infty)$ είναι ισοδύναμο με το $[0,1]$.

47) i) Να δειχθεί ότι το σύνολο A των σημείων του επιπέδου τα οποία βρίσκονται στο πρώτο τεταρτημόριο και έχουν ακέραιες συντατεγμένες είναι αριθμήσιμο.

∗ii) Να βρεθεί μια "αρίθμηση" των σημείων του A από διαδοχικούς φυσικούς αριθμούς.

48) i) Να δειχθεί ότι το σύνολο όλων των ευθειών του επιπέδου που διέρχονται από την αρχή των αξόνων είναι υπέραριθμήσιμο.

ii) Να δειχθεί ότι υπάρχει ευθεία του επιπέδου η οποία διέρχεται από την αρχή των αξόνων και δεν περιέχει κανένα άλλο σημείο με ρητές συντεταγμένες.

∗49) Να εξετασθεί ποιά από τα παρακάτω σύνολα απεικονίσεων είναι πεπερασμένα, ποιά είναι άπειρα, ποιά είναι αριθμήσιμα και ποιά είναι υπεραριθμήσιμα.

i) $\{f:\mathbb{N}\to\{0,1\}: f(n)\le f(n+1)$ για κάθε $n\in\mathbb{N}\}$.

ii) $\{f:\mathbb{N}\to\{0,1\}: f(2n)\ne f(2n+1)$ για κάθε $n\in\mathbb{N}\}$.

iii) $\{f:\mathbb{N}\to\{0,1\}: f(n)\ne f(n+1)$ για κάθε $n\in\mathbb{N}\}$.

iv) $\{f:\mathbb{N}\to\mathbb{N}: f(n)\le f(n+1)$ για κάθε $n\in\mathbb{N}\}$.

v) $\{f:\mathbb{N}\to\mathbb{N}: f(n)\ge f(n+1)$ για κάθε $n\in\mathbb{N}\}$.

50) Στην ετήσια συνάντηση των οικογενειών με επώνυμο ΠΑΠΑΔΟΠΟΥΛΟΣ συμμετέχουν πολλά άτομα. Η συνάντηση ολοκληρώνεται με δείπνο στο οποίο η χρέωση είναι σταθερή ανά οικογένεια. Στη διάρκεια της τελευταίας συνάντησης ο διοργανωτής διαπίστωσε ότι χάθηκαν οι αιτήσεις συμμετοχής των συμμετεχόντων. Να βρεθεί με ποιο τρόπο μπορεί να υπολογισθεί ο αριθμός των οικογενειών που συμμετέχουν στη συνάντηση ώστε να γίνει η χρέωση για το δείπνο.

[6] Ένας αριθμός ονομάζεται **αλγεβρικός** αν είναι ρίζα κάποιου πολυωνύμου με ακέραιους συντελεστές.

1.7 Παράρτημα: Αναπαράσταση συνόλων στον υπολογιστή

Υπάρχουν πολλοί τρόποι αναπαράστασης (πεπερασμένων) συνόλων σε υπολογιστή.

Στην ενότητα αυτή θα δούμε ένα τρόπο αναπαράστασης υποσυνόλων του $E_n = \{0, 1, 2, 3, \ldots, n\}$ χρησιμοποιώντας την κλάση **bitset** της *C++*.

Η ιδέα της αναπαράστασης είναι η εξής: Κάθε υποσύνολο A του $E_n = \{0, 1, 2, 3, \ldots, n\}$ μπορεί να κωδικοποιηθεί από μια δυαδική λέξη $a_0a_1a_2 \cdots a_n$ με μήκος $n + 1$ όπου

$$a_j = \begin{cases} 1, & \text{αν } j \in A, \\ 0, & \text{αν } j \notin A. \end{cases}$$

Παραδείγματα

Έστω ότι θέλουμε να αναπαραστήσουμε υποσύνολα του $E_{10} = \{0, 1, 2, \ldots, 10\}$. Σε κάθε ένα από αυτά θα αντιστοιχίσουμε μια δυαδική λέξη μήκους 11.

1) Το υποσύνολο $A_1 = \{0, 1, 5\}$ αναπαρίσταται από τη (δυαδική) λέξη

	0	1	2	3	4	5	6	7	8	9	10
A_1:	1	1	0	0	0	1	0	0	0	0	0

2) Το υποσύνολο $A_2 = \{1, 3, 5, 7\}$ αναπαρίσταται από τη λέξη

	0	1	2	3	4	5	6	7	8	9	10
A_2:	0	1	0	1	0	1	0	1	0	0	0

3) Η (δυαδική) λέξη

0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	1	0	0	1	1	0	0

αναπαριστά το υποσύνολο $A_3 = \{1, 4, 7, 8\}$.

4) Η λέξη

0	1	2	3	4	5	6	7	8	9	10
0	1	0	1	0	1	0	1	0	1	0

αναπαριστά το υποσύνολο $A_4 = \{1, 3, 5, 7, 9\}$.

5) Η λέξη

0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0

αναπαριστά το κενό σύνολο $\emptyset$.

6) Η λέξη

0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1

αναπαριστά το σύνολο E_{10}.

Το πλεονεκτήματα αυτής της αναπαράστασης είναι ότι μπορούμε να ελέγξουμε άμεσα αν ένα στοιχείο j του E_n ανήκει σε ένα υποσύνολο A.

Επιπλέον, μπορούμε να κάνουμε εύκολα πράξεις στα σύνολα. Πράγματι, έστω $A, B \subseteq E_n$ και έστω $a_0a_1a_2 \cdots a_n$ και $b_0b_1b_2 \cdots b_n$ οι αναπαραστάσεις των A, B αντίστοιχα. Τότε:

Το συμπλήρωμα του A, δηλαδή το σύνολο $\overline{A}$, έχει αναπαράσταση $c_0c_1c_2\cdots c_n$ όπου $c_j = 1 - a_j$, για κάθε $j \in E_n$.

Η ένωση των A και B, δηλαδή το σύνολο $A \cup B$ έχει αναπαράσταση $c_0c_1c_2\cdots c_n$ όπου $c_j = \max\{a_j, b_j\}$, για κάθε $j \in E_n$.

Η τομή των A και B, δηλαδή το σύνολο $A \cap B$ έχει αναπαράσταση $c_0c_1c_2\cdots c_n$ όπου $c_j = \min\{a_j, b_j\} = a_jb_j$, για κάθε $j \in E_n$.

Παραδείγματα

Χρησιμοποιώντας ως βασικό σύνολο αναφοράς το E_{10} των προηγούμενων παραδειγμάτων:

Το συμπλήρωμα του $A_1 = \{0, 1, 5\}$ έχει αναπαράσταση

	0	1	2	3	4	5	6	7	8	9	10
A_1:	1	1	0	0	0	1	0	0	0	0	0
$\overline{A_1}$:	0	0	1	1	1	0	1	1	1	1	1

δηλαδή είναι το σύνολο $\overline{A_1} = \{2, 3, 4, 6, 7, 8, 9, 10\}$.

Η ένωση και η τομή των $A_2 = \{1, 3, 5, 7\}$ και $A_3 = \{1, 4, 7, 8\}$ έχουν αναπαραστάσεις

	0	1	2	3	4	5	6	7	8	9	10
A_2:	0	1	0	1	0	1	0	1	0	0	0
A_3:	0	1	0	0	1	0	0	1	1	0	0
$A_2 \cup A_3$:	0	1	0	1	1	1	0	1	1	0	0
$A_2 \cap A_3$:	0	1	0	0	0	0	0	1	0	0	0

δηλαδή είναι τα σύνολα $A_2 \cup A_3 = \{1, 3, 4, 5, 7, 8\}$ και $A_2 \cap A_3 = \{1, 7\}$.

Ένα μειονέκτημα αυτής της αναπαράστασης είναι ότι αν το n είναι "μεγάλο" τότε τα "μικρά" υποσύνολα του A αναπαρίστανται έχοντας πολλά 0 και λίγα 1. (Άρα έχουμε σπατάλη μνήμης.)

1.7.1 Η κλάση bitset της C++

Η κλάση `bitset` της C++ υλοποιεί ακριβώς την παραπάνω ιδέα.

Συγκεκριμένα, κάθε `bitset` είναι ένας πίνακας από bits ο οποίος έχει σταθερό μήκος `size`, το οποίο καθορίζεται με τη δήλωση του bitset, και το οποίο είναι τύπου int ή long.

Για να χρησιμοποιήσουμε την κλάση bitset απαιτείται ο header <bitset>, ενώ είναι πάρα πολύ χρήσιμος και ο header <string>

Η δήλωση ενός bitset μπορεί να έχει μια από τις μορφές:

```
bitset<size> A;
```

ή,

```
bitset<size> B (string("1010...001"));
```

Στην πρώτη περίπτωση δημιουργείται ένα bitset A με μέγεθος ίσο με size όπου όλα τα bits του είναι ίσα με 0, ενώ στη δεύτερη περίπτωση δημιουργείται ένα bitset B με μέγεθος ίσο με size του οποίου τα bits καθορίζονται από το string "1010...001" με μήκος ίσο με size το οποίο δίδεται ως όρισμα.

Προκειμένου να εκτυπώσουμε ένα bitset A αρκεί να δώσουμε την εντολή

```
cout << A;
```

Παρακάτω παρουσιάζεται ένα παράδειγμα δήλωσης και εκτύπωσης τριών bitset μήκους 8:

```
#include <iostream> // cout
#include <bitset>   // bitset
#include <string>   // string

using namespace std;

int main(){

bitset<8> A; // A : 00000000
bitset<8> B (string("11101001")); // B : 11001001
bitset<8> C (string("111")); // C : 00000111

cout << "A: " << A << '\n';
cout << "B: " << B << '\n';
cout << "C: " << C << '\n';

return 0;
}
```

Παρατηρείστε ότι στο bitset C δόθηκε ως όρισμα ένα string μήκους 3 το οποίο είναι μικρότερο του 8. Όπως μπορούμε να διαπιστώσουμε από την εκτύπωση το C πήρε την τιμή 00000111, δηλαδή τα 3 bits τοποθετήθηκαν στο τέλος του bitset C.

Οι πράξεις του συμπληρώματος, της ένωσης και της τομής bitset υλοποιούνται εύκολα χρησιμοποιώντας τους τελεστές ~, | και & αντίστοιχα[7]: Επίσης, από τον τύπο $A \setminus B = A \cap \overline{B}$, μπορούμε να βρούμε τη διαφορά $A \setminus B$ συνδυάζοντας τους τελεστές & και ~.

Παρακάτω παρουσιάζεται ένα παράδειγμα χρήσης των τελεστών αυτών:

```
#include <iostream> // cout
#include <bitset>   // bitset
#include <string>   // string

using namespace std;

int main(){

bitset<8> A; // A : 00000000
bitset<8> B (string("11001001")); // B : 11001001
bitset<8> C (string("111")); // C : 00000111

cout << "A: " << A << '\n';
cout << "B: " << B << '\n';
cout << "C: " << C << '\n';

cout << "Complement of B: " << ( B) << '\n'; // 00110110
cout << "Union of B and C: " << (B|C) << '\n'; // 11001111
cout << "Intersection of B and C: " << (B&C) << '\n'; // 00000001
cout << "Difference B \ C: " << (B&( C)) << '\n'; // 11001000

return 0;
```

[7] **Προσοχή**: Ένα συνηθισμένο λάθος είναι η λανθασμένη ταύτισή τους με τους λογικούς τελεστές !, || και && αντίστοιχα!

```
}
```

Προκειμένου να αλλάξουμε ένα ή περισσότερα bits ενός bitset A χρησιμοποιούμε τις παρακάτω μεθόδους:

1. `A.set()`: Θέτει όλα τα bits του A ίσα με 1.
2. `A.set(j)`: Θέτει το j-οστό bit του A ίσο με 1[8].
3. `A.reset()`: Θέτει όλα τα bits του A ίσα με 0.
4. `A.reset(j)`: Θέτει το j-οστό bit του A ίσο με 0.
5. `A.flip()`: Αλλάζει όλα τα bits του A από 0 σε 1 και αντιστρόφως.
6. `A.flip(j)`: Αλλάζει το j-οστό bit του A από 0 σε 1 και αντιστρόφως.

Προκειμένου να δούμε την τιμή ενός bit υπάρχουν δύο τρόποι:

1. `A.test(j)`: Επιστρέφει true αν το j-οστό bit του A είναι 1 και false αν είναι 0.
2. `A[j]`: Η σύνταξη που χρησιμοποιείται και στους πίνακες. Η τιμή του $A[j]$ είναι true αν το j-οστό bit του A είναι 1 και false αν είναι 0.

Η διαφορά των δύο τρόπων είναι ότι με τον πρώτο γίνεται έλεγχος αν το j είναι μικρότερο από το μέγεθος του bitset A και υπάρχει αντίστοιχο exception στην περίπτωση που δεν είναι, ενώ στο δεύτερο τρόπο δεν υπάρχει τέτοιος έλεγχος.

Επίσης, χρήσιμες είναι και οι παρακάτω μέθοδοι:

1. `A.size()`: Επιστρέφει το μέγεθος του bitset A·
2. `A.count()`: Επιστρέφει το πλήθος των 1 στο A, δηλαδή τον πληθάριθμο του A.
3. `A.all()`: Επιστρέφει true αν όλα τα bits του A είναι 1, αλλιώς false.
4. `A.any()`: Επιστρέφει false αν όλα τα bits του A είναι 0, αλλιώς true.
5. `A.none()`: Επιστρέφει true αν όλα τα bits του A είναι 0, αλλιώς false.

Τέλος, σημειώνεται ότι οι λογικοί τελεστές της ισότητας == και μη ισότητας ! = εφαρμόζονται και σε bitsets.

Παρατήρηση. Για bitset με μεγάλο μέγεθος συνιστάται η δήλωση τους χρησιμοποιώντας τον τελεστή new. Με τον τρόπο αυτό το bitset παίρνει μνήμη από το heap και όχι από το stack το οποίο συνήθως έχει περιορισμένο μέγεθος.

```
bitset<size>& A = *(new bitset<size>());
```

[8] Υπενθυμίζεται ότι, όπως και σε όλους του πίνακες, η αρίθμηση αρχίζει από το 0.

Ασκήσεις προς επίλυση

1) Έστω $E = [1000]$ και $A, B, C, D, F, G, H \subset E$ όπου

   $A = \{n \in E : n$ είναι πολλαπλάσιο του $2\}$.

   $B = \{n \in E : n$ είναι πολλαπλάσιο του $3\}$.

   $C = \{n \in E : n$ είναι τετράγωνο ακεραίου$\}$.

   $D = \{n \in E : n$ περιέχει ψηφίο ίσο με $1\}$.

   $F = \{n \in E : n$ έχει τελευταίο ψηφίο ίσο με $1\}$.

   $G = \{n \in E : n$ περιέχει ψηφίο ίσο με $7\}$.

   $H = \{n \in E : n$ είναι πρώτος αριθμός$\}$.

   Να βρεθούν τα σύνολα $((A \cap B) \cup C)^C$, $A \setminus G$ και $(H \cup B)^C \setminus D$. Πόσα στοιχεία περιέχει το καθένα; Ποιό σύνολο περιέχει τα περισσότερα στοιχεία; Ποιό τα λιγότερα;

2) Έστω $A, B \subseteq E_n = \{0, 1, \ldots, n\}$ και $a_0a_1a_2 \cdots a_n$, $b_0b_1b_2 \cdots b_n$ οι αντίστοιχες αναπαραστάσεις τους.

   (i) Πόσα είναι τα διαφορετικά υποσύνολα του E_n;

   (ii) Ποια είναι η αναπαράσταση της διαφοράς $A \setminus B$; Της συμμετρικής διαφοράς $A \triangle B$;

   (iii) Πόσα στοιχεία περιέχονται στο σύνολο A;

1.8 Παράρτημα: Το παράδοξο του Russell

Η μέθοδος ορισμού συνόλων με τη βοήθεια μιας *οποιασδήποτε ιδιότητας*, π.χ.

$$A = \{x \in \mathbb{N} : x \text{ είναι άρτιος}\},$$

$$B = \{\text{Το σύνολο των φοιτητών του Τμήματος Πληροφορικής}\},$$

$$C = \{\text{Το σύνολο των ψηλών ανθρώπων}\},$$

μπορεί να οδηγήσει σε παράδοξα και γενικά επιτρέπεται **μόνο** αν υπάρχει ένα σύνολο αναφοράς από το οποίο επιλέγονται τα στοιχεία αυτών των συνόλων, και μόνο αν η ιδιότητα τηρεί ορισμένες προϋποθέσεις. (Για το A το σύνολο αναφοράς είναι το $\mathbb{N}$, ενώ για το B το σύνολο αναφοράς είναι το σύνολο όλων των φοιτητών, ενώ το σύνολο C δεν ορίζεται διότι η ιδιότητα ορισμού του δεν είναι σαφώς καθορισμένη.)

Πιο συγκεκριμένα **δεν ορίζεται** *το σύνολο όλων των συνόλων*. Πράγματι, η παραδοχή της ύπαρξης του συνόλου όλων των συνόλων οδηγεί στο επόμενο παράδοξο, το οποίο οφείλεται στον Bertrand Russell (1872–1970).

Αν δεχτούμε ότι υπάρχει το σύνολο όλων των συνόλων τότε μπορούμε να ορίσουμε σύνολα όπως το επόμενο:

$$P = \{\text{σύνολο } X : X \notin X\},$$

δηλαδή το P είναι το σύνολο όλων συνόλων X με την ιδιότητα $X \notin X$. (Εδώ το σύνολο αναφοράς είναι το σύνολο όλων των συνόλων από το οποίο επιλέγονται τα σύνολα με την ιδιότητα $X \notin X$).

Το παράδοξο προκύπτει αν προσπαθήσουμε να ελέγξουμε αν ισχύει $P \in P$ ή $P \notin P$.

Αν $P \in P$, τότε πρέπει $P \notin P$.

Αν $P \notin P$, τότε πρέπει $P \in P$.

Επομένως, και στις δύο περιπτώσεις έχουμε αντίφαση. Οδηγηθήκαμε σε αντίφαση διότι θεωρήσαμε ότι υπάρχει ως σύνολο αναφοράς το σύνολο όλων των συνόλων.

Η παραπάνω κατασκευή ονομάζεται παράδοξο του Russell.

Περισσότερα στοιχεία για τα προβλήματα της θεμελίωσης των συνόλων περιέχονται στα κεφαλαία 1 και 3 του βιβλίου *Σημειώσεις στη συνολοθεωρία* του Γιάννη Ν. Μοσχοβάκη, το οποίο είναι διαθέσιμο και από το σύνδεσμο: http://www.math.ucla.edu/~ynm/lectures/g.pdf

Κεφάλαιο 2

Βασικές αρχές

2.1 Μαθηματική επαγωγή

Πρόταση 2.1 (**Αρχή της επαγωγής**). *Έστω* $\Pi(n)$ *μια πρόταση με* $n \in \mathbb{N}^*$, *για την οποία ισχύουν τα παρακάτω:*

i) Η $\Pi(1)$ *είναι αληθής.*

ii) Αν η $\Pi(k)$ *είναι αληθής, τότε και η* $\Pi(k+1)$ *είναι αληθής.*

Τότε η $\Pi(n)$ *είναι αληθής για κάθε* $n \in \mathbb{N}^*$.

Η πρόταση αυτή ονομάζεται **αρχή της** (**τέλειας**) **επαγωγής** και χρησιμοποιείται συχνά για την απόδειξη προτάσεων που αναφέρονται σε φυσικούς αριθμούς.

Παράδειγμα 2.1.1. *Να δειχθεί ότι*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},$$

για κάθε $n \in \mathbb{N}^*$.

Απόδειξη. Η πρόταση που θέλουμε να δείξουμε είναι η:

$$\Pi(n) : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

i) Η $\Pi(1)$: $1 = \frac{1(1+1)}{2}$ προφανώς ισχύει.

ii) Έστω ότι ισχύει η $\Pi(k)$, δηλαδή έστω ότι

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Θα δείξουμε ότι ισχύει και η $\Pi(k+1)$, δηλαδή θα δείξουμε ότι

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2},$$

(οπότε βάσει της αρχής της επαγωγής, η $\Pi(n)$ θα ισχύει για κάθε $n \in \mathbb{N}^*$).

Πράγματι,

$$\underbrace{1+2+\cdots+k}_{=\frac{k(k+1)}{2}}+(k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= (k+1)(\frac{k}{2}+1) = \frac{(k+1)(k+2)}{2}. \qquad \square$$

Παράδειγμα 2.1.2. *Να δειχθεί ότι $2^n > n$ για κάθε $n \in \mathbb{N}^*$.*

Απόδειξη. Εδώ $\Pi(n)$: $2^n > n$.

i) $\Pi(1)$: $2^1 > 1$ ισχύει.

ii) Έστω ότι ισχύει η

$$\Pi(k) : 2^k > k.$$

Θα δείξουμε ότι ισχύει και η

$$\Pi(k+1) : 2^{k+1} > k+1.$$

Πράγματι,

$$2^{k+1} = 2 \cdot 2^k > 2k \geq k+1$$

(αφού $k \in \mathbb{N}^*$ και άρα $k \geq 1$). $\square$

Παράδειγμα 2.1.3. *Να δειχθεί ότι $\left(\frac{4}{3}\right)^n + \left(\frac{5}{4}\right)^n > \frac{7n}{12}$ για κάθε $n \in \mathbb{N}^*$.*

Απόδειξη. Εδώ $\Pi(n) : \left(\frac{4}{3}\right)^n + \left(\frac{5}{4}\right)^n > \frac{7n}{12}$

i) $\Pi(1)$: $\frac{4}{3} + \frac{5}{4} > \frac{7}{12} \Leftrightarrow \frac{31}{12} > \frac{7}{12}$ ισχύει.

ii) Έστω ότι ισχύει η

$$\Pi(k) : \left(\frac{4}{3}\right)^k + \left(\frac{5}{4}\right)^k > \frac{7k}{12}.$$

Θα δείξουμε ότι ισχύει και η

$$\Pi(k+1) : \left(\frac{4}{3}\right)^{k+1} + \left(\frac{5}{4}\right)^{k+1} > \frac{7(k+1)}{12}$$

Πράγματι,

$$\begin{aligned}\left(\frac{4}{3}\right)^{k+1}+\left(\frac{5}{4}\right)^{k+1} &= \frac{4}{3}\left(\frac{4}{3}\right)^{k}+\frac{5}{4}\left(\frac{5}{4}\right)^{k}\\ &= \left(\frac{4}{3}\right)^{k}+\left(\frac{5}{4}\right)^{k}+\frac{1}{3}\left(\frac{4}{3}\right)^{k}+\frac{1}{4}\left(\frac{5}{4}\right)^{k}\\ &> \frac{7k}{12}+\frac{1}{3}+\frac{1}{4}\\ &= \frac{7k}{12}+\frac{7}{12}\\ &= \frac{7(k+1)}{12}\end{aligned}$$

□

Παράδειγμα 2.1.4. *Να δειχθεί ότι ο αριθμός $7^n + 3^n - 2$ είναι πολλαπλάσιο του 8, για κάθε $n \in \mathbb{N}^*$.*

Απόδειξη. Εδώ $\Pi(n) : 7^n + 3^n - 2$ είναι πολλαπλάσιο του 8.

i) $\Pi(1)$: $7^1 + 3^1 - 2$ πολλαπλάσιο του 8, ισχύει.

ii) Έστω ότι ισχύει n

$$\Pi(k) : 7^k + 3^k - 2 \text{ είναι πολλαπλάσιο του 8.}$$

Θα δείξουμε ότι ισχύει και n

$$\Pi(k+1) : 7^{k+1} + 3^{k+1} - 2 \text{ είναι πολλαπλάσιο του 8.}$$

Πράγματι,

$$\begin{aligned}7^{k+1} + 3^{k+1} - 2 &= 7 \cdot 7^k + 3 \cdot 3^k - 2\\ &= (8-1) \cdot 7^k + (4-1) \cdot 3^k - 2\\ &= 8 \cdot 7^k + 4 \cdot 3^k - (7^k + 3^k) - 2\\ &= 8 \cdot 7^k + 4 \cdot 3^k - (7^k + 3^k - 2) - 4\\ &= 8 \cdot 7^k + 4 \cdot (3^k - 1) - (7^k + 3^k - 2)\end{aligned}$$

Οπότε επειδή ο αριθμός $8 \cdot 7^k$ είναι πολλαπλάσιο του 8, ο αριθμός $4(3^k - 1)$ είναι πολλαπλάσιο του 8 (αφού $3^k - 1$ άρτιος) και ο αριθμός $7^k + 3^k - 2$ είναι επίσης πολλαπλάσιο του 8 από την υπόθεση της επαγωγής έπεται ότι και ο αριθμός $7^{k+1} + 3^{k+1} - 2$ είναι πολλαπλάσιο του 8. □

Παράδειγμα 2.1.5. *Να δειχθεί ότι ο αριθμός $2^{2^{-n}}$ είναι άρρητος για κάθε $n \in \mathbb{N}^*$.*

Απόδειξη. Έστω n πρόταση $\Pi(n)$: "Ο $2^{2^{-n}}$ είναι άρρητος".

i) $\Pi(1)$: Ο $2^{2^{-1}} = \sqrt{2}$ είναι άρρητος, το οποίο ισχύει.

ii) Έστω ότι ισχύει η

$$\Pi(k): \text{ Ο } 2^{2^{-k}} \text{ είναι άρρητος.}$$

Θα δείξουμε ότι ισχύει και η

$$\Pi(k+1): \text{ Ο } 2^{2^{-(k+1)}} \text{ είναι άρρητος.}$$

Πράγματι, αν $2^{2^{-(k+1)}}$ είναι ρητός, τότε υπάρχουν $a, b \in \mathbb{N}^*$ ώστε

$$2^{2^{-(k+1)}} = \frac{a}{b}.$$

Υψώνοντας κατά μέλη στο τετράγωνο προκύπτει ότι

$$\left(2^{2^{-(k+1)}}\right)^2 = \frac{a^2}{b^2}$$

ή, ισοδύναμα

$$2^{2 \cdot 2^{-(k+1)}} = 2^{2^{-k}} = \frac{a^2}{b^2},$$

το οποίο από την υπόθεση της επαγωγής είναι άτοπο, αφού ο $2^{2^{-k}}$ είναι άρρητος. Άρα, η $\Pi(k+1)$ είναι επίσης αληθής.

Επομένως, από την αρχή της επαγωγής η $\Pi(n)$ ισχύει για κάθε $n \in \mathbb{N}^*$. □

Παράδειγμα 2.1.6. *Να δειχθεί ότι η παράσταση* $(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$ *είναι θετικό ακέραιο πολλαπλάσιο του* 2 *και η παράσταση* $(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n}$ *είναι θετικό ακέραιο πολλαπλάσιο του* $\sqrt{2}$*, για κάθε* $n \in \mathbb{N}^*$.

Απόδειξη. Έστω οι προτάσεις

$\Pi(n)$: Το $(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$ είναι θετικό ακέραιο πολλαπλάσιο του 2.

$Q(n)$: Το $(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n}$ είναι θετικό ακέραιο πολλαπλάσιο του $\sqrt{2}$.

i) Για $n = 1$ ισχύει ότι

$$(1+\sqrt{2})^2 + (1-\sqrt{2})^2 = 1 + 2\sqrt{2} + 2 + 1 - 2\sqrt{2} + 2 = 6 = 3 \cdot 2$$

και

$$(1+\sqrt{2})^2 - (1-\sqrt{2})^2 = 4\sqrt{2}.$$

Άρα, οι $\Pi(1)$ και $Q(1)$ είναι αληθείς.

ii) Έστω ότι ισχύουν οι $\Pi(k)$ και $Q(k)$, δηλαδή υπάρχουν $a, b \in \mathbb{N}^*$ ώστε

$$(1+\sqrt{2})^{2k} + (1-\sqrt{2})^{2k} = a \cdot 2$$

και

$$(1+\sqrt{2})^{2k} - (1-\sqrt{2})^{2k} = b \cdot \sqrt{2}.$$

Θα δείξουμε ότι ισχύουν και οι $\Pi(k+1)$ και $Q(k+1)$.

Πράγματι,

$$\begin{aligned}(1+\sqrt{2})^{2k+2}+(1-\sqrt{2})^{2k+2} &= (1+\sqrt{2})^2(1+\sqrt{2})^{2k}+(1-\sqrt{2})^2(1-\sqrt{2})^{2k}\\ &= (3+2\sqrt{2})(1+\sqrt{2})^{2k}+(3-2\sqrt{2})(1-\sqrt{2})^{2k}\\ &= 3\left((1+\sqrt{2})^{2k}+(1-\sqrt{2})^{2k}\right)+2\sqrt{2}\left((1+\sqrt{2})^{2k}-(1-\sqrt{2})^{2k}\right)\\ &= 3a\cdot 2+2\sqrt{2}\cdot b\sqrt{2}=(3a+2b)\cdot 2,\ \text{όπου } 3a+2b\in\mathbb{N}^*.\end{aligned}$$

Επίσης,

$$\begin{aligned}(1+\sqrt{2})^{2k+2}-(1-\sqrt{2})^{2k+2} &= (1+\sqrt{2})^2(1+\sqrt{2})^{2k}-(1-\sqrt{2})^2(1-\sqrt{2})^{2k}\\ &= (3+2\sqrt{2})(1+\sqrt{2})^{2k}-(3-2\sqrt{2})(1-\sqrt{2})^{2k}\\ &= 3\left((1+\sqrt{2})^{2k}-(1-\sqrt{2})^{2k}\right)+2\sqrt{2}\left((1+\sqrt{2})^{2k}+(1-\sqrt{2})^{2k}\right)\\ &= 3\cdot b\sqrt{2}+2\sqrt{2}\cdot a\cdot 2=(3b+4a)\sqrt{2},\ \text{όπου } 3b+4a\in\mathbb{N}^*.\end{aligned}$$

Άρα, οι $\Pi(k+1)$ και $Q(k+1)$ είναι αληθείς.

Επομένως, από την αρχή της επαγωγής οι $\Pi(n)$ και $Q(n)$ είναι αληθείς για κάθε $n\in\mathbb{N}^*$. □

Παρατήρηση. Υπάρχουν περιπτώσεις όπου η $\Pi(n)$ δεν ισχύει (ή δεν έχει νόημα) για n μικρότερο από κάποιο φυσικό αριθμό ν. Τότε ξεκινάμε αποδεικνύοντας την $\Pi(\nu)$ αντί της $\Pi(1)$.

Παράδειγμα 2.1.7. *Να δειχθεί ότι*

$$\left(\frac{3}{2}\right)^n > n+1,\ \textit{για κάθε } n\geq 4.$$

Απόδειξη. Αρκεί λοιπόν τώρα, για την πρόταση $\Pi(n)$: $\left(\frac{3}{2}\right)^n > n+1$ να δείξουμε ότι:

i) $\Pi(4)$: αληθής, δηλαδή

$$\left(\frac{3}{2}\right)^4 > 4+1 \Leftrightarrow \frac{81}{16} > 5,$$

το οποίο ισχύει.

ii) Έστω ότι ισχύει η $\Pi(k)$, δηλαδή

$$\left(\frac{3}{2}\right)^k > k+1.$$

Τότε ισχύει και η $\Pi(k+1)$.

Πράγματι,

$$\left(\frac{3}{2}\right)^{k+1}=\left(\frac{3}{2}\right)^k\cdot\left(\frac{3}{2}\right) > (k+1)\frac{3}{2}=\frac{3}{2}k+\frac{3}{2}=k+\frac{k}{2}+\frac{3}{2}=k+\frac{k+3}{2}\geq k+2=k+1+1,$$

δηλαδή

$$\left(\frac{3}{2}\right)^{k+1} > (k+1)+1,$$

άρα ισχύει η $\Pi(k+1)$. □

Παράδειγμα 2.1.8. *Να δειχθεί ότι ο αριθμός $2n^3 - 3n^2 + n$ είναι πολλαπλάσιο του 6, για κάθε $n \in \mathbb{N}^*$ με $n \geq 2$.*

Απόδειξη. Αρκεί λοιπόν τώρα, για την πρόταση
$\Pi(n)$: $2n^3 - 3n^2 + n$ πολλαπλάσιο του 6,
να δείξουμε ότι:

i) $\Pi(2)$: αληθής, δηλαδή

$$2 \cdot 2^3 - 3 \cdot 2^2 + 2 = 6, \text{ πολλαπλάσιο του } 6$$

το οποίο ισχύει.

ii) Έστω ότι ισχύει η $\Pi(k)$, δηλαδή

$$2k^3 - 3k^2 + k \text{ είναι πολλαπλάσιο του } 6$$

Τότε ισχύει και η $\Pi(k+1)$, δηλαδή

$$2(k+1)^3 - 3(k+1)^2 + k + 1 \text{ είναι πολλαπλάσιο του } 6$$

Πράγματι,

$$\begin{aligned} &2(k+1)^3 - 3(k+1)^2 + k + 1 \\ &= 2\left(k^3 + 3k^2 + 3k + 1\right) - 3\left(k^2 + 2k + 1\right) + k + 1 \\ &= (2k^3 - 3k^2 + k) + 6k^2, \end{aligned}$$

το οποίο είναι πολλαπλάσιο του 6, αφού $6k^2$ είναι πολλαπλάσιο του 6 και λόγω της υπόθεσης της επαγωγής $2k^3 - 3k^2 + k$ είναι επίσης πολλαπλάσιο του 6. □

Σε ορισμένες περιπτώσεις προκειμένου να αποδείξουμε μια πρόταση μας διευκολύνει να χρησιμοποιήσουμε μια άλλη μορφή της αρχής της επαγωγής, η οποία ονομάζεται **αρχή της πλήρους επαγωγής** και διατυπώνεται ως εξής:

Πρόταση 2.2 (Αρχή της πλήρους επαγωγής). *Έστω $\Pi(n)$ μια πρόταση με $n \in \mathbb{N}^*$, για την οποία ισχύουν τα παρακάτω:*

i) Η $\Pi(1)$ είναι αληθής.

ii) Αν η $\Pi(k)$ είναι αληθής για κάθε $1 \leq k < n$, τότε και η $\Pi(n)$ είναι αληθής.

Τότε η $\Pi(n)$ είναι αληθής για κάθε $n \in \mathbb{N}^*$.

Παρατηρήσεις.

1. Αποδεικνύεται ότι η αρχή της (τελείας) επαγωγής και της πλήρους επαγωγής είναι ισοδύναμες, δηλαδή κάθε πρόταση που αποδεικνύεται με την μια μορφή της επαγωγής μπορεί να αποδειχθεί και με την άλλη μορφή της.

2. Επειδή υπάρχουν περιπτώσεις όπου η $\Pi(n)$ δεν ισχύει (ή δεν έχει νόημα) για n μικρότερο από κάποιο φυσικό αριθμό ν, και εδώ ξεκινάμε αποδεικνύοντας την $\Pi(\nu)$ αντί της $\Pi(1)$. Επιπλέον, υποθέτουμε ότι η $\Pi(k)$ είναι αληθής για κάθε $\nu \leq k < n$ αντί για $1 \leq k < n$.

Παράδειγμα 2.1.9. *Να δειχθεί ότι κάθε φυσικός αριθμός μεγαλύτερος ή ίσος του 2 είναι πρώτος ή είναι γινόμενο πρώτων αριθμών.*

Απόδειξη. Έστω η πρόταση $\Pi(n)$: "Ο n είναι πρώτος αριθμός ή είναι γινόμενο πρώτων αριθμών." Τότε,

i) $\Pi(2)$ αληθής, αφού ο αριθμός 2 είναι πρώτος αριθμός.

ii) Έστω ότι $\Pi(k)$ είναι αληθής για κάθε $2 \leq k < n$. Τότε ισχύει και η $\Pi(n)$.

Πράγματι, αν n είναι πρώτος τότε η $\Pi(n)$ ισχύει.

Αν n είναι σύνθετος τότε υπάρχουν φυσικοί αριθμοί p και q ώστε

$$n = pq \text{ όπου } 2 \leq p, q < n.$$

Επειδή $2 \leq p, q < n$, από την υπόθεση της επαγωγής ο p είτε είναι πρώτος είτε είναι γινόμενο πρώτων. Επίσης ο q είτε είναι πρώτος είτε είναι γινόμενο πρώτων. Συνεπώς, ο $pq = n$ είναι γινόμενο πρώτων.

Άρα, σε κάθε περίπτωση η $\Pi(n)$ ισχύει. □

Παράδειγμα 2.1.10. *Έστω η ακολουθία (a_n) με*

$$a_1 = 2$$
$$a_2 = 4$$
$$a_n = 3a_{\lfloor n/2 \rfloor} + 6, \text{ για κάθε } n \geq 3.$$[1]

Να δειχθεί ότι κάθε όρος της ακολουθίας (a_n) είναι άρτιος.

Απόδειξη. Έστω η πρόταση $\Pi(n)$: "Ο a_n είναι άρτιος."

i) $\Pi(1)$: αληθής, αφού $a_1 = 2$.

$\Pi(2)$: αληθής, αφού $a_2 = 4$.

ii) Έστω ότι η $\Pi(k)$ είναι αληθής για κάθε $2 \leq k < n$. Τότε ισχύει και η $\Pi(n)$.

Πράγματι, επειδή $n \geq 3$ ισχύει ότι

$$a_n = 3a_{\lfloor n/2 \rfloor} + 6.$$

Επειδή, $1 \leq \lfloor n/2 \rfloor < n$, από την υπόθεση της επαγωγής και από το γεγονός ότι a_1 είναι άρτιος, έπεται ότι $a_{\lfloor n/2 \rfloor}$ είναι άρτιος. Επομένως, $3a_{\lfloor n/2 \rfloor}$ είναι επίσης άρτιος και άρα και ο a_n είναι άρτιος. □

Παράδειγμα 2.1.11. *Έστω η ακολουθία (a_n) με*

$$a_1 = 1$$
$$a_2 = 1$$
$$a_n = a_{n-1} + a_{n-2}, \text{ για κάθε } n \geq 3.$$

[1] $\lfloor x \rfloor$ (ή $[x]$) είναι ο μέγιστος ακέραιος που είναι μικρότερος ή ίσος του x, $x \in \mathbb{R}$.

Να δειχθεί ότι a_n είναι άρτιος αν και μόνο αν το n είναι πολλαπλάσιο του 3.

Απόδειξη. Έστω η πρόταση Π(n): "Ο a_n είναι άρτιος αν και μόνο αν το n είναι πολλαπλάσιο του 3".

i) Η Π(1) ισχύει αφού το $n = 1$ δεν είναι πολλαπλάσιο του 3 και το $a_1 = 1$ είναι περιττός.

Η Π(2) ισχύει αφού το $n = 2$ δεν είναι πολλαπλάσιο του 3 και το $a_2 = 1$ είναι περιττός.

Η Π(3) ισχύει αφού το $n = 3$ είναι πολλαπλάσιο του 3 και το $a_3 = a_2 + a_1 = 1 + 1 = 2$ είναι άρτιος.

ii) Έστω ότι η πρόταση Π(k) είναι αληθής για κάθε $3 \leq k < n$. Τότε ισχύει και η Π(n).

Πράγματι, διακρίνουμε 2 περιπτώσεις:

α) Το n είναι πολλαπλάσιο του 3.

Τότε το $n - 3$ είναι επίσης πολλαπλάσιο του 3 και $1 \leq n - 3 < n$ οπότε από την υπόθεση της επαγωγής a_{n-3} είναι άρτιος. Επιπλέον,

$$a_n = a_{n-1} + a_{n-2} = (a_{n-2} + a_{n-3}) + a_{n-2} = 2a_{n-2} + a_{n-3},$$

δηλαδή ο a_n είναι άθροισμα του άρτιου $2a_{n-2}$ και του άρτιου a_{n-3}, επομένως είναι άρτιος. Άρα, στην περίπτωση αυτή η πρόταση Π(n) ισχύει.

β) Το n δεν είναι πολλαπλάσιο του 3. Στην περίπτωση αυτή, ή το $n - 1$ είναι πολλαπλάσιο του 3, ή το $n - 2$ είναι πολλαπλάσιο του 3.

Επειδή $1 \leq n - 2 < n - 1 < n$, από την υπόθεση της επαγωγής, ή το a_{n-1} είναι άρτιος και το a_{n-2} περιττός, ή το a_{n-1} είναι περιττός και το a_{n-2} είναι άρτιος. Επιπλέον

$$a_n = a_{n-1} + a_{n-2}$$

δηλαδή ο a_n είναι άθροισμα ενός άρτιου και ενός περιττού αριθμού, επομένως είναι περιττός. Άρα, στην περίπτωση αυτή η πρόταση Π(n) ισχύει.

Επομένως, η πρόταση Π(n) ισχύει σε κάθε περίπτωση.

Άρα, από την αρχή της πλήρους επαγωγής η πρόταση Π(n) ισχύει για κάθε $n \in \mathbb{N}^*$. □

Αλγεβρικές παραστάσεις

Μια αλγεβρική παράσταση αποτελείται από ορισμένες μεταβλητές που συνδέονται με τις 4 γνωστές δυαδικές πράξεις +, −, · και :

Παραδείγματα

- Μια αλγεβρική παράσταση με 1 εμφάνιση μεταβλητής είναι για παράδειγμα η $A = x_1$.
- Αλγεβρικές παραστάσεις που έχουν 2 εμφανίσεις μεταβλητών είναι οι επόμενες:

$$A = x_1 + x_2, B = x_1 - x_2, \Gamma = x_1 \cdot x_2 \text{ και } \Delta = x_1 : x_2$$

- Μια αλγεβρική παράσταση που έχει 10 εμφανίσεις μεταβλητών είναι η

$$A = (((x_1 - x_2) + (x_3 : x_4)) : (x_5 - x_6)) + (((x_7 - x_8) + x_9) \cdot x_{10})$$

Παρατηρούμε ότι σε κάθε ένα από τα προηγούμενα παραδείγματα το πλήθος των εμφανίσεων των μεταβλητών είναι κατά ένα περισσότερο από το πλήθος των εμφανίσεων των πράξεων.

Αυτό όπως θα δούμε ισχύει γενικά για κάθε αλγεβρική παράσταση. Για την απόδειξη θα χρησιμοποιηθεί η μέθοδος της πλήρους επαγωγής.

Το κρίσιμο σημείο στην απόδειξη, όπως θα δούμε είναι η διάσπαση κάθε αλγεβρικής παράστασης A με τουλάχιστον 2 μεταβλητές σε μια από τις παρακάτω μορφές:

$$A = A_1 + A_2 \text{ ή } A = A_1 - A_2 \text{ ή } A = A_1 \cdot A_2 \text{ ή } A = A_1 : A_2$$

όπου A_1, A_2 είναι αλγεβρικές παραστάσεις.

Για παράδειγμα, για την τελευταία από τις παραπάνω παραστάσεις A είναι

$$A = A_1 + A_2$$

όπου $A_1 = ((x_1 - x_2) + (x_3 : x_4)) : (x_5 - x_6)$ και $A_2 = ((x_7 - x_8) + x_9) \cdot x_{10}$

Παράδειγμα 2.1.12. *Να αποδειχθεί η πρόταση* $\Pi(n)$*: "Σε μια αλγεβρική παράσταση με* n *εμφανίσεις μεταβλητών, υπάρχουν* $n-1$ *εμφανίσεις των τεσσάρων (δυαδικών) πράξεων* $+, -, \cdot, :$*".*

Απόδειξη. Η $\Pi(1)$ προφανώς ισχύει, αφού όταν έχουμε μια μόνο εμφάνιση μεταβλητής, δεν μπορεί να υπάρξει καμιά δυαδική πράξη.

Έστω ότι η $\Pi(k)$ είναι αληθής για κάθε $1 \leq k < n$.

Θα δείξουμε ότι ισχύει η $\Pi(n)$. Πράγματι, κάθε αλγεβρική παράσταση A, με $n > 1$ εμφανίσεις μεταβλητών, θα έχει μια από τις επόμενες μορφές: $A_1 + A_2$, $A_1 - A_2$, $A_1 \cdot A_2$ και $A_1 : A_2$, όπου A_1, A_2 είναι αλγεβρικές παραστάσεις με n_1, n_2 εμφανίσεις μεταβλητών αντίστοιχα και $n_1 + n_2 = n$.

Επειδή $1 \leq n_1, n_2 < n$, από την υπόθεση της επαγωγής προκύπτει ότι η A_1 έχει $n_1 - 1$ εμφανίσεις των τεσσάρων πράξεων και ότι η A_2 έχει $n_2 - 1$ εμφανίσεις των τεσσάρων πράξεων.

Συνολικά, στην A οι εμφανίσεις των τεσσάρων πράξεων είναι ίσες με το άθροισμα των εμφανίσεων των τεσσάρων πράξεων στις A_1, A_2 συν μια επιπλέον εμφάνιση πράξης, (αυτή που συνδέει της A_1 και A_2).

Επομένως, οι εμφανίσεις των πράξεων στην A ισούνται με

$$(n_1 - 1) + (n_2 - 1) + 1 = n_1 + n_2 - 1 = n - 1,$$

δηλαδή η $\Pi(n)$ ισχύει.

Έτσι, η αλγεβρική παράσταση $(x + y) \cdot (x + w)$ έχει 4 εμφανίσεις μεταβλητών και 3 εμφανίσεις πράξεων (2 προσθέσεις και 1 πολλαπλασιασμό).

Επίσης, η αλγεβρική παράσταση $\frac{(a+b)\cdot\gamma}{(a+\gamma)\cdot(b-\delta)}$ έχει 7 εμφανίσεις μεταβλητών και 6 εμφανίσεις πράξεων (2 προσθέσεις, 1 αφαίρεση, 2 πολλαπλασιασμούς και 1 διαίρεση). □

Παράδειγμα 2.1.13. *Να δειχθεί ότι για κάθε* $n \in \mathbb{N}$*, η συνάρτηση* $\cos nx$ *είναι πολυώνυμο του* $\cos x$*.*

Λύση. Έστω η πρόταση $\Pi(n)$: "Η συνάρτηση $\cos nx$ είναι πολυώνυμο του $\cos x$".

Η $\Pi(0)$ είναι αληθής διότι $\cos 0 \cdot x = \cos 0 = 1$.

Επίσης, η $\Pi(1)$ είναι αληθής, διότι $\cos 1 \cdot x = \cos x$.

Έστω ότι η $\Pi(k)$ είναι αληθής για κάθε $k \in \{1, 2, \ldots, n-1\}$ όπου $n \geq 2$.

Θα δειχθεί ότι και η $\Pi(n)$ είναι αληθής.

Από τη σχέση

$$\cos(x+y) = \cos x \cos y - \sin x \sin y$$

έπεται ότι

$$\cos(nx) = \cos((n-1)x + x) = \cos(n-1)x \cos x - \sin(n-1)x \sin x$$

και

$$\begin{aligned}\cos((n-2)x) &= \cos((n-1)x - x)\\ &= \cos(n-1)x \cos(-x) - \sin(n-1)x \sin(-x)\\ &= \cos(n-1)x \cos x + \sin(n-1)x \sin x\end{aligned}$$

Προσθέτωντας κατά μέλη τις δύο ισότητες έχουμε ότι

$$\cos(nx) + \cos(n-2)x = 2\cos(n-1)x \cos x$$

ή, ισοδύναμα

$$\cos(nx) = 2\cos(n-1)x \cos x - \cos(n-2)x$$

Επειδή $0 \leq n-1, n-2 < n$, από την υπόθεση της επαγωγής ισχύει ότι τα $\cos(n-1)x$, $\cos(n-2)x$ είναι πολυώνυμα του $\cos x$. Επομένως, το $\cos nx$ είναι επίσης πολυώνυμο του $\cos x$ διότι προκύπτει ως διαφορά πολυωνύμων του $\cos x$. Άρα, η $\Pi(n)$ είναι επίσης αληθής.

Επομένως, από την αρχή της επαγωγής, η $\Pi(n)$ ισχύει για κάθε $n \in \mathbb{N}$. □

Η επαγωγική προσέγγιση στην επίλυση προβλημάτων

Η επαγωγική προσέγγιση σε ένα πρόβλημα αποτελείται από δύο μέρη:

Συνήθως το πρόβλημα έχει μια παράμετρο n, $n \in \mathbb{N}^*$ που εκφράζει το "μέγεθος" του προβλήματος

i) Για μικρές τιμές της παραμέτρου n γνωρίζουμε τις απαντήσεις στο πρόβλημα.

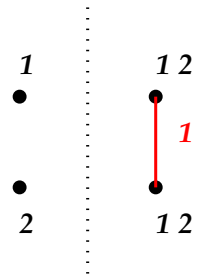
ii) Μπορούμε να λύσουμε το πρόβλημα με παράμετρο n χρησιμοποιώντας την λύση του προβλήματος με παράμετρο $n-1$, ή γενικότερα τις λύσεις του προβλήματος με παράμετρο k, όπου $k < n$.

Παράδειγμα 2.1.14. *Μια παρέα n ατόμων κουτσομπολεύουν ανά δύο μέσω τηλεφώνου. Κάθε άτομο γνωρίζει τουλάχιστον ένα κουτσομπολιό που δεν το γνωρίζουν τα υπόλοιπα άτομα. Σε μια τηλεφωνική συνομιλία μεταξύ των A και B, ο A λέει στον B όλα τα κουτσομπολιά που έχει ακούσει και ο B ανταποδίδει. Έστω a_n ο ελάχιστος αριθμός τηλεφωνικών κλήσεων που πρέπει να γίνουν μεταξύ n ατόμων, ώστε όλα τα κουτσομπολιά να είναι γνωστά στον καθένα.*

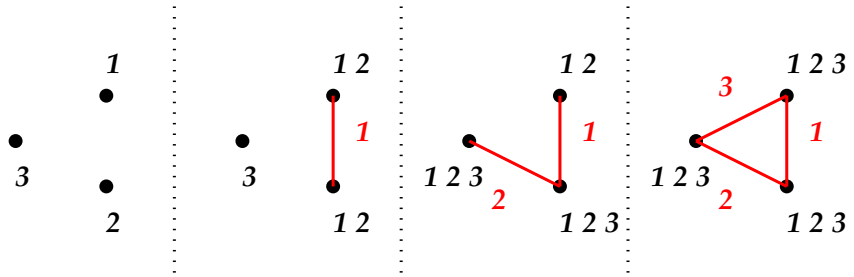
i) Να δειχθεί ότι $a_2 = 1$, $a_3 = 3$ και $a_4 = 4$.

ii) Να δειχθεί ότι $a_n \leq 2n-4$, για κάθε $n \geq 4$.

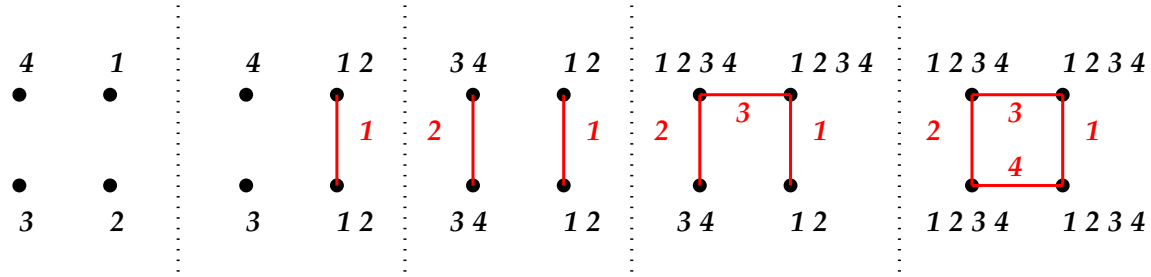
Λύση. i) Πράγματι, για $n = 2$ αρκεί ένα τηλεφώνημα.



Για $n = 3$ αρκούν τρία τηλεφωνήματα.



Για $n = 4$ αρκούν τέσσερα τηλεφωνήματα.



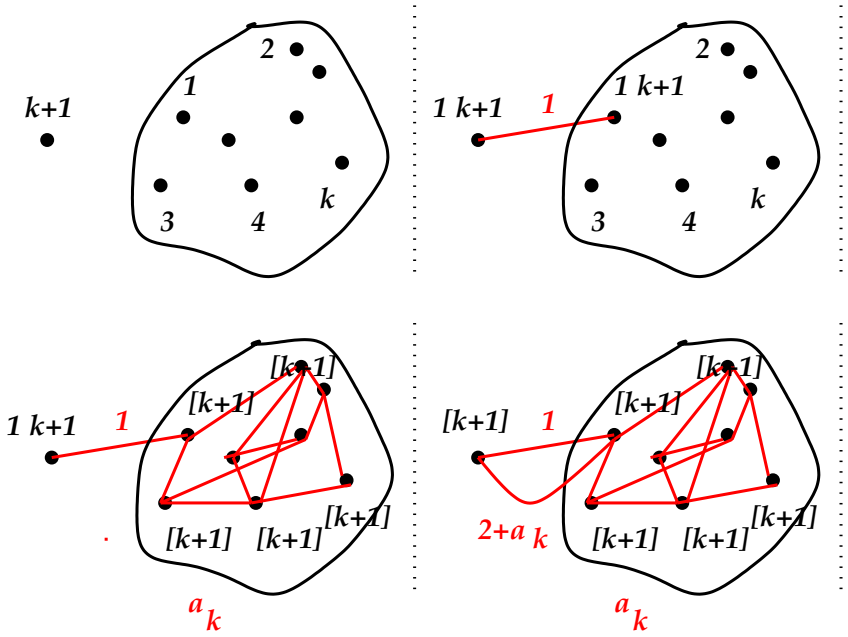
ii) Έστω η πρόταση $\Pi(n) : a_n \leq 2n - 4$.

Για $n = 4$ έχουμε ότι $a_4 = 2 \cdot 4 - 4 = 4$, άρα η $\Pi(4)$ είναι αληθής.

Έστω ότι η πρόταση $\Pi(k)$ είναι αληθής για κάποιο $k \geq 4$, δηλαδή $a_k \leq 2k - 4$.

Θα δείξουμε ότι και η πρόταση $\Pi(k+1)$ είναι αληθής, δηλαδή $a_{k+1} \leq 2(k+1) - 4$.

Πράγματι, έστω ότι έχουμε $k + 1$ άτομα. Αρχικά, το άτομο $k + 1$ επικοινωνεί με το άτομο 1 και ανταλλάσουν τα κουτσομπολιά που γνωρίζουν. Στην συνέχεια τα άτομα 1, 2, ..., k ανταλλάσουν τα κουτσομπολιά που γνωρίζουν χρησιμοποιώντας a_k κλήσεις (αγνοώντας το άτομο $k+1$). Στο τέλος, το άτομο 1 καλεί το άτομο $k+1$ και του μεταφέρει όλα τα υπόλοιπα κουτσομπολιά.



Άρα, $a_{k+1} \leq 1 + a_k + 1 \leq 1 + (2k-4) + 1 \leq 2(k+1) - 4$. □

Παράδειγμα 2.1.15. *Έστω τρεις στύλοι και n διαφορετικοί δίσκοι, όπως φαίνεται στο επόμενο σχήμα:*

Να βρεθεί πως μπορούμε να μεταφέρουμε τους n δίσκους σε άλλο στύλο, όταν μετακινούμε μόνο ένα δίσκο κάθε φορά και κανένας δίσκος δεν πρέπει να τοποθετηθεί πάνω σε μικρότερό του. Πόσες κινήσεις θα χρειαστούμε;

Λύση. Έστω a_n ο ζητούμενος αριθμός των κινήσεων που απαιτούνται όταν έχουμε να μεταφέρουμε n δίσκους.

Αν $n = 1$, τότε το πρόβλημα λύνεται άμεσα. Μετακινούμε τον μοναδικό δίσκο από τον στύλο που βρίσκεται σε ένα διαφορετικό στύλο. Άρα, $a_1 = 1$

Θα λύσουμε το πρόβλημα για $n \geq 2$ δίσκους.

Έστω ότι γνωρίζουμε να λύνουμε το πρόβλημα για $n-1$ δίσκους, τότε στην περίπτωση που έχουμε να μεταφέρουμε n δίσκους:

- Μεταφέρουμε τους $n-1$ μικρότερους δίσκους σε κάποιο άλλο στύλο (αγνοώντας τον μεγαλύτερο δίσκο).
- Έπειτα, μεταφέρουμε τον μεγαλύτερο δίσκο στον άδειο στύλο που απομένει.
- Και μεταφέρουμε τους $n-1$ μικρότερους δίσκους στον στύλο όπου βρίσκεται ο μεγαλύτερος δίσκος.

Συνολικά, θα χρειαστούμε $a_{n-1} + 1 + a_{n-1}$ κινήσεις, επομένως

$$a_n = 2a_{n-1} + 1$$

Με την βοήθεια του αναδρομικού τύπου μπορούμε να δείξουμε με επαγωγή ότι

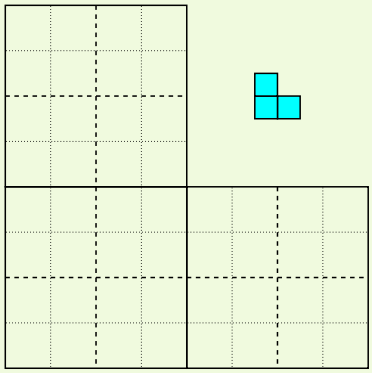
$$a_n = 2^n - 1$$

Πράγματι, για $n = 1$ έχουμε $a_1 = 2^1 - 1 = 1$ άρα ο ισχυρισμός ισχύει.
Υποθέτουμε ότι $a_k = 2^k - 1$ για κάποιο $k \geq 1$ και θα δείξουμε ότι $a_{k+1} = 2^{k+1} - 1$.
Πράγματι, χρησιμοποιώντας τον παραπάνω αναδρομικό τύπο

$$a_{k+1} = 2a_k + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 1.$$

Άρα, από την αρχή της επαγωγής ο ισχυρισμός ισχύει για κάθε $n \geq 1$. □

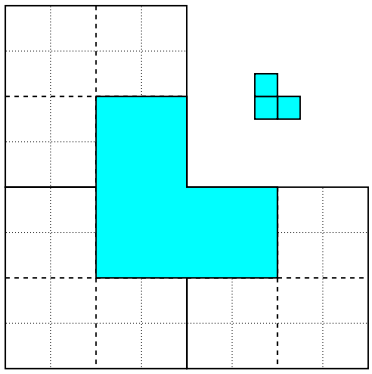
Παράδειγμα 2.1.16. *Να βρεθεί πως μπορούμε να καλύψουμε με σχήματα L-τρόμινο () μια $2^n \times 2^n$ L-τρόμινο σκακιέρα.*

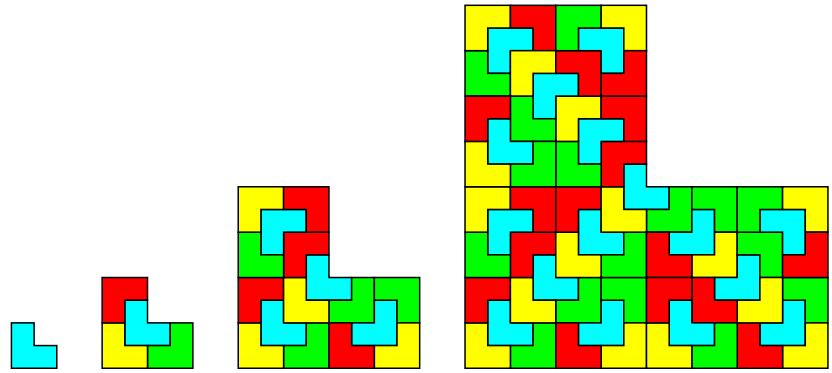


Δεν επιτρέπονται οι επικαλύψεις στα L-τρόμινο αλλά επιτρέπονται οι περιστροφές.

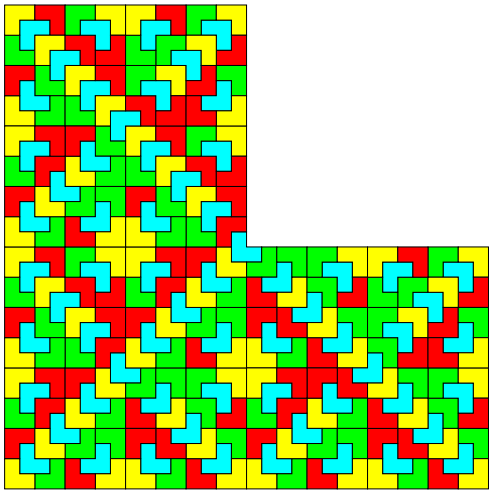
Λύση. Για $n = 1$, η κάλυψη μιας $2^1 \times 2^1$ L-τρόμινο σκακιέρας είναι προφανής.

Έστω ότι μπορούμε να καλύψουμε μια $2^n \times 2^n$ σκακιέρα. Τότε μπορούμε να καλύψουμε την $2^{n+1} \times 2^{n+1}$ σκακιέρα διαμερίζοντας την σκακιέρα σε τέσσερα $2^n \times 2^n$ τμήματα.

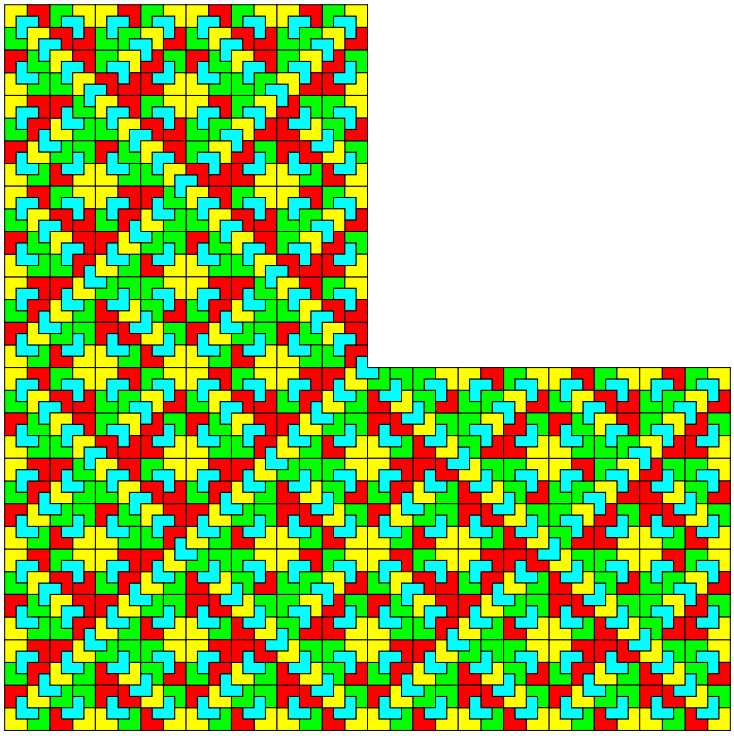




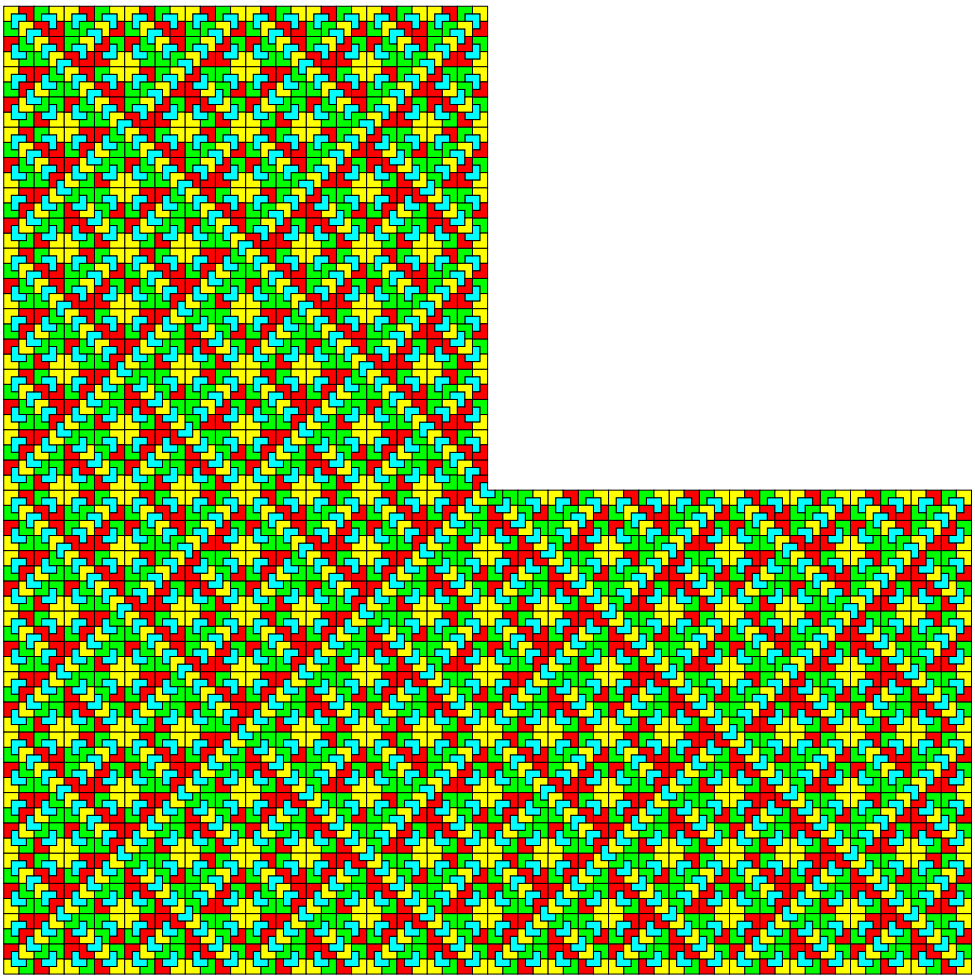
$n = 1$ $n = 2$ $n = 3$ $n = 4$



$n = 5$



$n = 6$



$n = 7$

□

Η αρχή της επαγωγής είναι ισοδύναμη με την αρχή της καλής διάταξης:

Πρόταση 2.3 (Αρχή της καλής διάταξης). *Κάθε μη κενό υποσύνολο του $\mathbb{N}^*$ έχει ελάχιστο στοιχείο.*

Χρησιμοποιώντας την αρχή της καλής διάταξης μπορούμε να αποδείξουμε την αρχή της επαγωγής. Πράγματι, έστω $\Pi(n)$ μια πρόταση με $n \in \mathbb{N}^*$, για την οποία ισχύουν τα παρακάτω:

i) Η $\Pi(1)$ είναι αληθής.

ii) Αν η $\Pi(k)$ είναι αληθής, τότε και η $\Pi(k+1)$ είναι αληθής.

Θα δείξουμε, χρησιμοποιώντας την αρχή της καλής διάταξης, ότι η $\Pi(n)$ είναι αληθής για κάθε $n \in \mathbb{N}^*$.

Απόδειξη. Έστω

$$A = \{n \in \mathbb{N}^* : \text{ Η πρόταση } \Pi(n) \text{ είναι ψευδής}\}.$$

Θα δείξουμε ότι το A είναι κενό.

Πράγματι, αν το A είναι μη κενό, τότε από την αρχή της καλής διάταξης έχει ελάχιστο στοιχείο, έστω n_0. Προφανώς, $n_0 > 1$, αφού η $\Pi(1)$ είναι αληθής.

Τότε για $k = n_0 - 1 \in \mathbb{N}^*$ η πρόταση $\Pi(k)$ είναι αληθής. Όμως, αφού η $\Pi(k)$ είναι αληθής, από την υπόθεση της επαγωγής έπεται ότι η $\Pi(k+1) = \Pi(n_0)$ είναι επίσης αληθής, το οποίο είναι άτοπο.

Άρα, το σύνολο A είναι κενό. Επομένως, η πρόταση $\Pi(n)$ αληθεύει για κάθε $n \in \mathbb{N}^*$. □

Παράδειγμα 2.1.17. *Να δειχθεί ότι ο αριθμός $\sqrt{2}$ είναι άρρητος.*

Λύση. Αν ο $\sqrt{2}$ είναι ρητός τότε υπάρχουν $a, b \in \mathbb{N}$ ώστε $\sqrt{2} = \dfrac{a}{b}$.

Έστω A το σύνολο των αριθμητών όλων των κλασμάτων $\dfrac{m}{n} = \sqrt{2}$ με $m, n \in \mathbb{N}^*$.

Επειδή $A \subseteq \mathbb{N}^*$ και $A \neq \emptyset$ από την αρχή της καλής διάταξης έπεται ότι το A έχει ελάχιστο στοιχείο. Έστω $m_0 = \min A$.

Έστω $\sqrt{2} = \frac{m_0}{n_0}$, ή ισοδύναμα $m_0^2 = 2n_0^2$.

Επειδή, m_0^2 είναι άρτιος, έπεται ότι και m_0 είναι άρτιος, άρα $m_0 = 2m_1$ όπου $m_1 \in \mathbb{N}$ και $m_1 < m_0$.

Ισοδύναμα, ισχύει ότι $(2m_1)^2 = 2n_0^2$, ή $2m_1^2 = n_0^2$.

Επειδή, n_0^2 είναι άρτιος, έπεται ότι και n_0 είναι άρτιος, άρα $n_0 = 2n_1$ όπου $n_1 \in \mathbb{N}$ και $n_1 < n_0$.

Ισοδύναμα, ισχύει ότι $2m_1^2 = (2n_1)^2$, ή $m_1^2 = 2n_1^2$, ή $\frac{m_1}{n_1} = \sqrt{2}$.

Άρα, $m_1 \in A$ με $m_1 < m_0$, το οποίο είναι άτοπο. Άρα, το σύνολο A είναι κενό, δηλαδή ο $\sqrt{2}$ είναι άρρητος. □

Παράδειγμα 2.1.18. *Να δειχθεί ότι η εξίσωση $8x^4 + 4y^4 + 2z^4 = t^4$ δεν έχει θετικές ακέραιες λύσεις (x, y, z, t).*

Λύση. Έστω A το σύνολο των θετικών φυσικών αριθμών x που εμφανίζονται στις θετικές ακέραιες λύσεις (x, y, z, t) της εξίσωσης.

Αν $A \neq \emptyset$ τότε επειδή $A \subseteq \mathbb{N}^*$ έπεται ότι το A έχει ελάχιστο στοιχείο. Έστω $m = \min A$.

Τότε υπάρχουν $a, b, c \in \mathbb{N}$ ώστε

$$8m^4 + 4a^4 + 2b^4 = c^4.$$

Από την εξίσωση έπεται ότι c^4 είναι άρτιος, άρα και ο c είναι άρτιος, δηλαδή $c = 2c_1$ όπου $c_1 \in \mathbb{N}^*$. Αντικαθιστώντας στην εξίσωση έχουμε ότι

$$8m^4 + 4a^4 + 2b^4 = 16c_1^4 \Leftrightarrow 4m^4 + 2a^4 + b^4 = 8c_1^4.$$

Επομένως, ο b^4 είναι επίσης άρτιος, δηλαδή ο b είναι άρτιος, δηλαδή $b = 2b_1$ όπου $b_1 \in \mathbb{N}^*$. Άρα,

$$4m^4 + 2a^4 + 16b_1^4 = 8c_1^4 \Leftrightarrow 2m^4 + a^4 + 8b_1^4 = 4c_1^4.$$

Ομοίως, ο a είναι άρτιος, δηλαδή $a = 2a_1$, όπου $a_1 \in \mathbb{N}^*$. Άρα,

$$2m^4 + 16a_1^4 + 8b_1^4 = 4c_1^4 \Leftrightarrow m^4 + 8a_1^4 + 4b_1^4 = 2c_1^4.$$

Επομένως, ο m είναι άρτιος, δηλαδή $m = 2m_1$, όπου $m_1 \in \mathbb{N}^*$ με $m_1 < m$. Αντικαθιστώντας στην προηγούμενη ισότητα έπεται ότι

$$16m_1^4 + 8a_1^4 + 4b_1^4 = 2c_1^4 \Leftrightarrow 8m_1^4 + 4a_1^4 + 2b_1^4 = c_1^4$$

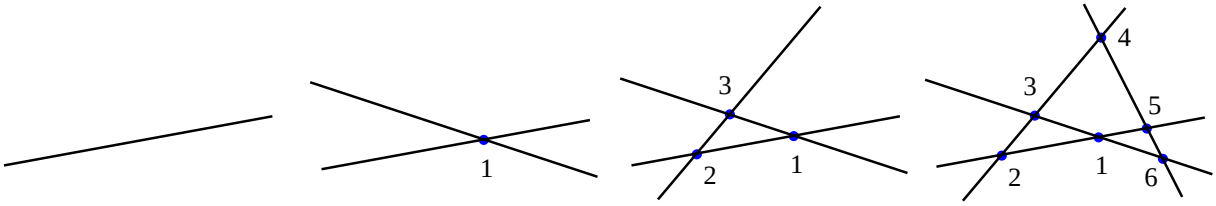
δηλαδή η τετράδα (m_1, a_1, b_1, c_1) αποτελεί λύση της εξίσωσης $8x^4 + 4y^4 + 2z^4 = t^4$, επομένως $m_1 \in A$ με $m_1 < m = \min A$. το οποίο είναι άτοπο. Άρα, $A = \emptyset$, δηλαδή η εξίσωση δεν έχει θετικές ακέραιες λύσεις. □

2.1.1 Γεωμετρικά προβλήματα απαρίθμησης

Παράδειγμα 2.1.19 (Σημεία τομής ευθειών). *Δίδονται n ευθείες ενός επιπέδου οι οποίες ανά δύο δεν είναι παράλληλες και ανά τρεις δεν διέρχονται από το ίδιο σημείο. Να ευρεθεί το πλήθος των σημείων τομών τους.*

Λύση. Έστω a_n το πλήθος των σημείων τομής των n ευθείων.

Προφανώς, $a_1 = 0$, $a_2 = 1$, $a_3 = 3$ και $a_4 = 6$



Παρατηρούμε ότι κάθε φορά που προσθέτουμε μια ευθεία αυτή τέμνει τις υπόλοιπες n σε n καινούργια σημεία δηλαδή

$$a_{n+1} = a_n + n.$$

Με τη βοήθεια αυτού του αναδρομικού τύπου και την μέθοδο της επαγωγής θα δεχθεί ότι το ζητούμενο πλήθος των σημείων τομής δίδεται από τον τύπο

$$a_n = \frac{n^2 - n}{2}.$$

Πράγματι, $a_1 = 0 = \dfrac{1^2 - 1}{2}$ δηλαδή ο τύπος ισχύει για $n = 1$.

Έστω ότι ο τύπος ισχύει για $n = k$, δηλαδή $a_k = \dfrac{k^2 - k}{2}$, θα δειχθεί ότι ο τύπος ισχύει για $n = k + 1$, δηλαδή $a_{k+1} = \dfrac{(k+1)^2 - (k+1)}{2} = \dfrac{k^2 + 2k + 1 - k - 1}{2} = \dfrac{k^2 + k}{2}$.

Είναι

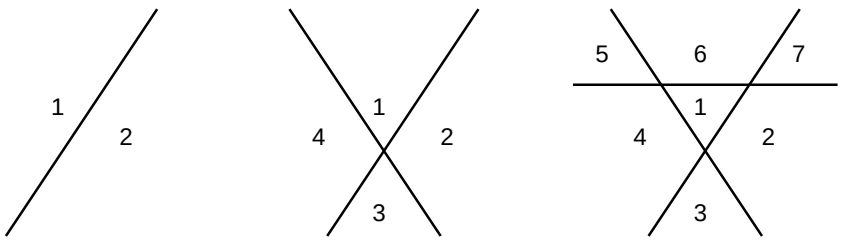
$$a_{k+1} = a_k + k = \frac{k^2 - k}{2} + k = \frac{k^2 - k + 2k}{2} = \frac{k^2 + k}{2}$$

Άρα, ο τύπος ισχύει και για $n = k + 1$, οπότε από την αρχή της επαγωγής ο τύπος ισχύει για κάθε $n \in \mathbb{N}^*$. □

Παράδειγμα 2.1.20 (**Διαμερίσεις του επιπέδου από ευθείες**). *Μια ευθεία χωρίζει το επίπεδο σε δύο περιοχές. Δύο ευθείες χωρίζουν το επίπεδο σε 4 το πολύ περιοχές. Σε πόσες το πολύ περιοχές μπορεί να χωρισθεί ένα επίπεδο από n ευθείες;*

Λύση. Έστω a_n το μέγιστο πλήθος των περιοχών που μπορεί να χωρισθεί το επίπεδο από n ευθείες.

Παρατηρούμε ότι προκειμένου να μεγιστοποιήσουμε τον αριθμο των περιοχών πρέπει να μην υπάρχουν παράλληλες ευθείες και καμία 3-άδα ευθειών να μην συντρέχει σε σημείο.



Έτσι, κάθε φορά που προσθέτουμε μια ευθεία τέμνει τις προηγούμενες n ευθείες σε n διαφορετικά σημεία και χωρίζεται σε $n+1$ ευθύγραμμα μέρη κάθε ένα από τα οποία χωρίζει μια υπάρχουσα περιοχή σε 2 μέρη.

Άρα, προκύπτει ο αναδρομικός τύπος

$$a_{n+1} = a_n + (n+1).$$

Με τη βοήθεια του αναδρομικού τύπου θα αποδείξουμε επαγωγικά ότι για κάθε $n \geq 1$ ισχύει ο τύπος

$$a_n = 1 + \frac{n(n+1)}{2}.$$

Πράγματι, έχουμε ότι $a_1 = 1 + \frac{1(1+1)}{2} = 2$, δηλαδή ο τύπος ισχύει για $n = 1$.

Έστω ότι ο τύπος ισχύει για $n = k$, δηλαδή $a_k = 1 + \frac{k(k+1)}{2}$.

Θα δείξουμε ότι ο τύπος ισχύει και για $n = k+1$. Από τον αναδρομικό τύπο έχουμε ότι

$$a_{k+1} = a_k + (k+1),$$

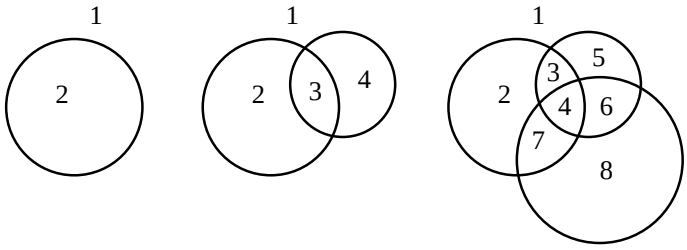
οπότε, από την επαγωγική υπόθεση για το a_k, προκύπτει ότι

$$a_{k+1} = 1 + \frac{k(k+1)}{2} + (k+1) = 1 + \frac{k(k+1) + 2(k+1)}{2} = 1 + \frac{(k+1)(k+2)}{2}.$$

Άρα, ο τύπος ισχύει και για $n = k+1$. Άρα, από την αρχή της επαγωγής ο τύπος ισχύει για κάθε $n \geq 1$. □

Παράδειγμα 2.1.21 (Διαμερίσεις του επιπέδου από κύκλους). *Να βρεθεί ο μέγιστος αριθμός περιοχών που χωρίζεται το επίπεδο από n κύκλους (συμπεριλαμβανομένης της "εξωτερικής" περιοχής) .*

Λύση. Έστω a_n ο μέγιστος αριθμός των περιοχών που χωρίζεται το επίπεδο από n κύκλους. Προφανώς, $a_1 = 2$.



Παρατηρούμε ότι προκειμένου να μεγιστοποιήσουμε τον αριθμό των περιοχών πρέπει να μην υπάρχουν κύκλοι που δεν τέμνονται καθόλου ή κύκλοι που εφάπτονται. Επίσης κάθε 3-αδα κύκλων να μην τέμνεται στα ίδια 2 σημεία.

Είναι γνωστό ότι δύο διακεκριμένοι κύκλοι μπορεί να τέμνονται το πολύ σε 2 διαφορετικά σημεία. (Δύο κύκλοι που διέρχονται από το 3 κοινά σημεία ταυτίζονται.)

Έτσι, κάθε φορά που προσθέτουμε ένα κύκλο τέμνει τους προηγούμενους n κύκλους σε $2n$ διαφορετικά σημεία και χωρίζεται σε $2n$ καμπυλόγραμμα μέρη κάθε ένα από τα οποία χωρίζει μια υπάρχουσα περιοχή σε 2 μέρη.

Άρα,

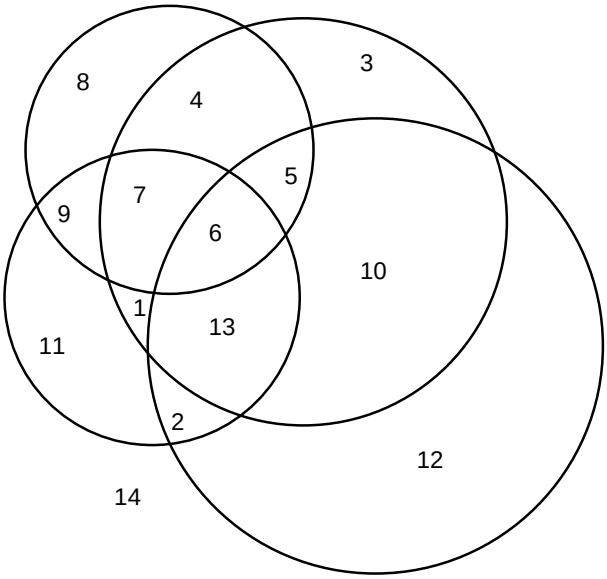
$$a_{n+1} = a_n + 2n$$

Επομένως, επαγωγικά προκύπτει (Άσκηση) ότι

$$a_n = n(n-1) + 2.$$

Σχόλιο: Από την παραπάνω άσκηση προκύπτει ότι σε ένα διάγραμμα Venn δεν μπορούμε να χρησιμοποιήσουμε μόνο κύκλους για να αναπαραστήσουμε όλα τα δυνατά 2^n υποσύνολα n συνόλων, όπου $n \geq 4$, αφού

$$a_4 = 4 \cdot 3 + 2 = 14 \neq 16 = 2^4,$$



$$a_5 = 5 \cdot 4 + 2 = 22 \neq 32 = 2^5, \text{ κ.ο.κ.}$$ □

2.1.2 Ασκήσεις προς επίλυση

1) Να δειχθεί ότι:

i) $1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$, για κάθε $n \in \mathbb{N}$.

ii) $\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$, για κάθε $n \in \mathbb{N}^*$.

iii) $\frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}$, για κάθε $n \in \mathbb{N}^*$.

iv) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, για κάθε $n \in \mathbb{N}^*$.

v) $1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$, για κάθε $n \in \mathbb{N}^*$.

vi) $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$, για κάθε $n \in \mathbb{N}^*$.

vii) $1 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$, για κάθε $n \in \mathbb{N}^*$.

viii) $1^5 + 2^5 + \cdots + n^5 + 1^7 + 2^7 + \cdots + n^7 = 2(1^3 + 2^3 + \cdots + n^3)^2$, για κάθε $n \in \mathbb{N}^*$.

ix) $1 + 3 + 5 + \cdots + (2n-1) = n^2$, για κάθε $n \in \mathbb{N}^*$.

x) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$, για κάθε $n \in \mathbb{N}^*$.

xi) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$, για κάθε $n \in \mathbb{N}^*$.

xii) $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots n \cdot n! = (n+1)! - 1$, για κάθε $n \in \mathbb{N}^*$.

xiii) $\frac{1 \cdot 2!}{2} + \frac{2 \cdot 3!}{2^2} + \cdots + \frac{n \cdot (n+1)!}{2^n} = \frac{(n+2)!}{2^n} - 2$, για κάθε $n \in \mathbb{N}^*$.

xiv) $\frac{1 \cdot d!}{d} + \frac{2 \cdot (d+1)!}{d^2} + \cdots + \frac{n \cdot (n+d-1)!}{d^n} = \frac{(n+d)!}{d^n} - d!$, για κάθε $n \in \mathbb{N}^*$ και $d \in \mathbb{N}^*$.

xv) $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$, για κάθε $n \in \mathbb{N}^*$.

xvi) $\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \frac{1}{7 \cdot 10} + \cdots + \frac{1}{(3n-2)(3n+1)} = \frac{n}{3n+1}$, για κάθε $n \in \mathbb{N}^*$.

xvii) $\frac{1}{a(a+1)} + \frac{1}{(a+1)(a+2)} + \cdots + \frac{1}{(a+n-1)(a+n)} = \frac{n}{a(a+n)}$, για κάθε $n \in \mathbb{N}^*$ και $-a \notin \mathbb{N}$.

xviii) $\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$, για κάθε φυσικό αριθμό $n \geq 2$.

xix) $\frac{(n+1)(n+2) \cdots (2n-1)2n}{1 \cdot 3 \cdot 5 \cdots (2n-1)} = 2^n$, για κάθε $n \in \mathbb{N}^*$.

xx) $\left(1 + \frac{1}{1}\right)^1 \cdot \left(1 + \frac{1}{2}\right)^2 \cdot \left(1 + \frac{1}{3}\right)^3 \cdots \left(1 + \frac{1}{n-1}\right)^{n-1} = \frac{n^{n-1}}{(n-1)!}$, για κάθε $n \geq 2$.

xxi) $\left(1 + \frac{1}{1}\right)^2 \cdot \left(1 + \frac{1}{2}\right)^3 \cdot \left(1 + \frac{1}{3}\right)^4 \cdots \left(1 + \frac{1}{n-1}\right)^n = \frac{n^n}{(n-1)!}$, για κάθε $n \geq 2$.

xxii) $\frac{1}{1} + \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 2 \cdot 3} + \cdots + \frac{1}{1 \cdot 2 \cdot 3 \cdots n} \leq \frac{2n-1}{n}$, για κάθε $n \geq 3$.

xxiii) $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$, για κάθε φυσικό αριθμό $n \geq 1$.

xxiv) $1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}\geq\sqrt{n}$, για κάθε $n\in\mathbb{N}^*$.

xxv) $\sum_{k=1}^{n}\frac{5}{2k-1}\leq n+\frac{14}{3}$, για κάθε $n\in\mathbb{N}^*$.

xxvi) $\frac{2}{1\cdot 3}+\frac{2}{5\cdot 7}+\cdots+\frac{2}{(4n+1)(4n+3)}\leq 1$, για κάθε $n\in\mathbb{N}$.

xxvii) $\sum_{k=1}^{n}\frac{1}{(k+1)\sqrt{k}}<2-\frac{2}{\sqrt{n+1}}$ για κάθε $n\in\mathbb{N}^*$.

xxviii) $\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}<\frac{5}{2}-\frac{1}{n}$, για κάθε $n\in\mathbb{N}^*$.

xxix) $\frac{a^n+b^n}{2}\geq\left(\frac{a+b}{2}\right)^n$ για κάθε $n\in\mathbb{N}$ και $a,b>0$.

xxx) $(n-1)a^n+b^n\geq na^{n-1}b$ για κάθε $n\in\mathbb{N}$ και $a,b>0$.

xxxi) $n^{n+1}>(n+1)^n$ για κάθε $n\geq 3$.

2) Να δειχθεί ότι

$$a^n-b^n=(a-b)\sum_{k=1}^{n}a^{n-k}b^{k-1},$$

για κάθε $n\in\mathbb{N}^*$ και $a,b\in\mathbb{R}^*$.

3) Να δειχθεί ότι

i) $(1+\alpha)^n>1+n\alpha$, για κάθε $n\geq 2$, όπου $\alpha>-1$ και $\alpha\neq 0$. (**Ανισότητα Bernoulli**)

ii) $(1+\alpha)^n\geq 1+n\alpha+\frac{n(n-1)}{2}\alpha^2$, για κάθε $n\in\mathbb{N}$, όπου $\alpha>0$,

iii) $(1+\alpha)^n\leq 1+na+\frac{n(n-1)}{2}\alpha^2$, για κάθε $n\in\mathbb{N}$, όπου $-1<\alpha<0$.

iv) $(1+\alpha)^n<\frac{1}{1-n\alpha}$, για κάθε $n\geq 2$ και $0<\alpha<\frac{1}{n}$.

4) i) Να δειχθεί ότι αν $a>b>0$ και $p,q\in\mathbb{N}^*$ τότε $a^{\frac{p}{q}}>b^{\frac{p}{q}}$.

ii) Να δειχθεί ότι

$$\frac{1}{\sqrt{4n+1}}<\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdots\frac{2n-3}{2n-2}\cdot\frac{2n-1}{2n}<\frac{1}{\sqrt{3n+1}},$$

για κάθε $n\in\mathbb{N}^*$.

5) Έστω $x\in\mathbb{R}$ τέτοιο ώστε $x+\frac{1}{x}\in\mathbb{Z}$. Να δειχθεί ότι για κάθε $n\in\mathbb{N}$ ισχύει ότι $x^n+\frac{1}{x^n}\in\mathbb{Z}$.

(Υπόδειξη: Αν $a_n=x^n+\frac{1}{x^n}$, τότε $a_{n+1}=a_1a_n-a_{n-1}$.)

6) i) Να υπολογισθεί το άθροισμα $\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}$, όπου $n\in\mathbb{N}$.

ii) Να υπολογισθεί το γινόμενο $\left(1-\frac{4}{9}\right)\left(1-\frac{4}{16}\right)\left(1-\frac{4}{25}\right)\cdots\left(1-\frac{4}{n^2}\right)$, όπου $n\geq 3$.

iii) Να υπολογισθεί το άθροισμα $1 \cdot 3 + 3 \cdot 5 + \cdots + (2n-1)(2n+1)$, όπου $n \in \mathbb{N}^*$.

iv) Να υπολογισθεί το άθροισμα $\dfrac{1 \cdot 3!}{3} + \dfrac{2 \cdot 4!}{3^2} + \cdots + \dfrac{n(n+2)!}{3^n}$, όπου $n \in \mathbb{N}^*$.

7) Έστω a_1, a_2, …, a_n μια μετάθεση των αριθμών $1, 2, \ldots, n$, όπου $n \in \mathbb{N}^*$. Να δειχθεί ότι

i) $\dfrac{a_1}{1} + \dfrac{a_2}{2} + \dfrac{a_3}{3} + \cdots + \dfrac{a_n}{n} \geq n.$

ii) $\dfrac{1}{a_1} + \dfrac{2}{a_2} + \dfrac{3}{a_3} + \cdots + \dfrac{n}{a_n} \geq n.$

8) Για κάθε $n, k \in \mathbb{N}^*$ ορίζουμε $S_k(n) = 1^k + 2^k + \cdots + n^k$. Να δειχθεί ότι για κάθε $n, k \in \mathbb{N}^*$ ισχύει ότι

$$2^{k-1}(S_1(n))^k = \sum_{j=1}^{\lfloor \frac{k+1}{2} \rfloor} \binom{k}{2j-1} S_{2k-j}(n).$$

9) i) Αν $a_1 = 2$, $a_2 = 3$ και $a_n = 3a_{n-1} - 2a_{n-2}$ για κάθε $n \geq 3$, να δειχθεί ότι $a_n = 2^{n-1} + 1$ για κάθε $n \in \mathbb{N}^*$.

ii) Αν $a_0 = 2$, $a_1 = 5$ και $a_{n+2} = 5a_{n+1} - 6a_n$, να δειχθεί ότι $a_n = 2^n + 3^n$, για κάθε $n \in \mathbb{N}$.

iii) Μια ακολουθία $(a_n)_{n \in \mathbb{N}^*}$ ορίζεται από τη σχέση $a_{n+3} = 3a_{n+2} - 3a_{n+1} + a_n$, για κάθε $n \geq 4$, όπου $a_1 = 0$, $a_2 = 1$ και $a_3 = 4$. Να δειχθεί ότι $a_n = (n-1)^2$, για κάθε $n \in \mathbb{N}^*$.

iv) Έστω ότι $a_1 = 1$ και $a_{n+1} = a_n + 8n$ για κάθε $n \geq 1$. Να δειχθεί ότι $a_n = (2n-1)^2$, για κάθε $n \in \mathbb{N}^*$.

v) Η ακολουθία (x_n) ορίζεται από τις σχέσεις $x_1 = 1$, $x_2 = 2$ και $x_n = (n-1)(x_{n-1} + x_{n-2})$. Να δειχθεί ότι $x_n = n!$, για κάθε $n \in \mathbb{N}^*$.

vi) Μια ακολουθία $(a_n)_{n \in \mathbb{N}^*}$ ορίζεται από τη σχέση $a_n = a_{n-1} + a_{n-2}$, για κάθε $n \geq 3$, όπου $a_1 = 1$, $a_2 = 1$. Να δειχθεί ότι $a_n < 2^n - 1$, για κάθε $n \geq 2$.

vii) Μια ακολουθία $(a_n)_{n \in \mathbb{N}^*}$ ορίζεται από τη σχέση $a_n = a_{n-1} + a_{n-2} + a_{n-3}$, για κάθε $n \geq 4$, όπου $a_1 = 1$, $a_2 = 2$ και $a_3 = 3$. Να δειχθεί ότι $a_n < 2^n$, για κάθε $n \in \mathbb{N}^*$.

viii) Έστω ότι $a_0 = 1$ και για $n \geq 1$ ισχύει ότι $a_n = \sum_{i=0}^{n-1} 2a_i$. Να δειχθεί ότι $a_n = 2 \cdot 3^{n-1}$ για κάθε $n \geq 1$.

10) i) Να δειχθεί ότι για κάθε $n \in \mathbb{N}$, η συνάρτηση $\cos nx$ είναι πολυώνυμο του $\cos x$.
(Υπόδειξη: Να χρησιμοποιηθούν οι σχέσεις $\cos(n+1)x = \cos nx \cos x - \sin nx \sin x$ και $\cos(n-1)x = \cos nx \cos x + \sin nx \sin x$.) (Για τη λύση βλέπε Παράδειγμα 2.1.13.)

ii) Να δειχθεί ότι για κάθε $n \in \mathbb{N}$, η συνάρτηση $\dfrac{\sin nx}{\sin x}$ είναι πολυώνυμο του $\cos x$.

iii) Να δειχθεί ότι $\dfrac{1}{2} + \cos x + \cos 2x + \cos 3x + \cdots + \cos nx = \dfrac{\sin\left(n + \frac{1}{2}\right)x}{2 \sin \frac{x}{2}}$, για κάθε $n \in \mathbb{N}$ και για κάθε $x \in \mathbb{N}$ με $\sin \frac{x}{2} \neq 0$.

11) Να δειχθεί ότι $\underbrace{\sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}_{n \text{ ριζικά}} = 2 \cos \dfrac{\pi}{2^{n+1}}$ για κάθε $n \in \mathbb{N}^*$.

12) i) Να δειχθεί ότι για κάθε n-άδα θετικών αριθμών $x_1, x_2, \ldots, x_n$ με $x_1 x_2 \cdots x_n = 1$, ισχύει ότι $x_1 + x_2 + \cdots + x_n \geq n$.

ii) Να δειχθεί ότι για κάθε n-άδα θετικών αριθμών $x_1, x_2, \ldots, x_n$ με $x_1 x_2 \cdots x_n = 1$, ισχύει ότι $(1 + x_1)(1 + x_2) \cdots (1 + x_n) \geq 2^n$.

13) Να δειχθεί ότι μπορούμε να δημιουργήσουμε οποιοδήποτε ταχυδρομικό τέλος μεγαλύτερο ή ίσο των 8 λεπτών χρησιμοποιώντας μόνο γραμματόσημα των 3 και 5 λεπτών.

(Για παράδειγμα, μπορούμε να δημιουργήσουμε το ταχυδρομικό τέλος των 13 λεπτών χρησιμοποιώντας 2 γραμματόσημα των 5 λεπτών και 1 γραμματόσημο των 3 λεπτών.)

14) Να δειχθεί ότι μπορούμε να πληρώσουμε οποιοδήποτε πολλαπλάσιο των 10 ευρώ και μεγαλύτερο ή ίσο των 40 ευρώ, χρησιμοποιώντας μόνο χαρτονομίσματα των 20 και 50 ευρώ.

15) i) Να δειχθεί ότι ο αριθμός $n^3 - n$ είναι πολλαπλάσιο του 3 για κάθε $n \in \mathbb{N}$. (Υπόδειξη: $(n + 1)^3 = n^3 + 3n^2 + 3n + 1$.)

ii) Να δειχθεί ότι ο αριθμός $n^3 + (n+1)^3 + (n+2)^3$ είναι πολλαπλάσιο του 9, για κάθε $n \in \mathbb{N}^*$.

iii) Να δειχθεί ότι ο αριθμός $5^n - 1$ διαιρείται από το 4, για κάθε $n \in \mathbb{N}$.

iv) Να δειχθεί ότι ο αριθμός $7^n + 4^n + 1$ διαιρείται με το 6, για κάθε $n \in \mathbb{N}^*$.

v) Να δειχθεί ότι ο αριθμός $4^n + 15n - 1$ διαιρείται από το 9, για κάθε $n \in \mathbb{N}$.

∗16) Να δειχθεί ότι για κάθε $n \geq 3$, το προτελευταίο ψηφίο του 3^n είναι άρτιο.

17) i) Να δειχθεί ότι για την ακολουθία συναρτήσεων $(f_n(x))$ με $f_1(x) = 2x + 1$ και $f_n(x) = f_1(f_{n-1}(x))$ ισχύει ότι

$$f_n(x) = 2^n x + 2^n - 1, \text{ για κάθε } n \in \mathbb{N}^*.$$

ii) Να βρεθεί ο τύπος της $g_n(x)$ για την ακολουθία συναρτήσεων $(g_n(x))$ όπου $g_1(x) = \frac{4x-3}{2x+1}$ και $g_n(x) = g_1(g_{n-1}(x))$ για κάθε $n \geq 2$.

iii) Έστω μια ακολουθία συναρτήσεων $(f_n(x))$ με $f_0(x) = x$, $f_{n+1}(x) = 4f_n(x)(1 - f_n(x))$ για κάθε $n \in \mathbb{N}$. Να δειχθεί ότι $\displaystyle\int_0^1 f_n(x)dx = \frac{2^{2n-1}}{2^{2n} - 1}$ για κάθε $n \in \mathbb{N}^*$. (Υπόδειξη. $x = \sin^2 \theta$.)

iv) Να δειχθεί ότι για την ακολουθία συναρτήσεων $(f_n(x))$ με $f_1(x) = 2x^2 - 1/[-1, 1] \to [-1, 1]$ και $f_n(x) = f_1(f_{n-1}(x))$ ισχύει ότι

$$f_n(x) = \cos(2^n \arccos(x)), \text{ για κάθε } n \in \mathbb{N}^*.$$

(Υπόδειξη. $f_1(x) = (\phi \circ g \circ \phi^{-1})(x)$, όπου $\phi(x) = \cos(x)$, $g(x) = 2x$.)

18) Έστω μια σειρά n ατόμων, όπου $n \geq 2$. Αν το πρώτο άτομο της σειράς είναι γυναίκα και το τελευταίο άτομο της σειράς είναι άνδρας, να δειχθεί ότι υπάρχει στη σειρά τουλάχιστον μια γυναίκα ακριβώς μπροστά από έναν άνδρα.

19) Έστω X πεπερασμένο σύνολο με n στοιχεία, $n \in \mathbb{N}$. Να δειχθεί ότι ο αριθμός των υποσύνολων του X ισούται με 2^n.

20) Να βρεθεί που είναι το σφάλμα στην επόμενη "επαγωγική απόδειξη".

Πρόταση Όλα τα τριαντάφυλλα έχουν το ίδιο χρώμα.

Απόδειξη. Θα χρησιμοποιηθεί επαγωγή ως προς τον αριθμό n των τριαντάφυλλων.

Έστω η πρόταση $\Pi(n)$: "Σε κάθε σύνολο με n τριαντάφυλλα όλα έχουν το ίδιο χρώμα."

Η $\Pi(1)$ είναι προφανώς αληθής.

Έστω ότι η $\Pi(k)$ είναι αληθής, δηλαδή σε κάθε σύνολο με k τριαντάφυλλα όλα έχουν το ίδιο χρώμα. Θα αποδειχθεί ότι και η $\Pi(k+1)$ είναι αληθής.

Έστω $\{r_1, r_2, \ldots, r_k, r_{k+1}\}$ είναι ένα σύνολο με k+1 τριαντάφυλλα. Τότε τα υποσύνολα $\{r_1, r_2, \ldots, r_k\}$ και $\{r_2, \ldots, r_k, r_{k+1}\}$ περιέχουν k τριαντάφυλλα, επομένως, από την υπόθεση της επαγωγής, σε κάθε σύνολο όλα τα τριαντάφυλλα έχουν το ίδιο χρώμα. Επειδή το r_2 ανήκει και στα δύο σύνολα, έπεται όλα τα τριαντάφυλλα έχουν το ίδιο χρώμα, άρα η $\Pi(k+1)$ είναι αληθής. □

21) Να βρεθεί που είναι το σφάλμα στην παρακάτω "επαγωγική απόδειξη":

Πρόταση Για κάθε $n \in \mathbb{N}$ ισχύει ότι $2^n = 1$.

Απόδειξη. Θα χρησιμοποιηθεί επαγωγή ως προς τον αριθμό n.

Έστω η πρόταση $\Pi(n)$: "$2^n = 1$."

Η $\Pi(0)$ είναι προφανώς αληθής, αφού $2^0 = 1$.

Έστω ότι η $\Pi(k)$ είναι αληθής για κάθε $k < n$, δηλαδή $2^k = 1$ για κάθε $k < n$.

Θα αποδειχθεί ότι και η $\Pi(n)$ είναι αληθής.

Πράγματι,

$$2^n = \frac{2^{n-1} \cdot 2^{n-1}}{2^{n-2}} = \frac{1 \cdot 1}{1} = 1,$$

άρα, η $\Pi(n)$ είναι επίσης αληθής, δηλαδή η πρόταση $\Pi(n)$ ισχύει για κάθε $n \in \mathbb{N}$. □

22) Να βρεθεί που είναι το σφάλμα στην παρακάτω "επαγωγική απόδειξη":

Πρόταση Για κάθε $n \in \mathbb{N}$ ισχύει ότι $2n = 0$.

Απόδειξη. Θα χρησιμοποιηθεί επαγωγή ως προς τον αριθμό n.

Έστω η πρόταση $\Pi(n)$: "$2n = 0$."

Η $\Pi(0)$ είναι προφανώς αληθής, αφού $2 \cdot 0 = 0$.

Έστω ότι η $\Pi(k)$ είναι αληθής για κάθε $k < n$, δηλαδή $2k = 0$ για κάθε $k < n$.

Θα αποδειχθεί ότι και η $\Pi(n)$ είναι αληθής.

Πράγματι, έστω $n = x + y$ όπου $x, y < n$, τότε

$$2n = 2(x + y) = 2x + 2y = 0 + 0 = 0,$$

άρα, η $\Pi(n)$ είναι επίσης αληθής, δηλαδή η πρόταση $\Pi(n)$ ισχύει για κάθε $n \in \mathbb{N}$. □

23) Να αποδειχθεί ότι σε μια παράσταση συνόλων, (όπου οι πράξεις που χρησιμοποιούμε είναι η ένωση, η τομή και το συμπλήρωμα) ισχύει ότι αν υπάρχουν n εμφανίσεις μεταβλητών, τότε υπάρχουν τουλάχιστον $n - 1$ εμφανίσεις πράξεων.

24) i) Να δειχθεί ότι το άθροισμα των γωνιών ενός κυρτού n-γώνου ισούται με $(n-2)\pi$.

ii) Να δειχθεί ότι ο αριθμός a_n των διαγωνίων που ορίζουν οι κορυφές ενός κυρτού n-γώνου ισούται με $a_n = \dfrac{n(n-3)}{2}$.

25) Έστω ότι για μια πρόταση $\Pi(n)$ μπορούμε να αποδείξουμε ότι αν η $\Pi(k)$ είναι αληθής, τότε και η $\Pi(k+3)$ είναι επίσης αληθής. Τι πρέπει να ισχύει έτσι ώστε η $\Pi(n)$ να είναι αληθής για κάθε $n \in \mathbb{N}$;

26) i) Να δοθεί μια πρόταση $\Pi(n)$ η οποία είναι ψευδής για κάθε $n \in \mathbb{N}^*$ αλλά για την οποία ισχύει το επαγωγικό βήμα, δηλαδή η συνεπαγωγή ότι αν η $\Pi(n)$ είναι αληθής, τότε και η $\Pi(n+1)$ είναι επίσης αληθής.

ii) Να δοθεί μια πρόταση $\Pi(n)$ η οποία είναι αληθής για κάθε φυσικό αριθμό n μέχρι τα 2 εκατομμύρια, αλλά είναι ψευδής για κάθε n μεγαλύτερο από τα 2 εκατομμύρια.

27) Έστω απεικονίσεις $f, g : \mathbb{N}^* \to \mathbb{N}^*$ οι οποίες ορίζονται αναδρομικά ως εξής:

$$\begin{aligned} f(1) &= 1, \\ f(n+1) &= f(n) + 2n + 1, \text{ για κάθε } n \in \mathbb{N}^*, \end{aligned}$$

και

$$\begin{aligned} g(1) &= 1, \\ g(2) &= 4, \\ g(n+1) &= \frac{(g(n)-1)^2}{g(n-1)}, \text{ για κάθε } n \geq 1. \end{aligned}$$

Να δειχθεί ότι $f(n) = g(n)$, για κάθε $n \in \mathbb{N}^*$.

∗28) Έστω απεικονίσεις $f : \mathbb{N} \to \mathbb{N}^*$ και $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ οι οποίες ορίζονται αναδρομικά ως εξής:

$$\begin{aligned} f(0) &= 1, \\ f(n) &= nf(n-1), \text{ για κάθε } n \in \mathbb{N}^*, \end{aligned}$$

και

$$g(n,m) = \begin{cases} m, & \text{αν } n = 0 \\ g(n-1, nm), & \text{αν } n > 0. \end{cases}$$

Να δειχθεί ότι $f(n) = g(n,1)$, για κάθε $n \in \mathbb{N}$.

29) i) Η συνάρτηση $S : \mathbb{N}^* \to \mathbb{N}^*$ ορίζεται αναδρομικά ως εξής:

$$S(n) = \begin{cases} n + 10, & \text{αν } n < 100 \\ S(S(n-11)), & \text{αν } n \geq 100. \end{cases}$$

α) Να βρεθούν οι τιμές $S(99)$, $S(100)$, $S(102)$ και $S(120)$.

β) Να δειχθεί ότι $S(n) = 109$ για κάθε $n \geq 99$.

∗ii) Η συνάρτηση McCarthy $M : \mathbb{N}^* \to \mathbb{N}^*$ ορίζεται αναδρομικά ως εξής:

$$M(n) = \begin{cases} n - 10, & \text{αν } n > 100 \\ M(M(n+11)), & \text{αν } n \leq 100. \end{cases}$$

α) Να βρεθούν οι τιμές $M(102)$, $M(101)$, $M(99)$, $M(97)$, $M(87)$ και $M(76)$.

β) Να δειχθεί ότι $M(n) = 91$ για κάθε $n \leq 101$.

30) Η συνάρτηση Ackermann $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ορίζεται αναδρομικά ως εξής:

$$A(m,n) = \begin{cases} n+1, & \text{αν } m = 0 \\ A(m-1,1), & \text{αν } n = 0 \\ A(m-1, A(m,n-1)), & \text{αν } m,n > 0. \end{cases}$$

i) Να βρεθούν οι τιμές $A(0,1)$, $A(1,1)$, $A(2,2)$ και $A(2,3)$.

∗ii) Να δειχθεί ότι για κάθε $n \geq 0$ ισχύει ότι
$A(1,n) = n+2$,
$A(2,n) = 2n+3$,
$A(3,n) = 2^{n+3} - 3$.

∗31) Έστω μια συνάρτηση $f : \mathbb{N}^* \to \mathbb{N}^*$ με την ιδιότητα

$$f(n+1) > f(f(n)), \text{ για κάθε } n \in \mathbb{N}^*.$$

i) Να δειχθεί ότι $f(n) \geq n$, για κάθε $n \in \mathbb{N}^*$.

ii) Να δειχθεί ότι $f(n) = n$, για κάθε $n \in \mathbb{N}^*$.

∗32) Ο ξενώνας της Μουσικής Σχολής έχει έναν διάδρομο απείρου μήκους και άπειρο πλήθος δωματίων στη μια πλευρά του διαδρόμου. Τα δωμάτια είναι αριθμημένα στην σειρά με ακέραιους αριθμούς, και σε κάθε δωμάτιο υπάρχει ένα πιάνο με ουρά. Ένας πεπερασμένος αριθμός φοιτητών μένει σ' αυτά τα δωμάτια (αρκετοί φοιτητές μπορεί να μένουν στο ίδιο δωμάτιο). Κάθε μέρα δύο φοιτητές που μένουν σε γειτονικά δωμάτια, το k και το $k+1$, ενοχλούνται ο ένας από την μουσική του άλλου και μετακομίζουν, στο $(k-1)$ και στο $(k+2)$ δωμάτιο.

i) Να δειχθεί ότι αν ένας φοιτητής έμενε σε ένα από τα τρία δωμάτια $k-1$, k, $k+1$, τότε τουλάχιστον ένα από αυτά τα δωμάτια θα κατοικείται οποιαδήποτε από τις επόμενες μέρες.

ii) Να δειχθεί ότι αν ένας φοιτητής έμενε στο δωμάτιο k δεν μπορεί να μετακινηθεί σε δωμάτιο με αριθμό μεγαλύτερο από το $k+3m$ και μικρότερο από το $k-3m$, όπου m ο αριθμός των φοιτητών.

iii) Να δειχθεί ότι το άθροισμα των τετραγώνων των αριθμών των δωματίων που κατοικεί κάθε φοιτητής αυξάνει σε κάθε μετακόμιση.

iv) Να δειχθεί ότι οι κινήσεις σταματούν έπειτα από πεπερασμένο αριθμό ημερών.

33) Να δειχθεί, με τη χρήση επαγωγής, ότι κάθε πεπερασμένο μη κενό σύνολο φυσικών αριθμών έχει ελάχιστο στοιχείο.

34) Να δειχθεί ότι η εξίσωση $x^2 + y^2 + z^2 + t^2 = 2xyzt$ δεν έχει θετικές ακέραιες λύσεις.

2.1.3 Παράρτημα: Αναδρομικοί (επαγωγικοί) ορισμοί στο $\mathbb{N}$

Η αναδρομή θεωρείται μια από τις σημαντικότερες τεχνικές στην επιστήμη των υπολογιστών.

Μια συνάρτηση f με πεδίο ορισμού το σύνολο των φυσικών αριθμών $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ ονομάζεται ακολουθία.

Για παράδειγμα η συνάρτηση $f(n) : \mathbb{N} \to \mathbb{R}$ με τύπο

$$f(n) = 3^n$$

είναι μια ακολουθία με τιμές

$$f(0) = 3^0 = 1, f(1) = 3^1 = 3, f(2) = 3^2 = 9, f(3), = 3^3 = 27, \ldots$$

Για κάθε $n \in \mathbb{N}$ η τιμή ακολουθίας f υπολογίζεται από τον τύπο $f(n) = 3^n$.

Συγκρίνοντας τις τιμές της συνάρτησης f για δύο διαδοχικούς αριθμούς n, $n+1$ παρατηρούμε ότι

$$f(n+1) = 3^{n+1} = 3 \cdot 3^n = 3 \cdot f(n)$$

Η παρατήρηση αυτή μας δίνει έναν εναλλακτικό τρόπο υπολογισμού των τιμών της ακολουθίας f για κάθε φυσικό αριθμό n, χρησιμοποιώντας τους επόμενους δυο κανόνες:

$$f(0) = 1$$

$$f(n+1) = 3 \cdot f(n), \text{ για κάθε } n \geq 0$$

Για παράδειγμα, η τιμή $f(4)$ υπολογίζεται ως εξής:

$$f(4) = 3 \cdot f(3) = 3 \cdot (3 \cdot f(2)) = 3^2 \cdot f(2) = 3^3 \cdot f(1) = 3^4 \cdot f(0) = 3^4 \cdot 1 = 3^4 = 81.$$

Ο εναλλακτικός τρόπος υπολογισμού των τιμών της f ονομάζεται **αναδρομικός** διότι για τον υπολογισμό του $f(n+1)$ απαιτείται ο υπολογισμός του $f(n)$.

Η πρώτη ισότητα $f(0) = 1$ είναι απαραίτητη, γιατί χωρίς αυτή ο υπολογισμός του $f(n)$ θα ήταν αδύνατος.

Γενικότερα, για να ορίσουμε **αναδρομικά** μια ακολουθία $f(n)$ για κάθε $n \in \mathbb{N}$ αρκεί:

1. Να ορίσουμε την $f(0)$, και
2. Να διαθέτουμε έναν κανόνα που μας δίνει την τιμή $f(n+1)$ συναρτήσει της $f(n)$[2].

Παράδειγμα 2.1.22. *Να ορισθεί αναδρομικά η ακολουθία $f(n) = n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$, όπου $0! = 1$. Στη συνέχεια να υπολογισθεί η τιμή $f(4)$.*

Είναι $f(0) = 0! = 1$, οπότε ορίζουμε

$$f(0) = 1.$$

Παρατηρούμε ότι $f(n+1) = 1 \cdot 2 \cdot 3 \cdots n \cdot (n+1) = n! \cdot n = f(n) \cdot n$, οπότε ορίζουμε

$$f(n+1) = n \cdot f(n), \text{ για κάθε } n \geq 0.$$

Με βάση του παραπάνω κανόνες

$$f(4) = 4 \cdot f(3) = 4 \cdot 3 \cdot f(2) = 12 \cdot 2 \cdot f(1) = 24 \cdot 1 \cdot f(0) = 24 \cdot 1 = 24.$$

[2] Η, γενικότερα, συναρτήσει των $f(n_1), f(n_2), \ldots, f(n_k)$, όπου $n_1, n_2, \ldots, n_k \leq n$.

Παράδειγμα 2.1.23. *Να ορισθεί αναδρομικά η ακολουθία* $f(n) = 0+1+2+\cdots+n$. *Στη συνέχεια να υπολογισθεί η τιμή* $f(4)$.

Είναι $f(0) = 0$, οπότε ορίζουμε

$$f(0) = 0.$$

Παρατηρούμε ότι $f(n+1) = 0 + 1 + 2 + \cdots (n-1) + n + (n+1) = f(n) + (n+1)$, οπότε ορίζουμε

$$f(n+1) = (n+1) + f(n), \text{ για κάθε } n \geq 0.$$

Με βάση του παραπάνω κανόνες

$$f(4) = 4 + f(3) = 4 + 3 + f(2) = 7 + 2 + f(1) = 9 + 1 + f(0) = 10 + 0 = 10.$$

Παράδειγμα 2.1.24. *Να υπολογισθεί η τιμή* $f(4)$ *για την ακολουθία* f *που ορίζεται από τους παρακάτω κανόνες*

$$f(0) = 2$$

$$f(1) = 5$$

$$f(n+2) = f(n+1) + f(n), \text{ για κάθε } n \geq 0.$$

Είναι

$$\begin{aligned} f(4) &= f(3) + f(2) \\ &= (f(2) + f(1)) + (f(1) + f(0)) \\ &= ((f(1) + f(0)) + 5) + (5 + 2) \\ &= (5 + 2) + 5 + 7 \\ &= 14. \end{aligned}$$

Ασκήσεις προς επίλυση

1) Να ορισθούν αναδρομικά οι παρακάτω ακολουθίες, για κάθε $n \in \mathbb{N}$.

   i) $f(n) = n$.

   ii) $f(n) = 0^2 + 1^2 + 2^2 + 3^2 + \cdots + n^2$.

   iii) $f(n) = 3^{n+5}$.

   iv) $f(n) = 7^{2n}$.

2) Να ορισθεί αναδρομικά η ακολουθία $f(n) = 2^n + 3^n$, για κάθε $n \in \mathbb{N}$ με $n \geq 5$.

3) Να υπολογισθεί η τιμή $f(5)$ της ακολουθιας f που ορίζεται από τις σχέσεις

$$f(1) = 2$$

$$f(2) = 3$$

$$f(n+2) = f(n+1)f(n), \text{ για κάθε } n \geq 1.$$

2.1.4 Παράρτημα: Επαγωγή και ορθότητα προγραμμάτων

Η αρχή της επαγωγής μπορεί να χρησιμοποιηθεί και για την απόδειξη της ορθότητας αλγορίθμων και προγραμμάτων.

Παράδειγμα 2.1.25. *Έστω A ένας πίνακας ακεραίων με m θέσεις $A[0], A[1], \ldots, A[m-1]$. Να δειχθεί ότι το επόμενο πρόγραμμα υπολογίζει το μέγιστο στοιχείο του πίνακα.*

```
int getmax(A){
   max = A[0];
   for(i=1; i<=m-1; i++){
    if(max < A[i]) max = A[i];
   }
   return max;
}
```

Απόδειξη. Θεωρούμε την πρόταση $\Pi(n)$: "Κατά το ξεκίνημα της n-οστής επανάληψης του βρόχου for η μεταβλητή max περιέχει το μέγιστο των πρώτων n στοιχείων του πίνακα."

Η πρόταση $\Pi(1)$ είναι αληθής, αφού η μεταβλητή max περιέχει την τιμή του $A[0]$.

Έστω ότι η $\Pi(k)$ είναι αληθής. Τότε και η $\Pi(k+1)$ είναι αληθής.

Πράγματι, από την υπόθεση της επαγωγής, πριν την k-οστή επάναληψη η max αποθηκεύει τη μέγιστη τιμή των πρώτων k στοιχείων του πίνακα. Όταν τελειώσει η k-οστή επανάληψη, η μεταβλητή max θα περιέχει το μέγιστο μεταξύ των πρώτων k στοιχείων και του $(k+1)$-οστού στοιχείου του πίνακα, άρα η $\Pi(k+1)$ είναι αληθής.

Όταν τελειώσει η εκτέλεση όλων των επαναλήψεων του βρόχου for, το μέγιστο θα έχει βρεθεί, καθώς θα έχουν εξετασθεί όλα τα στοιχεία του πίνακα. □

Παράδειγμα 2.1.26. *Έστω A ένας πίνακας ακεραίων με m θέσεις $A[0], A[1], \ldots, A[m-1]$. Να δειχθεί ότι το επόμενο πρόγραμμα υπολογίζει το άθροισμα των στοιχείων του πίνακα.*

```
int sum(A){
   s = A[0];
   for(i=1; i<=m-1; i++){
    s = s + A[i];
   }
   return s;
}
```

Απόδειξη. Θεωρούμε την πρόταση $\Pi(n)$: "Κατά το ξεκίνημα της n-οστής επανάληψης του βρόχου for, η μεταβλητή s περιέχει το άθροισμα των πρώτων n στοιχείων του πίνακα."

Η πρόταση $\Pi(1)$ είναι αληθής, αφού η μεταβλητή s περιέχει την τιμή του $A[0]$.

Έστω ότι η $\Pi(k)$ είναι αληθής. Τότε και η $\Pi(k+1)$ είναι αληθής.

Πράγματι, από την υπόθεση της επαγωγής, πριν την k-οστή επάναληψη η s αποθηκεύει το άθροισμα των πρώτων k στοιχείων του πίνακα. Όταν τελειώσει η k-οστή επανάληψη, η μεταβλητή max θα περιέχει το άθροισμα των πρώτων k στοιχείων και του $(k+1)$-οστού στοιχείου του πίνακα, άρα η $\Pi(k+1)$ είναι αληθής.

Όταν τελειώσει η εκτέλεση όλων των επαναλήψεων του βρόχου for το συνολικό άθροισμα θα έχει βρεθεί, καθώς θα έχουν προστεθεί όλα τα στοιχεία του πίνακα. □

Οι προτάσεις $\Pi(n)$ που χρησιμοποιήσαμε στα προηγούμενα δύο παραδείγματα εξαρτώνται από το πλήθος των επαναλήψεων του βρόχου και ονομάζονται **αναλλοίωτες** ή **αμετάβλητες βρόχου**.

Ιδιαίτερα σημαντική είναι η χρήση της επαγωγής στην απόδειξη της ορθότητας προγραμμάτων που περιέχουν αναδρομή.

Παράδειγμα 2.1.27. *Να δειχθεί ότι το επόμενο πρόγραμμα υπολογίζει τη συνάρτηση του παραγοντικού, δηλαδή $f(n) = n!$.*

```
int factorial(n){
   if(n==0){ return 1; }
   if(n==1){ return 1; }
   return n * factorial(n-1);
}
```

Απόδειξη. Έστω η πρόταση $\Pi(n)$: "Ισχύει ότι factorial$(n) = n!$ για κάθε $n \in \mathbb{N}$."

Η πρόταση $\Pi(0)$ είναι αληθής, αφού factorial$(0) = 1 = 0!$.

Η πρόταση $\Pi(1)$ είναι αληθής, αφού factorial$(1) = 1 = 1!$.

Έστω ότι η πρόταση $\Pi(k)$, όπου $k \geq 1$, είναι αληθής, δηλαδή factorial$(k) = k!$. Θα αποδειχθεί ότι και η $\Pi(k+1)$ είναι αληθής.

Πράγματι, επειδή $k + 1 \geq 2$, προκύπτει ότι το πρόγραμμα factorial$(k+1)$ επιστρέφει την τιμή $(k+1)$factorial(k), δηλαδή factorial$(k+1) = (k+1)$factorial(k). Από την υπόθεση της επαγωγής factorial$(k) = k!$, οπότε factorial$(k+1) = (k+1)k! = (k+1)!$. Άρα, η πρόταση $\Pi(n)$ ισχύει. □

2.2 Αρχή εγκλεισμού-αποκλεισμού

Οι παρακάτω κανόνες μεταξύ πληθαρίθμων συνόλων ισχύουν για **πεπερασμένα σύνολα**.

Πρόταση 2.4 (Κανόνας αθροίσματος). *Αν A, B είναι ξένα σύνολα ισχύει ότι*

$$|A \cup B| = |A| + |B|.$$

Γενικότερα, αν A_i είναι ανά δύο ξένα σύνολα ισχύει ότι

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

Στη περίπτωση όπου τα σύνολα δεν είναι κατ' ανάγκην ανά δύο ξένα εφαρμόζεται η αρχή εγκλεισμού-αποκλεισμού.

Πρόταση 2.5 (Αρχή εγκλεισμού-αποκλεισμού για ενώσεις συνόλων).

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{2.1}$$

Γενικότερα, για $n \geq 2$ ισχύει ότι

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = S_1 - S_2 + S_3 - \cdots + (-1)^{\nu-1} S_\nu + \cdots + (-1)^{n-1} S_n, \tag{2.2}$$

όπου
S_1 *είναι το άθροισμα των* $|A_i|$, *όπου* $1 \leq i \leq n$,
S_2 *είναι το άθροισμα των* $|A_i \cap A_j|$, *όπου* $1 \leq i < j \leq n$,
S_3 *είναι το άθροισμα των* $|A_i \cap A_j \cap A_k|$, *όπου* $1 \leq i < j < k \leq n$,
$\vdots$
S_n *είναι* $|A_1 \cap A_2 \cap \cdots \cap A_n|$.

Απόδειξη. (Με επαγωγή ως προς n.)

Για $n = 2$ (δηλ. ο τύπος (2.1)) ισχύει (βλέπε παράγραφο 1.4.1).

Υποθέτουμε ότι ισχύει για το n, δηλαδή

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

και θα αποδείξουμε ότι ισχύει για το $n+1$, δηλαδή

$$|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| = \sum_{1 \leq i \leq n+1} |A_i| - \sum_{1 \leq i < j \leq n+1} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n+1} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n} |A_1 \cap A_2 \cap \cdots \cap A_{n+1}|.$$

Εφαρμόζουμε τον τύπο (2.1) για τα σύνολα

$$A = A_1 \cup A_2 \cup \cdots \cup A_n \text{ και } B = A_{n+1},$$

οπότε

$$|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| = |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}|\,.$$

Επιπλέον,

$$|(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}| = |(A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1})|,$$

το οποίο από την υπόθεση της επαγωγής ισούται με

$$\sum_{1\le i\le n} |A_i \cap A_{n+1}| - \sum_{1\le i<j\le n} |(A_i \cap A_{n+1}) \cap (A_j \cap A_{n+1})| + \sum_{1\le i<j<k\le n} |(A_i \cap A_{n+1}) \cap (A_j \cap A_{n+1}) \cap (A_k \cap A_{n+1})| - \\ \cdots + (-1)^{n-1}|(A_1 \cap A_{n+1}) \cap (A_2 \cap A_{n+1}) \cap \cdots \cap (A_n \cap A_{n+1})|$$

ή, ισοδύναμα, με

$$\sum_{1\le i\le n} |A_i \cap A_{n+1}| - \sum_{1\le i<j\le n} |A_i \cap A_j \cap A_{n+1}| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k \cap A_{n+1}| - \\ \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}|.$$

Συνεπώς, έχουμε ότι

$$|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| = |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - \Big(\sum_{1\le i\le n} |A_i \cap A_{n+1}| - \sum_{1\le i<j\le n} |A_i \cap A_j \cap A_{n+1}| + \\ \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k \cap A_{n+1}| - \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}| \Big)$$

οπότε, από την υπόθεση της επαγωγής προκύπτει ότι

$$\begin{aligned}
&|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| \\
&= \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n| + |A_{n+1}| \\
&- \Big(\sum_{1\le i\le n} |A_i \cap A_{n+1}| - \sum_{1\le i<j\le n} |A_i \cap A_j \cap A_{n+1}| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k \cap A_{n+1}| - \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}| \Big) \\
&= \sum_{1\le i\le n+1} |A_i| - \sum_{1\le i<j\le n+1} |A_i \cap A_j| + \sum_{1\le i<j<k\le n+1} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n}|A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}|. \qquad \square
\end{aligned}$$

Υπενθυμίζουμε ότι ισχύουν οι παρακάτω σχέσεις (**Κανόνες De Morgan**):

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Γενικότερα,

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n},$$
$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}.$$

Η αρχή εγκλεισμού-αποκλεισμού πολλές φορές δίνεται στην επόμενη ισοδύναμη μορφή:

Πρόταση 2.6 (Αρχή εγκλεισμού-αποκλεισμού για τομές συμπληρωμάτων). *Έστω $A, B \subseteq \mathcal{E}$. Τότε ισχύει ότι*

$$|\overline{A} \cap \overline{B}| = |\mathcal{E}| - (|A| + |B|) + |A \cap B| \tag{2.3}$$

και γενικότερα για κάθε $A_1, A_2, \ldots, A_n \subseteq E$ ισχύει ότι

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |\mathcal{E}| - S_1 + S_2 - \cdots + (-1)^\nu S_\nu + \cdots + (-1)^n S_n. \tag{2.4}$$

Απόδειξη. Παρατηρούμε ότι, αφού

$$(A \cup B) \cup (\overline{A \cup B}) = \mathcal{E},$$

παίρνουμε

$$\begin{aligned}
&|A \cup B| + |\overline{A \cup B}| = |\mathcal{E}| \Leftrightarrow \\
&|\overline{A \cup B}| = |\mathcal{E}| - |A \cup B| \Leftrightarrow \\
&|\overline{A} \cap \overline{B}| = |\mathcal{E}| - (|A| + |B| - |A \cap B|)
\end{aligned}$$

και γενικότερα,

$$\begin{aligned}
|\overline{A_1 \cup A_2 \cup \cdots \cup A_n}| &= |\mathcal{E}| - |A_1 \cup A_2 \cup \cdots \cup A_n| \Leftrightarrow \\
|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| &= |\mathcal{E}| - (S_1 - S_2 + S_3 - \cdots + (-1)^{\nu-1} S_\nu + \cdots + (-1)^{n-1} S_n) \\
&= |\mathcal{E}| - S_1 + S_2 - S_3 + \cdots + (-1)^\nu S_\nu + \cdots + (-1)^n S_n.
\end{aligned}$$

□

Τέλος, αν στους τύπους (2.3) και (2.4) θέσουμε $\overline{A_i}$ αντί A_i για κάθε $i \in [n]$, προκύπτει η επόμενη ισοδύναμη μορφή:

Πρόταση 2.7 (Αρχή εγκλεισμού-αποκλεισμού για τομές συνόλων). *Έστω $A, B \subseteq \mathcal{E}$. Τότε ισχύει ότι*

$$|A \cap B| = |\mathcal{E}| - (|\overline{A}| + |\overline{B}) + |\overline{A} \cap \overline{B}| \tag{2.5}$$

και γενικότερα για κάθε $A_1, A_2, \ldots, A_n \subseteq E$ ισχύει ότι

$$|A_1 \cap A_2 \cap \cdots \cap A_n| = |\mathcal{E}| - \overline{S_1} + \overline{S_2} - \cdots + (-1)^\nu \overline{S_\nu} + \cdots + (-1)^n \overline{S_n}. \tag{2.6}$$

όπου
$\overline{S_1}$ είναι το άθροισμα των $|\overline{A_i}|$, όπου $1 \le i \le n$,
$\overline{S_2}$ είναι το άθροισμα των $|\overline{A_i} \cap \overline{A_j}|$, όπου $1 \le i < j \le n$,
$\overline{S_3}$ είναι το άθροισμα των $|\overline{A_i} \cap \overline{A_j} \cap \overline{A_k}|$, όπου $1 \le i < j < k \le n$,
$\vdots$
$\overline{S_n}$ είναι $|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}|$.

Εφαρμογές

1. Όταν ζητείται ο πληθάριθμος ενός συνόλου, του οποίου τα στοιχεία *έχουν μια τουλάχιστον ιδιότητα* από n δοσμένες ιδιότητες, τότε εφαρμόζεται ο πρώτος τύπος:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = S_1 - S_2 + S_3 - \cdots + (-1)^{n-1} S_n.$$

2. Όταν ζητείται ο πληθάριθμος ενός συνόλου, του οποίου τα στοιχεία *δεν έχουν καμιά ιδιότητα* από n δοσμένες ιδιότητες, τότε εφαρμόζεται ο δεύτερος τύπος:

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |\mathcal{E}| - S_1 + S_2 - S_3 + \cdots + (-1)^n S_n.$$

3. Όταν ζητείται ο πληθάριθμος ενός συνόλου, του οποίου τα στοιχεία *έχουν n ιδιότητες*, τότε εφαρμόζεται ο τρίτος τύπος:

$$|A_1 \cap A_2 \cap \cdots \cap A_n| = |\mathcal{E}| - \overline{S_1} + \overline{S_2} - \cdots + (-1)^n \overline{S_n}. \tag{2.7}$$

Παράδειγμα 2.2.1. *Πόσοι φυσικοί αριθμοί μικρότεροι ή ίσοι του* 100 *διαιρούνται από τουλάχιστον έναν από τους αριθμούς* 2, 5*;*

Λύση. Θεωρούμε τα σύνολα:
A_1: αριθμοί του [100] που είναι διαιρετοί με το 2.
A_2: αριθμοί του [100] που είναι διαιρετοί με το 5.
Ζητείται ο πληθάριθμος του συνόλου $A_1 \cup A_2$.
Προφανώς,

$$|A_1| = \lfloor \frac{100}{2} \rfloor = 50, \ |A_2| = \lfloor \frac{100}{5} \rfloor = 20 \text{ και } |A_1 \cap A_2| = \lfloor \frac{100}{10} \rfloor = 10.$$

Από τον τύπο (2.1) προκύπτει ότι

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 50 + 20 - 10 = 60. \qquad \square$$

Παράδειγμα 2.2.2. *Σε ένα σχολείο υπάρχουν 100 μαθητές και από αυτούς οι 50 μιλάνε Γαλλικά, οι 40 Γερμανικά, και οι 20 μιλάνε και τις δύο γλώσσες. Πόσοι μαθητές δεν μιλάνε καμία από τις 2 γλώσσες;*

Λύση. Θεωρούμε τα σύνολα
A_1: μαθητές που μιλάνε Γαλλικά.
A_2: μαθητές που μιλάνε Γερμανικά.
Ζητείται ο πληθάριθμος του συνόλου $\overline{A_1} \cap \overline{A_2}$.
Προφανώς, $|\mathcal{E}| = 100$, $|A_1| = 50$, $|A_2| = 40$ και $|A_1 \cap A_2| = 20$.
Από τον τύπο (2.3) της αρχής εγκλεισμού αποκλεισμού προκύπτει ότι

$$|\overline{A_1} \cap \overline{A_2}| = \mathcal{E} - (|A_1| + |A_2|) + |A_1 \cap A_2| = 100 - (50 + 40) + 20 = 30.$$

Παρατήρηση. Επιπλέον προκύπτει ότι οι μαθητές του σχολείου οι οποίοι μιλάνε τουλάχιστον μία από τις δύο γλώσσες είναι 70. Πράγματι, ισχύει ότι

$$\mathcal{E} = (A_1 \cup A_2) \cup (\overline{A_1 \cup A_2}).$$

Άρα, (κανόνας αθροίσματος)

$$|\mathcal{E}| = |A_1 \cup A_2| + |\overline{A_1 \cup A_2}|$$
$$|\mathcal{E}| = |A_1 \cup A_2| + |\overline{A_1} \cap \overline{A_2}|$$
$$100 = |A_1 \cup A_2| + 30,$$

οπότε

$$|A_1 \cup A_2| = 100 - 30 = 70. \qquad \square$$

Παράδειγμα 2.2.3. *Μια έρευνα αγοράς για ένα προϊόν έδωσε τα παρακάτω αποτελέσματα:*

	Ερωτηθέντα άτομα: 2000	*Άτομα που γνωρίζουν το προϊόν:* 1150
Παντρεμένοι	1281	632
Γυναίκες	1048	410
Παντρεμένες γυναίκες	838	218

*Πόσα από τα ερωτηθέντα άτομα έχουν **τουλάχιστον μια** από τις παρακάτω ιδιότητες:*

Γνωρίζουν το προϊόν.
Είναι παντρεμένοι.
Είναι γυναίκες.

Λύση. Θεωρούμε τα σύνολα
A_1 : άτομα που γνωρίζουν το προϊόν,
A_2 : άτομα που είναι παντρεμένοι, και
A_3 : άτομα που είναι γυναίκες.

Προφανώς,

$$|A_1| = 1150,\ |A_2| = 1281,\ |A_3| = 1048,$$
$$|A_1 \cap A_2| = 632, |A_1 \cap A_3| = 410,\ |A_2 \cap A_3| = 838,$$
$$|A_1 \cap A_2 \cap A_3| = 218.$$

Άρα ο τύπος (1) της αρχής εγκλεισμού-αποκλεισμού (για $n = 3$) δίνει:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \\ &= 1150 + 1281 + 1048 - 632 - 410 - 838 + 218 \\ &= 1817. \qquad \square\end{aligned}$$

Παράδειγμα 2.2.4. *Μια διαφημιστική εταιρεία ενδιαφέρεται να συγκεντρώσει στοιχεία για τις προτιμήσεις* 3500 *πελατών ενός τουριστικού γραφείου σχετικά με τις διακοπές που επιθυμούν:* 2000 *άτομα δήλωσαν ότι προτιμούν διακοπές στην Ελλάδα.* 1600 *άτομα δήλωσαν ότι προτιμούν διακοπές σε κάποιο παραθαλάσσιο μέρος.* 1300 *άτομα δήλωσαν ότι προτιμούν διακοπές με οργανωμένη ομάδα. Επίσης,* 700 *άτομα δήλωσαν ότι προτιμούν οργανωμένες διακοπές στην Ελλάδα,* 500 *άτομα δήλωσαν ότι επιθυμούν οργανωμένες διακοπές σε κάποιο παραθαλάσσιο μέρος και* 1300 *άτομα δήλωσαν ότι επιθυμούν διακοπές σε κάποιο Ελληνικό παραθαλάσσιο μέρος. Τέλος,* 300 *άτομα δήλωσαν ότι επιθυμούν οργανωμένες διακοπές σε κάποιο Ελληνικό παραθαλάσσιο μέρος.*

i) Να βρεθεί ο αριθμός των ατόμων που επιθυμούν μη οργανωμένες διακοπές σε μη παραθαλάσσιο μέρος του εξωτερικού.

ii) Να βρεθεί ο αριθμός των ατόμων που επιθυμούν οργανωμένες διακοπές στην Ελλάδα ή/και σε κάποιο παραθαλάσσιο μέρος.

iii) Να βρεθεί ο αριθμός των ατόμων που επιθυμούν μη οργανωμένες διακοπές στην Ελλάδα ή/και σε κάποιο παραθαλάσσιο μέρος.

Λύση. Έστω

E το σύνολο όλων των ατόμων.

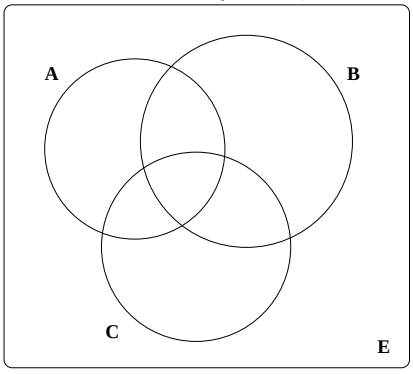
A το σύνολο των ατόμων που προτιμούν διακοπές στην Ελλάδα.

B το σύνολο των ατόμων που προτιμούν διακοπές σε παραθαλάσσιο μέρος.

C το σύνολο των ατόμων που προτιμούν διακοπές με οργανωμένη ομάδα.

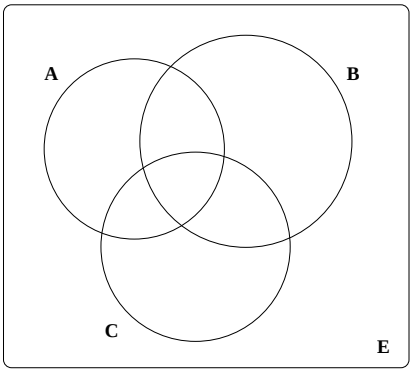
Γνωρίζουμε ότι $|E| = 3500$, $|A| = 2000$, $|B| = 1600$, $|C| = 1300$, $|A \cap B| = 1300$, $|A \cap C| = 700$, $|B \cap C| = 500$ και $|A \cap B \cap C| = 300$.

Θα απαντήσουμε στα ερωτήματα της άσκησης με τη βοήθεια του επόμενου διαγράμματος Venn.

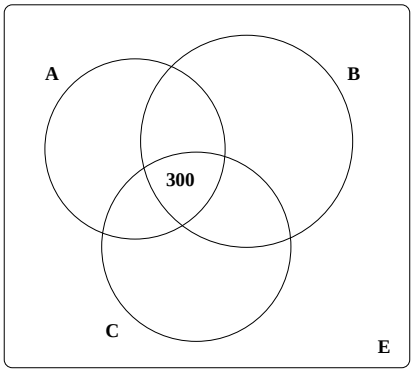


Κάθε μια από τις 8 περιοχές που ορίζονται στο διάγραμμα αντιστοιχεί σε κάποιο σύνολο της μορφής $A^* \cap B^* \cap C^*$, όπου X^* είναι είτε το X είτε το $\overline{X}$. Θα αρχίσουμε να υπολογίζουμε τους πληθαρίθμους κάθε περιοχής ξεκινώντας από την κεντρική περιοχή, έπειτα θα ασχοληθούμε με τις περιοχές που γειτονεύουν με την κεντρική. Στη συνέχεια, με τις περιοχές που γειτονεύουν με αυτές και τέλος με την εξωτερική περιοχή.

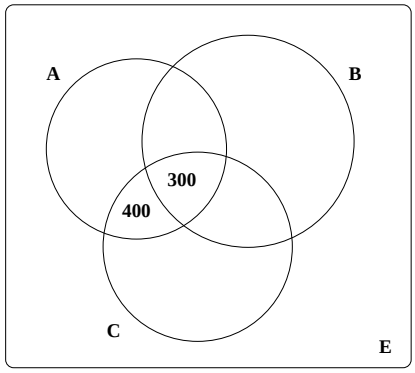
Προκειμένου να γίνει πιο κατανοητή η διαδικασία στα επόμενα σχήματα απεικονίζονται τα στάδια της συμπλήρωσης του διαγράμματος.



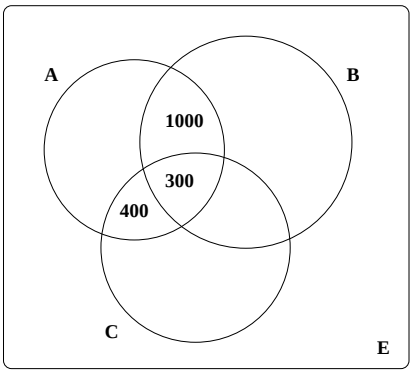
στάδιο 0



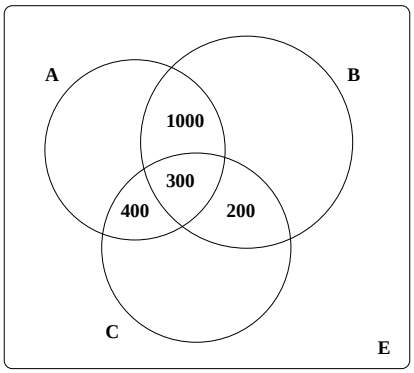
στάδιο 1



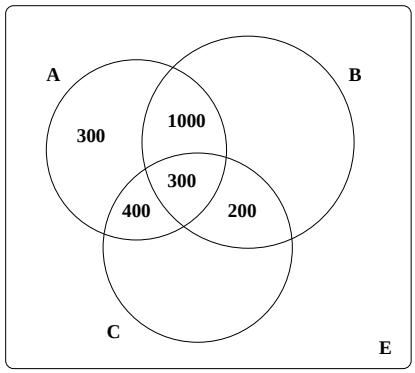
στάδιο 2



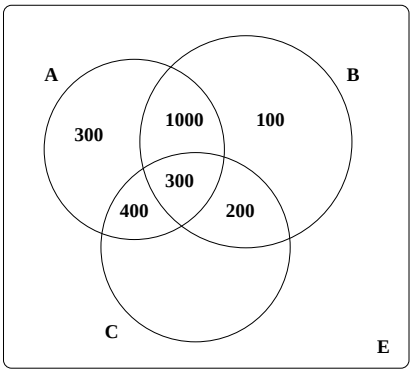
στάδιο 3



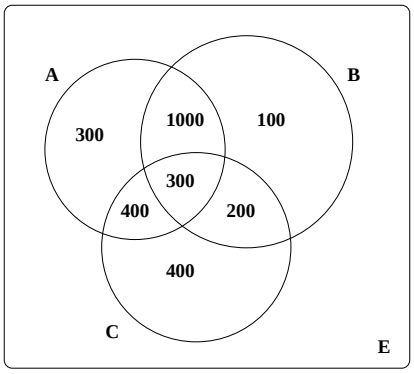
στάδιο 4



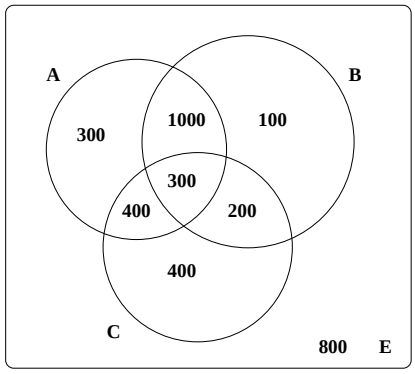
στάδιο 5



στάδιο 6



στάδιο 7

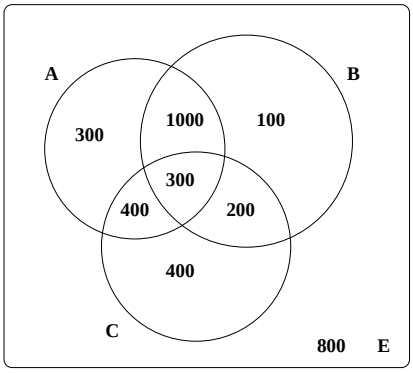


στάδιο 8

- $|A \cap B \cap C| = 300$ (βλέπε στάδιο 1)
- $|A \cap \overline{B} \cap C| = |A \cap C| - |A \cap B \cap C| = 700 - 300 = 400$ (βλέπε στάδιο 2).
- $|A \cap B \cap \overline{C}| = |A \cap B| - |A \cap B \cap C| = 1300 - 300 = 1000$ (βλέπε στάδιο 3).
- $|\overline{A} \cap B \cap C| = |B \cap C| - |A \cap B \cap C| = 500 - 300 = 200$ (βλέπε στάδιο 4).
- $|A \cap \overline{B} \cap \overline{C}| = |A| - |A \cap \overline{B} \cap C| - |A \cap B \cap \overline{C}| - |A \cap B \cap C| = 2000 - 400 - 1000 - 300 = 300.$ (βλέπε στάδιο 5).
- $|\overline{A} \cap B \cap \overline{C}| = |B| - |A \cap B \cap \overline{C}| - |\overline{A} \cap B \cap C| - |A \cap B \cap C| = 1600 - 1000 - 200 - 300 = 100.$ (βλέπε στάδιο 6).

- $|\overline{A} \cap \overline{B} \cap C| = |C| - |A \cap \overline{B} \cap C| - |\overline{A} \cap B \cap C| - |A \cap B \cap C| = 1300 - 400 - 200 - 300 = 400$. (βλέπε στάδιο 7).
- $|\overline{A} \cap \overline{B} \cap \overline{C}| = |E| - |A \cap \overline{B} \cap \overline{C}| - |\overline{A} \cap \overline{B} \cap C| - |\overline{A} \cap B \cap \overline{C}| - |\overline{A} \cap B \cap C| - |A \cap \overline{B} \cap C| - |A \cap B \cap \overline{C}| - |A \cap B \cap C| = 3500 - 300 - 400 - 100 - 200 - 400 - 1000 - 300 = 800$. (βλέπε στάδιο 8).

Όλες οι απαντήσεις που αφορούν τα παραπάνω στοιχεία μπορούν να βρεθούν εύκολα με τη βοήθεια του τελευταίου διαγράμματος:



i) Ο ζητούμενος αριθμός ισούται με τον πληθάριθμο $|E \setminus (A \cup B \cup C)| = |\overline{A} \cap \overline{B} \cap \overline{C}| = 800$.

ii) Ο ζητούμενος αριθμός ισούται με τον πληθάριθμο $|C \cap (A \cup B)| = |A \cap \overline{B} \cap C| + |\overline{A} \cap B \cap C| + |A \cap B \cap C| = 400 + 200 + 300 = 900$.

iii) Ο ζητούμενος αριθμός ισούται με τον πληθάριθμο $|(A \cup B) \setminus C| = |A \cap \overline{B} \cap \overline{C}| + |A \cap B \cap \overline{C}| + |\overline{A} \cap B \cap \overline{C}| = 300 + 1000 + 100 = 1400$. □

Παράδειγμα 2.2.5. *Να βρεθεί το πλήθος των αριθμών του συνόλου* [1000] *που δεν είναι διαιρετοί ούτε με το* 2*, ούτε με το* 3*, ούτε με το* 5*.*

Λύση. Έστω τα σύνολα:
A_1: αριθμοί του [1000] που είναι διαιρετοί με το 2.
A_2: αριθμοί του [1000] που είναι διαιρετοί με το 3.
A_3: αριθμοί του [1000] που είναι διαιρετοί με το 5.
Τότε,

$$|A_1| = \lfloor \frac{1000}{2} \rfloor = 500, \ |A_2| = \lfloor \frac{1000}{3} \rfloor = 333, \ |A_3| = \lfloor \frac{1000}{5} \rfloor = 200.$$

$$|A_1 \cap A_2| = \lfloor \frac{1000}{6} \rfloor = 166, \ |A_1 \cap A_3| = \lfloor \frac{1000}{10} \rfloor = 100, \ |A_2 \cap A_3| = \lfloor \frac{1000}{15} \rfloor = 66,$$

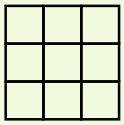
$$|A_1 \cap A_2 \cap A_3| = \lfloor \frac{1000}{30} \rfloor = 33.$$

Άρα ο τύπος (2.4) της αρχής εγκλεισμού-αποκλεισμού (για $n = 3$) δίνει:

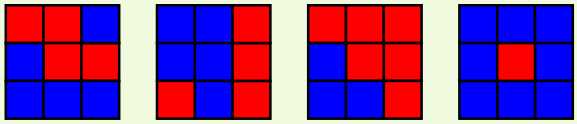
$$\begin{aligned} |\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| &= |\mathcal{E}| - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) - |A_1 \cap A_2 \cap A_3| \\ &= 1000 - (500 + 333 + 200) + (166 + 100 + 66) - 33 \\ &= 266. \end{aligned}$$

□

Παράδειγμα 2.2.6. *Κάθε μοναδιαίο τετράγωνο του επόμενου σχήματος χρωματίζεται κόκκινο ή μπλε.*

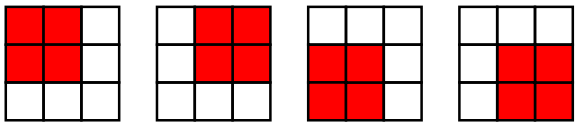


Για παράδειγμα,



Με πόσους διαφορετικούς τρόπους μπορεί να χρωματισθεί το παραπάνω σχήμα έτσι ώστε να περιέχει τουλάχιστον ένα κόκκινο τετράγωνο με διαστάσεις 2 επί 2;

Λύση. Παρατηρούμε ότι στο σχήμα υπάρχουν 4 πιθανές θέσεις εμφάνισης ενός κόκκινου τετραγώνου με διαστάσεις 2×2.



C_1 C_2 C_3 C_4

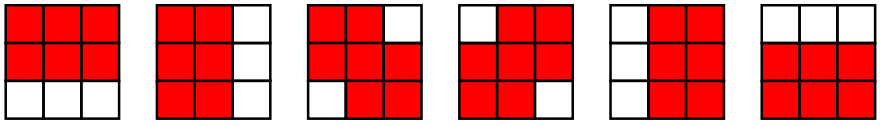
Έστω C_1, C_2, C_3, C_4 το σύνολο των χρωματισμών που περιέχουν ένα κόκκινο τετράγωνο με διαστάσεις 2×2 στην πάνω αριστερή, πάνω δεξιά, κάτω αριστερή και κάτω δεξιά γωνία του σχήματος αντίστοιχα.

Οι χρωματισμοί που περιέχουν τουλάχιστον ένα κόκκινο τετράγωνο με διαστάσεις 2×2 είναι το σύνολο $C_1 \cup C_2 \cup C_3 \cup C_4$.

Από την αρχή εγκλεισμού - αποκλεισμού έχουμε ότι

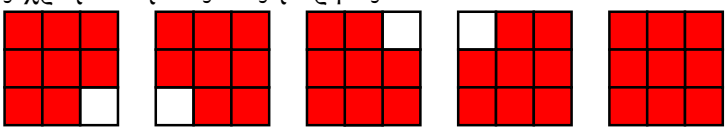
$$\begin{aligned}|C_1 \cup C_2 \cup C_3 \cup C_4| =& |C_1| + |C_2| + |C_3| + |C_4| \\ & - |C_1 \cap C_2| - |C_1 \cap C_3| - |C_1 \cap C_4| - |C_2 \cap C_3| - |C_2 \cap C_4| - |C_3 \cap C_4| \\ & + |C_1 \cap C_2 \cap C_3| + |C_1 \cap C_2 \cap C_4| + |C_1 \cap C_3 \cap C_4| + |C_2 \cap C_3 \cap C_4| - |C_1 \cap C_2 \cap C_3 \cap C_4|\end{aligned}$$

Τα σύνολα $C_1 \cap C_2$, $C_1 \cap C_3$, $C_1 \cap C_4$, $C_2 \cap C_3$, $C_2 \cap C_4$, $C_3 \cap C_4$ αποτελούνται από τους χρωματισμούς οι οποίοι περιέχουν έχουν κόκκινα μοναδιαία τετράγωνα στις επόμενες θέσεις, ενώ τα λευκά τετράγωνα μπορούν να έχουν οποιαδήποτε από τα δύο χρώματα.



$C_1 \cap C_2$ $C_1 \cap C_3$ $C_1 \cap C_4$ $C_2 \cap C_3$ $C_2 \cap C_4$ $C_3 \cap C_4$

Αντίστοιχα, τα σύνολα $C_1 \cap C_2 \cap C_3$, $C_1 \cap C_2 \cap C_4$, $C_1 \cap C_3 \cap C_4$, $C_2 \cap C_3 \cap C_4$, $C_1 \cap C_2 \cap C_3 \cap C_4$ αποτελούνται από τους χρωματισμούς της μορφής:



$C_1 \cap C_2 \cap C_3$ $C_1 \cap C_2 \cap C_4$ $C_1 \cap C_3 \cap C_4$ $C_2 \cap C_3 \cap C_4$ $C_1 \cap C_2 \cap C_3 \cap C_4$

Από την πολλαπλασιαστική αρχή προκύπτει ότι

$|C_1| = |C_2| = |C_3| = |C_4| = 2^5$,

$|C_1 \cap C_2| = |C_1 \cap C_3| = |C_2 \cap C_4| = |C_3 \cap C_4| = 2^3$,

$|C_1 \cap C_4| = |C_2 \cap C_3| = 2^2$,

$|C_1 \cap C_2 \cap C_3 = C_1 \cap C_2 \cap C_4| = |C_1 \cap C_3 \cap C_4| = |C_2 \cap C_3 \cap C_4| = 2^1$,
$|C_1 \cap C_2 \cap C_3 \cap C_4| = 1$.
Αντικαθιστώντας έχουμε ότι

$$|C_1 \cup C_2 \cup C_3 \cup C_4| = 4 \cdot 2^5 - (4 \cdot 2^3 + 2 \cdot 2^2) + 4 \cdot 2^1 - 1 \cdot 1 = 128 - 40 + 4 - 1 = 91.$$

Άρα, από τους $2^9 = 512$ διαφορετικούς χρωματισμούς του σχήματος, οι 91 χρωματισμοί περιέχουν τουλάχιστον ένα κόκκινο τετράγωνο με διαστάσεις 2×2. □

Παράδειγμα 2.2.7. *Να βρεθεί με πόσους τρόπους μπορούν να μοιρασθούν 7 διαφορετικά χαρτιά σε 4 παίχτες έτσι ώστε κάθε παίχτης να λάβει τουλάχιστον ένα χαρτί.*

Λύση. Επειδή είναι ευκολότερο να μετρήσουμε τους τρόπους να μην λάβουν κάποιοι παίχτες κανένα χαρτί, θεωρούμε τα παρακάτω σύνολα:

Έστω το σύνολο E όλων των τρόπων να μοιρασθούν τα 7 χαρτιά στους 4 παίχτες χωρίς περιορισμούς.

Επίσης, έστω D_1, D_2, D_3 και D_4 τα σύνολα των τρόπων να μοιρασθούν τα 7 χαρτιά έτσι ώστε ο πρώτος, ο δεύτερος, ο τρίτος και ο τέταρτος παίχτης να μην λάβουν κανένα χαρτί αντίστοιχα.

Τότε, τα σύνολα $\overline{D_1}$, $\overline{D_2}$, $\overline{D_3}$ και $\overline{D_4}$ είναι αντίστοιχα οι τρόποι να μοιρασθούν τα 7 χαρτιά έτσι ώστε ο πρώτος, ο δεύτερος, ο τρίτος και ο τέταρτος παίχτης να λάβει τουλάχιστον ένα χαρτί αντίστοιχα.

Άρα, το σύνολο $\overline{D_1} \cap \overline{D_2} \cap \overline{D_3} \cap \overline{D_4}$ περιέχει τους τρόπους να μοιρασθούν τα 7 χαρτιά στους 4 παίχτες έτσι ώστε κάθε παίχτης να λάβει τουλάχιστον ένα χαρτί.

Από την αρχή εγκλεισμού - αποκλεισμού έχουμε ότι

$$\begin{aligned}|\overline{D_1} \cap \overline{D_2} \cap \overline{D_3} \cap \overline{D_4}| =& |E| - |D_1| - |D_2| - |D_3| - |D_4| \\ &+ |D_1 \cap D_2| + |D_1 \cap D_3| + |D_1 \cap D_4| + |D_2 \cap D_3| + |D_2 \cap D_4| + |D_3 \cap D_4| \\ &- |D_1 \cap D_2 \cap D_3| - |D_1 \cap D_2 \cap D_4| - |D_1 \cap D_3 \cap D_4| - |D_2 \cap D_3 \cap D_4| \\ &+ |D_1 \cap D_2 \cap D_3 \cap D_4|\end{aligned}$$

Από την αρχή του γινομένου προκύπτει ότι $|E| = 4^7$ αφού για κάθε ένα από τα 7 χαρτιά έχουμε 4 επιλογές. Αντίστοιχα,
$|D_1| = |D_2| = |D_3| = |D_4| = 3^7$.
$|D_1 \cap D_2| = |D_1 \cap D_3| = |D_1 \cap D_4| = |D_2 \cap D_3| = |D_2 \cap D_4| = |D_3 \cap D_4| = 2^7$.
$|D_1 \cap D_2 \cap D_3| = |D_1 \cap D_2 \cap D_4| = |D_1 \cap D_3 \cap D_4| = |D_2 \cap D_3 \cap D_4| = 1^7$.
$|D_1 \cap D_2 \cap D_3 \cap D_4| = 0$.
Αντικαθιστώντας, έχουμε ότι

$$|\overline{D_1} \cap \overline{D_2} \cap \overline{D_3} \cap \overline{D_4}| = 4^7 - 4 \cdot 3^7 + 6 \cdot 2^7 - 4 \cdot 1^7 + 0 = 16384 - 8748 + 768 - 4 = 8400$$

Άρα, υπάρχουν 8400 τρόποι να μοιρασθούν τα 7 χαρτιά στους 4 παίχτες έτσι ώστε κάθε παίχτης να λάβει τουλάχιστον ένα χαρτί. □

Παράδειγμα 2.2.8. *Σε μια αίθουσα βρίσκονται n άτομα τα οποία κάθονται σε n διακεκριμένες θέσεις. Να βρεθεί ο αριθμός των τρόπων που μπορούν να αλλάξουν θέσεις τα n άτομα έτσι ώστε κανείς να μην κάθεται στην αρχική του θέση.*

Λύση. Οι τρόποι που μπορούν να καθίσουν τα n άτομα στις θέσεις τους χωρίς περιορισμό είναι $n!$.

Έστω A_i το σύνολο όλων των τρόπων να καθίσουν τα n άτομα έτσι ώστε το i-στό άτομο να κάθεται στην αρχική του θέση (και οι υπόλοιποι να μην έχουν κανένα περιορισμό).

Ζητείται να βρεθεί ο πληθάριθμος

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}} \cap \overline{A_n}|.$$

Παρατηρούμε ότι για κάθε $i \in [n]$ ισχύει ότι

$$|A_i| = (n-1)!$$

διότι το i-στό άτομο έχει μόνο ένα τρόπο να καθίσει και για τα υπόλοιπα $n-1$ άτομα υπάρχουν $(n-1)!$ τρόποι να καθίσουν.

Επίσης, για κάθε ζεύγος άτομων i, j ισχύει ότι

$$|A_i \cap A_j| = (n-2)!$$

διότι τα άτομα i, j έχουν ένα τρόπο να καθίσουν, και για τα υπόλοιπα $n-2$ άτομα υπάρχουν $(n-2)!$ τρόποι να καθίσουν.

Αντίστοιχα, για κάθε τριάδα ατόμων i, j, k ισχύει ότι

$$|A_i \cap A_j \cap A_k| = (n-3)!$$

κ.ο.κ. Για κάθε m-άδα ατόμων $i_1, i_2, \ldots, i_m$ με $1 \le i_1 < i_2 < \cdots < i_m \le n$ ισχύει ότι

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}| = (n-m)!$$

Από την αρχή εγκλεισμού-αποκλεισμού ισχύει ότι

$$\begin{aligned}
&|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}} \cap \overline{A_n}| \\
&= |\mathcal{E}| - S_1 + S_2 - S_3 + \cdots + (-1)^n S_n \\
&= |\mathcal{E}| - \sum_{1 \le i \le n} |A_i| + \sum_{1 \le i < j \le n} |A_i \cap A_j| - \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots \\
&\quad + (-1)^m \sum_{1 \le i_1 < i_2 < \cdots < i_m \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}| + \cdots + (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|.
\end{aligned}$$

Επειδή το πλήθος των ζευγών ισούται με τους συνδυασμούς $\binom{n}{2}$, το πλήθος των τριάδων ισούται με τους συνδυασμούς $\binom{n}{3}$, και γενικά, το πλήθος των m-αδων είναι ίσο με τους συνδυασμούς $\binom{n}{m}$, προκύπτει ότι

$$\begin{aligned}
&|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}} \cap \overline{A_n}| \\
&= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots + (-1)^m \binom{n}{m}(n-m)! + \cdots + (-1)^n \binom{n}{n}(n-n)! \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k}(n-k)!.
\end{aligned}$$

□

2.2.1 Έλεγχος συνέπειας δεδομένων και εκτίμηση φραγμάτων

Η αρχή εγκλεισμού-αποκλεισμού μπορεί να χρησιμοποιηθεί σε ορισμένες περιπτώσεις για τον έλεγχο στατιστικών δεδομένων.

Παράδειγμα 2.2.9. *Σε μια έρευνα που συμμετείχαν* 600 *φοιτητές καταγράφηκαν τα παρακάτω στατιστικά δεδομένα:*

Αριθμός γυναικών	*312*
Αριθμός τελειόφοιτων	*187*
Αριθμός εργαζόμενων φοιτητών	*265*
Αριθμός τελειόφοιτων γυναικών	*24*
Αριθμός εργαζόμενων γυναικών	*90*
Αριθμός εργαζόμενων τελειόφοιτων	*49*
Αριθμός εργαζόμενων τελειόφοιτων γυναικών	*14*

Δεν είναι προφανές αν τα παράπανω στατιστικά δεδομένα είναι συνεπή ή όχι. Χρησιμοποιώντας την αρχή εγκλεισμού-αποκλεισμού θα δείξουμε ότι στην πραγματικότητα δεν είναι συνεπή!

Λύση. Έστω

E: το σύνολο όλων των φοιτητών,
A_1: το σύνολο των φοιτητών που είναι γυναίκες,
A_2: το σύνολο των τελειόφοιτων,
A_3: το σύνολο των εργαζόμενων φοιτητών.
Από την αρχή εγκλεισμού-αποκλεισμού ισχύει ότι

$$\begin{aligned}\left|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}\right| &= |E| - |A_1 \cup A_2 \cup A_3| \\ &= |E| - (|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|) \\ &= 600 - 312 - 187 - 265 + 24 + 90 + 49 - 14 \\ &= -15.\end{aligned}$$

Άρα, τα δεδομένα που δίδονται είναι ασυνεπή. □

Με τη βοήθεια της αρχής εγκλεισμού-αποκλεισμού μπορούμε να υπολογίσουμε φράγματα για τις δυνατές τιμές των πληθαρίθμων ορισμένων συνόλων στην περίπτωση που τα δεδομένα που είναι διαθέσιμα είναι ελλιπή.

Στην παρακάτω πρόταση παρουσιάζονται μερικές ανισότητες που ισχύουν για τρία σύνολα, οι οποίες μπορούν να χρησιμοποιηθούν για το σκοπό αυτό.

Πρόταση 2.8. *Έστω $A, B, C \subseteq E$. Ισχύουν οι παρακάτω ανισότητες:*

(i) $|A \cap B| + |A \cap C| + |B \cap C| \geq |A| + |B| + |C| - |A \cup B \cup C|$.

(ii) $|A \cap B| + |A \cap C| - |B \cap C| \leq |A|$.

Απόδειξη. Από την αρχή εγκλεισμού-αποκλεισμού ισχύει ότι

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

ή, ισοδύναμα

$$|A \cup B \cup C| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) \geq |A \cap B \cap C| \geq 0$$

από την οποία προκύπτει ότι

$$|A \cap B| + |A \cap C| + |B \cap C| \geq |A| + |B| + |C| - |A \cup B \cup C| \,.$$

Επιπλέον, επειδή $|A| \geq |A \cap (B \cup C)|$ και $|A \cap B \cap C| \leq |B \cap C|$ ισχύει ότι

$$|A| \geq |A \cap (B \cup C)| = |A \cap B| + |A \cap C| - |A \cap B \cap C| \geq |A \cap B| + |A \cap C| - |B \cap C| \,. \qquad \square$$

2.2.2 Ασκήσεις προς επίλυση

1) Να βρεθεί ο $|A_1 \cup A_2|$ αν $|A_1| = 12$, $|A_2| = 18$ και:

   i) $A_1 \cap A_2 = \emptyset$, iii) $|A_1 \cap A_2| = 6$,
   ii) $|A_1 \cap A_2| = 1$, iv) $A_1 \subseteq A_2$.

2) Να βρεθεί πόσα στοιχεία περιέχονται στο σύνολο $\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}$ όπου $A_1, A_2, A_3 \subseteq E$, $|E| = 500$, $|A_1| = 200$, $|A_2| = 200$, $|A_3| = 250$, $|A_1 \cap A_2| = 80$, $|A_1 \cap A_3| = 120$, $|A_2 \cap A_3| = 90$, $|A_1 \cap A_2 \cap A_3| = 50$.

3) 345 φοιτητές ενός Πανεπιστημίου επέλεξαν το μάθημα της Ανάλυσης, 212 τα Διακριτά Μαθηματικά και 188 επέλεξαν και τα δύο αυτά μαθήματα. Πόσοι επέλεξαν τουλάχιστον ένα από τα δύο μαθήματα;

4) Μια έρευνα αγοράς διαπίστωσε ότι 96% των νοικοκυριών της Αθήνας έχουν τουλάχιστον μια τηλεόραση, 98% έχουν τηλέφωνο και 95% έχουν και τα δύο. Τι ποσοστό νοικοκυριών δεν έχει κανένα από τα δύο;

5) Να βρεθεί ο $|A_1 \cup A_2 \cup A_3|$, όπου $|A_1| = |A_2| = |A_3| = 100$ και

   i) Τα σύνολα είναι ανά δύο ξένα,

   ii) Υπάρχουν 50 κοινά στοιχεία σε κάθε ζεύγος συνόλων, ενώ δεν υπάρχει κανένα κοινό στοιχείο και στα τρία σύνολα,

   iii) $A_1 = A_2 = A_3$.

6) Έστω E ένα σύνολο με 1000 στοιχεία και $A, B, C \subseteq E$ για οποία ισχύουν $|A| = 400$, $|B| = 370$, $|C| = 600$, $|A \cap B| = 180$, $|A \cap C| = 250$, $|B \cap C| = 200$, $|A \cap B \cap C| = 80$.

   Να βρεθεί πόσα από τα στοιχεία του E:

   (i) ανήκουν σε ένα τουλάχιστον από τα A, B, C,

   (ii) δεν ανήκουν σε κανένα από τα A, B, C,

   (iii) ανήκουν στο A και δεν ανήκουν στα B, C,

   (iv) ανήκουν ακριβώς σε ένα από τα A, B, C.

7) Ένα τμήμα Πληροφορικής έχει 2504 φοιτητές. Από αυτούς 1876 έχουν επιλέξει Prolog, 999 έχουν επιλέξει Java και 345 έχουν επιλέξει C++. Επιπλέον, γνωρίζουμε ότι 876 έχουν επιλέξει και Prolog και Java, 231 έχουν επιλέξει και Prolog και C++, και 290 έχουν επιλέξει και Java και C++. Αν 189 από αυτούς τους φοιτητές έχουν επιλέξει και τις τρεις γλώσσες, πόσοι δεν έχουν επιλέξει καμία από αυτές;

8) Να βρεθεί, με τη χρήση της αρχής εγκλεισμού-αποκλεισμού, πόσοι πρώτοι αριθμοί είναι μικρότεροι ή ίσοι του 120;

9) Σε μια τάξη υπάρχουν συνολικά 40 μαθητές. Υπάρχουν 18 μαθητές που παίζουν σκάκι και 23 που παίζουν ποδόσφαιρο. Ορισμένοι μαθητές παίζουν μπάσκετ. Οι μαθητές που παίζουν σκάκι και ποδόσφαιρο είναι 9. Οι μαθητές που παίζουν σκάκι και μπάσκετ είναι 7, ενώ οι μαθητές που παίζουν ποδόσφαιρο και μπάσκετ είναι 12. Επίσης, 4 μαθητές ασχολούνται και με τα τρία παιχνίδια. Επιπρόσθετα, κάθε μαθητής ασχολείται τουλάχιστον με ένα παιχνίδι.

   i) Να βρεθεί πόσοι μαθητές παίζουν μπάσκετ.

ii) Να βρεθεί πόσοι μαθητές παίζουν μόνο μπάσκετ.

iii) Να βρεθεί πόσοι μαθητές παίζουν μπάσκετ και ποδόσφαιρο αλλά όχι σκάκι.

iv) Να βρεθεί πόσοι μαθητές παίζουν ακριβώς ένα παιχνίδι.

10) Σε μια έρευνα του Υπουργείου Τουρισμού ρωτήθηκαν 5000 άτομα αν έχουν επισκεφθεί την Κρήτη. Ο παρακάτω πίνακας δίνει κάποια στοιχεία της έρευνας αυτής:

	Ερωτηθέντα άτομα: 5000	Άτομα που είχαν επισκεφθεί την Κρήτη: 3620
Άνδρες	2597	2007
Άτομα άνω των 40 ετών	2957	2089
Άνδρες άνω των 40 ετών	1476	1088

Με χρήση της αρχής εγκλεισμού-αποκλεισμού να βρεθεί πόσες γυναίκες κάτω των 40 ετών δεν έχουν επισκεφθεί την Κρήτη.

11) Σε μια έρευνα σχετικά με τις εκπομπές της τηλεόρασης, 200 άτομα ρωτήθηκαν τις παρακάτω ερωτήσεις. Δίπλα σε κάθε μια, αναγράφεται ο άριθμος αυτών που απάντησαν θετικά:

i) Παρακολουθείτε τις αθλητικές εκπομπές; Απ. 50.

ii) Παρακολουθείτε τις ειδήσεις; Απ. 90.

iii) Παρακολουθείτε τα τηλεπαιχνίδια; Απ. 85.

iv) Παρακολουθείτε και τις αθλητικές εκπομπές και τις ειδήσεις; Απ. 35.

v) Παρακολουθείτε και τις αθλητικές εκπομπές και τα τηλεπαιχνίδια; Απ. 25.

vi) Παρακολουθείτε και τις ειδήσεις και τα τηλεπαιχνίδια; Απ. 45.

vii) Παρακολουθείτε και τις αθλητικές εκπομπές και τις ειδήσεις και τα τηλεπαιχνίδια; Απ. 20.

Να βρεθεί πόσοι από τους ερωτηθέντες:

1) Δεν παρακολουθούν ούτε αθλητικές εκπομπές, ούτε ειδήσεις, ούτε τηλεπαιχνίδια.

2) Παρακολουθούν αθλητικές εκπομπές και ειδήσεις αλλά όχι τηλεπαιχνίδια.

3) Παρακολουθούν μόνο αθλητικές εκπομπές.

12) Από 100 φοιτητές του Τμήματος Πληροφορικής οι οποίοι ρωτήθηκαν αν είχαν επιλέξει τα κατ' επιλογήν μαθήματα: Γραφικά υπολογιστών (Γ), Βιοπληροφορική (Β) και Κρυπτογραφία (Κ), 33 δήλωσαν ότι είχαν επιλέξει το Γ, 43 το Β, 52 το Κ, 15 τα Γ και Κ, 17 τα Β και Κ, 10 και τα τρία, 10 κανένα από τα τρία. Να βρεθεί:

(i) Πόσοι είχαν επιλέξει τα Γ και Β.

(ii) Πόσοι είχαν επιλέξει μόνο το Β.

(iii) Πόσοι είχαν επιλέξει μόνο το Κ.

13) Να βρεθεί ο αριθμός των υποσυνόλων του [1000] με 50 στοιχεία τα οποία δεν περιέχουν κανένα πολλαπλάσιο των αριθμών 2, 3 και 5.

14) Να βρεθεί πόσοι φυσικοί αριθμοί από το 1 μέχρι το 1000 δεν διαιρούνται ούτε με το 2, ούτε με το 5 και δεν περιέχουν στα ψηφία τους τον αριθμό 7.

15) Για μια ομάδα 100 εθελοντών είναι γνωστές οι εξής πληροφορίες: Όλοι οι άνδρες είναι πάνω από 30 χρονών. Υπάρχουν 50 γυναίκες στην ομάδα. Υπάρχουν 60 εργαζόμενα άτομα πάνω από 30 χρονών. Υπάρχουν 25 παντρεμένες γυναίκες. Υπάρχουν 15 παντρεμένα εργαζόμενα άτομα πάνω από 30 ετών. Υπάρχουν 10 παντρεμένες γυναίκες πάνω από 30.

    Με βάση τα παραπάνω στοιχεία, να απαντηθούν οι εξής ερωτήσεις:

    i) Πόσα είναι τα παντρεμένα εργαζόμενα άτομα;

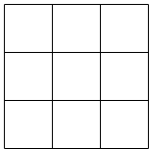
    ii) Πόσες ανύπαντρες γυναίκες είναι πάνω από 30;

    iii) Πόσοι ανύπαντροι άνδρες είναι κάτω από 30;

    iv) Πόσοι άνδρες είναι παντρεμένοι;

    v) Πόσα άτομα κάτω από τα 30 είναι εργαζόμενα;

16) Κάθε μοναδιαίο τετράγωνο του επόμενου σχήματος χρωματίζεται κόκκινο, μπλε ή κίτρινο.



    Με πόσους διαφορετικούς τρόπους μπορεί να χρωματισθεί το παραπάνω σχήμα έτσι ώστε να περιέχει τουλάχιστον ένα κόκκινο τετράγωνο με διαστάσεις 2 επί 2;

17) Σε μια στατιστική έρευνα στην οποία συμμετείχαν 100 άτομα καταγράφηκαν 3 χαρακτηριστικά: Φύλο (Άνδρας ή Γυναίκα), Οικογενειακή κατάσταση (Παντρεμένος ή Ανύπανδρος), Εργασιακή κατάσταση (Άνεργος ή Εργαζόμενος). Γνωρίζουμε ότι συμμετείχαν 54 άνδρες, 50 εργαζόμενα άτομα και 57 παντρεμένα άτομα. Επίσης, γνωρίζουμε ότι οι παντρεμένοι άνδρες ήταν 31, τα παντρεμένα εργαζόμενα άτομα ήταν 17 και οι εργαζόμενοι άνδρες 40. Τέλος, οι παντρεμένοι εργαζόμενοι άνδρες ήταν 17. Να βρεθούν οι τύποι (συνδυασμός χαρακτηριστικών) των ατόμων που δεν συμμετείχαν στην έρευνα αυτή.

18) Να δειχθεί ότι δεν υπάρχουν σύνολα A, B, C με $|A \cup B \cup C| = 100$, $|A| = 50$, $|B| = 45$, $|C| = 34$, $|A \cap B| = 20$ και $|A \cap B \cap C| = 10$.

19) Σε μια έρευνα ζητήθηκε η γνώμη των πολιτών για κάποιο σημαντικό ζήτημα. Μαζί με τα αποτελέσματα της έρευνας, δόθηκαν και τα παρακάτω στατιστικά στοιχεία σχετικά με τα άτομα που συμμετείχαν στην έρευνα.

	Άτομα που συμμετείχαν στη έρευνα: 1000	Άτομα με πτυχίο ανώτατης σχολής: 400
Άνδρες	600	300
Άνδρες άνω των 30 ετών	300	100
Άτομα άνω των 30 ετών	700	300

    Να εξετασθεί αν τα παραπάνω στατιστικά στοιχεία είναι συνεπή.

20) Σε μία στατιστική έρευνα ζητήθηκε από 100 μαθητές να συμπληρώσουν ένα ερωτηματολόγιο το οποίο μεταξύ άλλων ερευνούσε την γλωσσομάθεια των μαθητών. Όπως συνήθως, για τον έλεγχο της αξιοπιστίας των απαντήσεων, το ερωτηματολόγιο περιείχε αλληλοεπικαλυπτόμενες ερωτήσεις:

Ερώτηση 9: Γνωρίζετε Γαλλικά; 46 μαθητές απάντησαν θετικά.

Ερώτηση 12: Γνωρίζετε Ισπανικά; 27 μαθητές απάντησαν θετικά.

Ερώτηση 13: Γνωρίζετε Γερμανικά; 25 μαθητές απάντησαν θετικά.

Ερώτηση 19: Γνωρίζετε Γαλλικά και Γερμανικά; 19 μαθητές απάντησαν θετικά.

Ερώτηση 22: Γνωρίζετε Γαλλικά και Ισπανικά; 8 μαθητές απάντησαν θετικά.

Ερώτηση 30: Γνωρίζετε Ισπανικά και Γερμανικά; 10 μαθητές απάντησαν θετικά.

Ερώτηση 42: Γνωρίζετε Γαλλικά, Ισπανικά και Γερμανικά; 3 μαθητές απάντησα θετικά.

Με βάση τα παραπάνω στοιχεία, να δειχθεί ότι ορισμένοι μαθητές συμπλήρωσαν το ερωτηματολόγιο χωρίς να διαβάσουν τις ερωτήσεις.

21) Σε μία έρευνα που συμμετείχαν 100 φοιτητές καταγράφηκαν τα παρακάτω στατιστικά δεδομένα:

Αριθμός γυναικών	50
Αριθμός τελειόφοιτων	60
Αριθμός εργαζόμενων φοιτητών	55
Αριθμός μη τελειόφοιτων γυναικών	5
Αριθμός ανέργων γυναικών	30

Να βρεθούν φράγματα για τους αριθμούς των εργαζόμενων τελειόφοιτων γυναικών και των εργαζόμενων τελειόφοιτων.

2.2.3 Παράρτημα: Απαρίθμηση απεικονίσεων επί

Πρόταση 2.9 (**Αριθμός απεικονίσεων επί**). *Ο αριθμός των απεικονίσεων επί από το* $[n]$ *στο* $[k]$ *είναι ίσος με*

$$\sum_{j=0}^{k}(-1)^k\binom{k}{j}(k-j)^n.$$

Απόδειξη. Έστω S το σύνολο όλων των απεικονίσεων από το $[n]$ στο $[k]$. Ισχύει ότι $|S| = k^n$.

Έστω S_j το σύνολο όλων των απεικονίσεων από το $[n]$ στο $[k] \setminus \{j\}$. Ισχύει ότι $|S_i| = (k-1)^n$.

Για κάθε ακολουθία $j_1, j_2, \ldots, j_r$ στο $[k]$, το σύνολο $S_{j_1} \cap S_{j_2} \cap \cdots \cap S_{j_r}$ είναι το σύνολο όλων των απεικονίσεων από το $[n]$ στο $[k] \setminus \{j_1, j_2, \ldots, j_r\}$. Ισχύει ότι $|S_{j_1} \cap S_{j_2} \cap \cdots \cap S_{j_r}| = (k-r)^n$. Υπάρχουν $\binom{n}{r}$ διαφορετικές τομές των S_j με r όρους.

Το ζητούμενο σύνολο των απεικονίσεων επί είναι το σύνολο $\overline{S_1} \cap \overline{S_2} \cap \cdots \overline{S_k}$.

Από την αρχή εγκλεισμού-αποκλεισμού ισχύει ότι

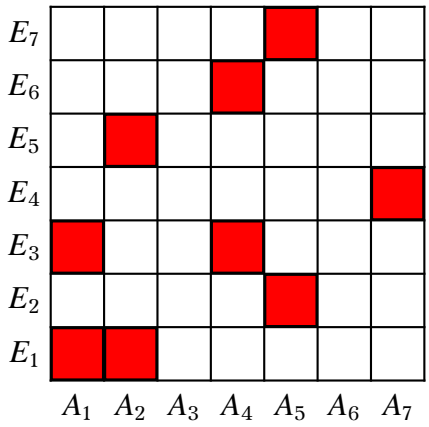
$$\begin{aligned}\left|\overline{S_1} \cap \overline{S_2} \cap \cdots \overline{S_k}\right| &= |S| - \sum_{j\in[k]}|S_j| + \sum_{\substack{j_1,j_2\in[k]\\ j_1<j_2}}|S_{j_1}\cap S_{j_2}| + \cdots + (-1)^r \sum_{\substack{j_1,j_2,\ldots,j_r\\ j_1<j_2<\cdots<j_r}}|S_{j_1}\cap S_{j_2}\cap\cdots\cap S_{j_r}| + \cdots \\ &\quad + (-1)^k|S_1\cap S_2\cap\cdots S_k| \\ &= k^n - \binom{k}{1}(k-1)^n + \binom{k}{2}(k-2)^n + \cdots + (-1)^r\binom{k}{r}(k-r)^n + \cdots + (-1)^k\binom{k}{k}(k-k)^n \\ &= \sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n.\end{aligned}$$

□

Ασκήσεις προς επίλυση

1) Να βρεθεί ο αριθμός των τρόπων με τους οποίους μπορεί να γίνει ανάθεση 7 ατομικών εργασιών E_1, E_2, E_3, E_4, E_5, E_6, E_7 σε 4 άτομα A_1, A_2, A_3, A_4 έτσι ώστε κάθε άτομο να αναλάβει τουλάχιστον μια εργασία.

2) Επτά φοιτητές $A_1, A_2, A_3, A_4, A_5, A_6, A_7$ πρέπει να αναλάβουν από μια από τις επτά εργασίες $E_1, E_2, E_3, E_4, E_5, E_6, E_7$. Ο A_1 δεν μπορεί να αναλάβει τις E_1 ή E_3, ο A_2 δεν μπορεί να αναλάβει τις E_1 ή E_5, ο A_4 δεν μπορεί να αναλάβει τις E_3 ή E_6, ο A_5 δεν μπορεί να αναλάβει τις E_2 ή E_7, ο A_7 δεν μπορεί να αναλάβει την E_4 και οι A_3 και A_6 μπορούν να αναλάβουν όλες τις εργασίες. Με πόσους τρόπους μπορεί να ανατεθούν οι επτά εργασίες στους επτά φοιτητές;



2.3 Αρχή του περιστερεώνα

Πρόταση 2.10 (Αρχή του περιστερεώνα I). *Έστω A, B δύο πεπερασμένα σύνολα.*

(i) Αν υπάρχει $1-1$ απεικόνιση $f : A \to B$, τότε $|A| \leq |B|$.

(ii) Αν υπάρχει απεικόνιση $f : A \to B$ η οποία είναι επί, τότε $|A| \geq |B|$.

Ισοδύναμα, χρησιμοποιώντας αντιθετοαναστροφή, η Πρόταση 2.10 διατυπώνεται ως εξής:

Πρόταση 2.11 (Αρχή του περιστερεώνα II). *Έστω A, B δύο πεπερασμένα σύνολα.*

(i) Αν $|A| > |B|$, τότε κάθε απεικόνιση $f : A \to B$ δεν είναι 1-1.

(ii) Αν $|A| < |B|$, τότε κάθε απεικόνιση $f : A \to B$ δεν είναι επί.

Η Πρόταση 2.11 (κυρίως το (i)) ονομάζεται **αρχή του περιστερεώνα** (ή **αρχή του Dirichlet**).

Στην πιο απλουστευμένη μορφή της (από την οποία έλαβε το ονομά της) η αρχή του περιστερεώνα διατυπώνει την προφανή παρατήρηση ότι:

Αν υπάρχουν n φωλιές (τα στοιχεία του B) για $n+1$ περιστέρια (τα στοιχεία του A), δεν είναι δυνατόν κάθε περιστέρι να έχει τη δική του φωλιά (και επομένως δύο περιστέρια θα μπούν στην ίδια φωλιά).

Η αρχή του περιστερεώνα έχει πολλές εφαρμογές όπως φαίνεται και από τα παρακάτω παραδείγματα.

Παράδειγμα 2.3.1. *Σε κάθε ομάδα 13 ατόμων υπάρχουν 2 άτομα που έχουν γενέθλια τον ίδιο μήνα.*

Απόδειξη. Πράγματι, αν A είναι το σύνολο των ατόμων και B το σύνολο των μηνών του έτους και $f : A \to B$ είναι η απεικόνιση η οποία αντιστοιχίζει σε κάθε άτομο τον μήνα που γεννήθηκε, τότε επειδή $|A| > |B|$ από την αρχή του περιστερεώνα έπεται ότι f δεν είναι $1-1$ και άρα υπάρχουν $x, y \in A$ με $x \neq y$ και $f(x) = f(y)$, δηλαδή οι x, y έχουν γενέθλια τον ίδιο μήνα. □

Παράδειγμα 2.3.2. *Ανάμεσα στους 7 δισεκατομμύρια ανθρώπους που ζουν αυτή τη στιγμή στη Γη υπάρχουν τουλάχιστον δύο που γεννήθηκαν στην ίδια ακριβώς στιγμή (έτος, ημέρα, ώρα, λεπτό, δευτερόλεπτο).*

Απόδειξη. Έστω A το σύνολο των ανθρώπων που ζουν αυτή τη στιγμή στη Γη και B το σύνολο όλων των στιγμών (έτος, ημέρα, ώρα, λεπτό, δευτερόλεπτο) των τελευταίων 150 ετών.

Αν θεωρήσουμε την απεικόνιση $f : A \to B$ που αντιστοιχίζει σε κάθε άτομο τη στιγμή που γεννήθηκε (έτος, ημέρα, ώρα, λεπτό, δευτερόλεπτο) τότε

$$|A| > 7 \text{ δισεκατομμύρια} = 7.000.000.000,$$
$$|B| = 150 \cdot 365 \cdot 24 \cdot 60 \cdot 60 = 4.743.360.000,$$

οπότε, από την αρχή του περιστερεώνα προκύπτει ότι η f δεν είναι 1-1, άρα υπάρχουν τουλάχιστον δύο άτομα που έχουν γεννηθεί την ίδια ακριβώς στιγμή. □

Παράδειγμα 2.3.3. *Σε κάθε τριάδα φυσικών αριθμών x, y, z υπάρχουν τουλάχιστον δύο που το άθροισμά τους είναι άρτιος.*

Απόδειξη. Πραγματικά, έστω $A = \{x, y, z\}$ το σύνολο των τριών ακεραίων και B το σύνολο $\{0, 1\}$.

Έστω $f : A \to B$ η απεικόνιση η οποία αντιστοιχίζει σε κάθε ακέραιο του A την τιμή 0 αν είναι άρτιος και την τιμή 1 αν είναι περιττός.

Επειδή $|A| > |B|$ από την αρχή του περιστερεώνα δύο τουλάχιστον από τους αριθμούς $\{x, y, z\}$ θα αντιστοιχίζονται στην ίδια τιμή 0 ή 1, δηλαδή θα είναι και οι δύο ή άρτιοι ή περιττοί.

Επομένως, το άθροισμά τους θα είναι άρτιος. □

Παράδειγμα 2.3.4. *Αν διαλέξουμε $n + 1$ διαφορετικούς αριθμούς από το σύνολο $[2n]$, τότε:*

(i) Υπάρχουν δύο αριθμοί από αυτούς που διαλέξαμε που διαφέρουν ακριβώς κατά n.

Απόδειξη. Έστω A το σύνολο των $n+1$ αριθμών που διαλέξαμε και B το σύνολο των ζευγών

$$\{\{1, n+1\}, \{2, n+2\}, \{3, n+3\}, \ldots, \{n, 2n\}\}.$$

Προφανώς τα ζεύγη του B αποτελούν μια διαμέριση του $[2n]$ με την ιδιότητα τα στοιχεία κάθε ζεύγους να διαφέρουν ακριβώς n. Θεωρούμε την απεικόνιση $f : A \to B$ η οποία αντιστοιχίζει τον αριθμό x του A στο ζεύγος του B που περιέχει το x. Επειδή

$$n + 1 = |A| > |B| = n,$$

από την αρχή του περιστερεώνα έπεται ότι η f δεν είναι $1-1$ και άρα υπάρχουν $x, y \in A$ με $f(x) = f(y)$, δηλαδή τα x, y διαφέρουν ακριβώς κατά n. □

(ii) Υπάρχουν δύο αριθμοί από αυτούς που διαλέξαμε που είναι διαδοχικοί.

Απόδειξη. Ορίζεται το ίδιο σύνολο A ενώ για σύνολο B θεωρούμε το σύνολο των ζευγών

$$\{\{1, 2\}, \{3, 4\}, \{5, 6\}, \ldots, \{2n-1, 2n\}\}.$$

Προφανώς τα ζεύγη του B αποτελούν μια διαμέριση του $[2n]$ με την ιδιότητα τα στοιχεία κάθε ζεύγους να είναι διαδοχικοί αριθμοί. Θεωρούμε την απεικόνιση $g : A \to B$ η οποία αντιστοιχίζει τον αριθμό x του A στο ζεύγος του B που περιέχει το x. Επειδή

$$n + 1 = |A| > |B| = n,$$

από την αρχή του περιστερεώνα έπεται ότι η g δεν είναι $1-1$ και άρα υπάρχουν $x, y \in A$ με $g(x) = g(y)$, δηλαδή τα x, y είναι διαδοχικοί αριθμοί. □

(iii) Υπάρχουν δύο αριθμοί από αυτούς που διαλέξαμε που έχουν άθροισμα $2n + 1$.

(Υπόδειξη: Θεωρήστε το σύνολο

$$\{\{1, 2n\}, \{2, 2n-1\}, \ldots, \{n, n+1\}\}.)$$

(iv) Υπάρχουν δύο αριθμοί από αυτούς που διαλέξαμε, που ο ένας διαιρεί τον άλλο.

Απόδειξη. Πραγματικά, εστω $A = \{a_1, a_2, \ldots, a_{n+1}\}$ το σύνολο των αριθμών που διαλέξαμε. Για κάθε $i \in [n+1]$ ο αριθμός a_i του A γράφεται κατα μοναδικό τρόπο υπό την μορφή

$$a_i = 2^{k_i}\rho_i,$$

όπου $k_i \in \mathbb{N}$ και ρ_i περιττός αριθμός. Επειδή $\rho_i \leq a_i \leq 2n$ και ρ_i περιττός έπεται ότι υπάρχουν το πολύ n διαφορετικά ρ_i. Έστω B το σύνολο των ρ_i. Τότε $|B| \leq n < n+1 = |A|$. Άρα, από την αρχή του περιστερεώνα η απεικόνιση $f : A \to B$ με $f(a_i) = \rho_i$ δεν είναι $1-1$. Άρα, υπάρχουν τουλάχιστον δύο στοιχεία a_i, a_j του A με $f(a_i) = f(a_j)$, δηλαδή $\rho_i = \rho_j = \rho$. Τότε όμως έχουμε $a_i = 2^{k_i}\rho$ και $a_j = 2^{k_j}\rho$. Έστω $k_i > k_j$ (εργαζόμαστε αντίστοιχα αν $k_i < k_j$), οπότε υπάρχει $m \in \mathbb{N}^*$ με $k_i = k_j + m$. Τότε,

$$\begin{aligned} a_i &= 2^{k_i}\rho = 2^{k_j+m}\rho = 2^{k_j}2^m\rho \\ &= 2^m 2^{k_j}\rho = 2^m a_j, \end{aligned}$$

δηλαδή ο a_i είναι πολλαπλάσιο του a_j. □

Παράδειγμα 2.3.5. *Αν διαλέξουμε $n+1$ διαφορετικούς φυσικούς αριθμούς τότε υπάρχουν τουλάχιστον δύο μεταξύ αυτών τέτοιοι ώστε η διαφορά τους να είναι πολλαπλάσιο του n.*

Απόδειξη. Πράγματι, έστω A το σύνολο των $n+1$ φυσικών αριθμών και $f : A \to \mathbb{N}$ όπου $f(x)$ το υπόλοιπο της διαίρεσης του $x \in A$ με το n.

Προφανώς, για κάθε $x \in A$ ισχύει ότι $f(x) \in \{0, 1, 2, \ldots, n-1\}$.

Επειδή

$$|A| = n+1 > n = |\{0, 1, 2, \ldots, n-1\}|,$$

από την αρχή του περιστερεώνα έπεται ότι η f δεν είναι 1-1, άρα υπάρχουν $x, y \in A$ με $f(x) = f(y)$, δηλαδή τα x, y έχουν το ίδιο υπόλοιπο υ όταν διαιρεθούν με το n. Άρα, η διαφορά τους $x - y$ θα έχει υπόλοιπο μηδέν όταν διαιρεθεί με το n, δηλαδή ο $x - y$ είναι πολλαπλάσιο του n. □

Παράδειγμα 2.3.6. *Από το σύνολο των αριθμών $\{1, 2, 3, 4, 5, 6, 7, 8\}$ επιλέγονται 6 αριθμοί. Να δειχθεί ότι υπάρχουν τουλάχιστον δύο από τους έξι αυτούς αριθμούς με άθροισμα 11.*

Απόδειξη. Τα 5 σύνολα $\{1\}$, $\{2\}$, $\{3, 8\}$, $\{4, 7\}$, $\{5, 6\}$ αποτελούν μια διαμέριση του $[8]$.

Έστω A το σύνολο των 6 αριθμών που επιλέχθηκαν, B το σύνολο των 5 προηγουμένων υποσυνόλων και $f : A \to B$ όπου $f(x)$ το σύνολο του B στο οποίο ανήκει το x.

Επειδή $|A| = 6 > 5 = |B|$, από την αρχή του περιστερεώνα, έπεται ότι η f δεν είναι $1-1$, άρα υπάρχουν $x, y \in A$ με $f(x) = f(y)$. Επειδή, $|\{1\}| = |\{2\}| = 1$ έπεται ότι υπάρχουν x, y με $f(x) = f(y) \in \{\{3, 8\}, \{4, 7\}, \{5, 6\}\}$. Άρα, το άθροισμά τους ισούται με 11. □

Παράδειγμα 2.3.7. *Έστω A το σύνολο 10 αριθμών μεταξύ του 1 και του 100. Να δειχθεί ότι υπάρχουν τουλάχιστον δύο υποσύνολα του A με το ίδιο άθροισμα στοιχείων.*

Απόδειξη. Ο αριθμός των υποσυνόλων που σχηματίζουν οι 10 αριθμοί ισούται με $2^{10} = 1024$. Έστω A το σύνολο όλων αυτών των υποσυνόλων.

Θεωρούμε την απεικόνιση $f : A \to \mathbb{N}$ με $f(X)$ το άθροισμα των στοιχείων του υποσυνόλου $X \in A$.

Επειδή οι 10 αριθμοί ανήκουν στο διάστημα [100] έπεται ότι για κάθε $X \in A$ ισχύει ότι $f(X) < 10 \cdot 100 = 1000$, δηλαδή $f(A) \subseteq [1000]$.

Επειδή $|A| = 1024 > 1000 \geq |f(A)|$ έπεται ότι η f δεν είναι 1-1, άρα υπάρχουν υποσύνολα X, Y στο A με $f(X) = f(Y)$. □

Παρατήρηση. Το παράδειγμα αυτό γενικεύται ως εξής: Έστω n αριθμοί μεταξύ του 1 και του m, όπου $2^n > mn$. Να δειχθεί ότι υπάρχουν τουλάχιστον δύο υποσύνολα αυτών των n αριθμών με το ίδιο άθροισμα στοιχείων.

Να σημειωθεί ότι ενώ υπάρχουν τέτοια υποσύνολα με το ίδιο άθροισμα είναι κατά κανόνα δύσκολο να τα βρούμε με κάποιο αλγόριθμο.

Παράδειγμα 2.3.8. *Δίδονται δεκατρείς διαφορετικοί πραγματικοί αριθμοί. Να δειχθεί ότι ανάμεσά τους υπάρχουν δύο, έστω οι x, y, για τους οποίους ισχύει η ανισότητα*

$$0 < \frac{x-y}{1+xy} < \sqrt{\frac{2-\sqrt{3}}{2+\sqrt{3}}}.$$

Απόδειξη. Είναι γνωστό ότι η απεικόνιση $\tan : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$ είναι επί. Επομένως, για κάθε $z \in \mathbb{R}$ υπάρχει $\theta_z \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ ώστε $\tan(\theta_z) = z$. Θεωρούμε τα θ_z που αντιστοιχούν στους 13 αυτούς αριθμούς.

Αν χωρίσουμε το διάστημα $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ σε 12 ίσα τμήματα μήκους $\frac{\pi}{12}$ τότε από την αρχή του περιστερεώνα, δύο τουλάχιστον από τα θ_z, έστω οι θ_x, θ_y με $\theta_x > \theta_y$, θα ανήκουν στο ίδιο διάστημα και επομένως

$$0 < \theta_x - \theta_y < \frac{\pi}{12}.$$

Επειδή η tan είναι αύξουσα στο $(0, \frac{\pi}{12})$ έπεται ότι

$$\tan 0 < \tan(\theta_x - \theta_y) < \tan\frac{\pi}{12} = \tan\left(\frac{\pi}{4} - \frac{\pi}{6}\right).$$

Χρησιμοποιώντας την ταυτότητα $\tan(a-b) = \frac{\tan a - \tan b}{1+\tan a \tan b}$ έπεται ότι

$$0 < \frac{\tan\theta_x - \tan\theta_y}{1+\tan\theta_x\tan\theta_y} < \frac{\tan\frac{\pi}{4} - \tan\frac{\pi}{6}}{1+\tan\frac{\pi}{4}\tan\frac{\pi}{6}}$$

οπότε

$$0 < \frac{x-y}{1+xy} < \frac{1-\frac{1}{\sqrt{3}}}{1+\frac{1}{\sqrt{3}}} = \sqrt{\frac{(\sqrt{3}-1)^2}{(\sqrt{3}+1)^2}} = \sqrt{\frac{2-\sqrt{3}}{2+\sqrt{3}}}$$

δηλαδή

$$0 < \frac{x-y}{1+xy} < \sqrt{\frac{2-\sqrt{3}}{2+\sqrt{3}}}.$$

□

Παράδειγμα 2.3.9. *Αν υπάρχουν n άτομα σε ένα δωμάτιο, τότε υπάρχουν δύο τουλάχιστον άτομα που έχουν τον ίδιο αριθμό φίλων στο δωμάτιο. (Θεωρούμε ότι η σχέση φιλίας είναι συμμετρική).*

Απόδειξη. Πραγματικά, έστω A το σύνολο των n ατόμων και $f : A \to \mathbb{N}$ με $f(x)$ το πλήθος των φίλων του $x \in A$. Προφανώς,

$$0 \leq f(x) \leq n-1.$$

Παρατηρούμε ότι δεν είναι δυνατόν να υπάρχουν

$$x, y \in A \text{ με } f(x) = 0 \text{ και } f(y) = n-1.$$

διότι δεν είναι δυνατόν ταυτόχρονα κάποιος να μην έχει κανένα φίλο στο δωμάτιο και κάποιος άλλος να είναι φίλος με όλα τα άτομα που βρίσκονται στο δωμάτιο.

Άρα,

$$\text{ή } f(x) \in \{0, 1, \ldots, n-2\} \text{ για κάθε } x \in A,$$
$$\text{ή } f(x) \in \{1, 2, \ldots, n-1\} \text{ για κάθε } x \in A.$$

Επειδή

$$|A| = n > n-1 = |\{0, 1, \ldots, n-2\}| = |\{1, 2, \ldots, n-1\}|,$$

από την αρχή του περιστερεώνα έπεται ότι η f δεν είναι $1-1$, άρα υπάρχουν $x, y \in A$ με $f(x) = f(y)$, δηλαδή οι x, y έχουν τον ίδιο αριθμό φίλων στο δωμάτιο. □

Παράδειγμα 2.3.10. *Τα 52 φύλλα της τράπουλας χωρίζονται σε 4 χρώματα: καρά, κούπες, πίκες, σπαθιά. Σε κάθε χρώμα υπάρχουν 13 φύλλα τα οποία αριθμούνται κυκλικά με την εξής σειρά: 2, 3, 4, 5, 6, 7, 8, 9, J, Q, K, A δηλαδή μετά το A ακολουθεί πάλι το 2, κ.ο.κ.*

Να δειχθεί ότι σε κάθε επιλογή 5 φύλλων από μια τράπουλα υπάρχουν τουλάχιστον 2 φύλλα με το ίδιο χρώμα τα οποία επιπλέον απέχουν στην κυκλική διάταξη το πολύ 6 θέσεις.

Απόδειξη. Πράγματι, αφού επιλέγονται 5 φύλλα και υπάρχουν μόνο 4 χρώματα, από την αρχή του περιστερεώνα έπεται ότι δύο τουλάχιστον φύλλα x, y θα έχουν το ίδιο χρώμα.

Επιπλέον, αν $|x-y|$ είναι ο αριθμός των φύλλων από το x μέχρι και το y και $|y-x|$ ο αριθμός των φύλλων από το y μέχρι και το x (στην παραπάνω κυκλική διάταξη) τότε $|x-y| + |y-x| = 13$.

Επομένως, πάλι από την αρχή του περιστερεώνα ένας τουλάχιστον από τους αριθμούς $|x-y|$ και $|y-x|$ είναι μικρότερος ή ίσος του 6. □

Παράδειγμα 2.3.11. *(α) Έστω ότι 17 άτομα σχηματίζουν ένα κύκλο στον οποίο δεν υπάρχουν δύο διαδοχικές γυναίκες. Να δειχθεί ότι στον κύκλο μπορεί να υπάρχουν το πολύ 8 γυναίκες.*

(β) 17 άνδρες και 17 γυναίκες σχηματίζουν κύκλο. Να δειχθεί ότι υπάρχει τουλάχιστον ένα άτομο που έχει αριστερά και δεξιά του γυναίκα.

Λύση. (α) Παρατηρούμε ότι κάθε γυναίκα που εμφανίζεται στον κύκλο έχει στα δεξιά της ένα (διαφορετικό) άνδρα. Αν στον κύκλο υπάρχουν $k \geq 9$ γυναίκες τότε ο κύκλος θα περιέχει τουλάχιστον k άνδρες, το οποίο είναι άτοπο διότι $2k \geq 18 > 17$.

(β) Έστω ότι δεν υπάρχει άτομο που έχει αριστερά και δεξιά του γυναίκα.

Αριθμούμε κυκλικά τα 34 άτομα (ξεκινώντας από οποιοδήποτε άτομο).

Τα 17 άτομα με άρτια αρίθμηση και τα 17 άτομα με περιττή αρίθμηση σχηματίζουν δύο νέους κύκλους, στους οποίους δεν υπάρχουν δύο διαδοχικές γυναίκες. (Αλλιώς θα υπήρχε ένα άτομο μεταξύ τους στον αρχικό κύκλο.)

Όμως, σε κάθε κύκλο με 17 άτομα στον οποίο δεν υπάρχουν δύο διαδοχικές γυναίκες, προκύπτει ότι μπορεί να περιλαμβάνονται το πολύ 8 γυναίκες.

Επομένως, στους δύο κύκλους που σχηματίσθηκαν μπορούν να περιλαμβάνονται το πολύ 8 + 8 = 16 γυναίκες, το οποίο είναι άτοπο.

Άρα, υπάρχει άτομο που έχει αριστερά και δεξιά του γυναίκα. □

Στη συνέχεια παρουσιάζονται διάφορες χρήσιμες παραλλαγές της αρχής του περιστερεώνα.

Πρόταση 2.12 (Γενικευμένη αρχή του περιστερεώνα). *Έστω A, B πεπερασμένα σύνολα.*

i) Αν $|A| = k|B| + 1$, τότε για κάθε $f : A \to B$ υπάρχει στοιχείο του B το οποίο είναι εικόνα τουλάχιστον $k+1$ στοιχείων του A, δηλαδή υπάρχει $y \in B$ ώστε $\left|f^{-1}(y)\right| \geq k+1$.

ii) Για κάθε $f : A \to B$ με $|A| > |B|$ υπάρχει $y \in B$ το οποίο είναι εικόνα τουλάχιστον $\lceil \frac{|A|}{|B|} \rceil$ προτύπων[3].

Απόδειξη.

i) Έστω ότι $\left|f^{-1}(y)\right| \leq k$ για κάθε $y \in B$. Τότε

$$\left|f^{-1}(B)\right| = \left|\bigcup_{y\in B} f^{-1}(y)\right| \leq \sum_{y\in B} |f^{-1}(y)| \leq \sum_{y\in B} k = k|B| < k|B| + 1 = |A|,$$

το οποίο είναι άτοπο, αφού για κάθε απεικόνιση $f : A \to B$ ισχύει ότι $f^{-1}(B) = A$.

Άρα, υπάρχει τουλάχιστον ένα $y \in B$ ώστε $\left|f^{-1}(y)\right| \geq k+1$.

ii) Άσκηση. □

Παράδειγμα 2.3.12. *Σε ένα συνέδριο συμμετέχουν 161 άτομα από 10 χώρες. Να δειχθεί ότι μια τουλάχιστον χώρα είχε στείλει στο συνέδριο τουλάχιστον 17 άτομα,*

Απόδειξη. Πράγματι, έστω A το σύνολο των 161 ατόμων και B το σύνολο των 10 χωρών. Έστω $f : A \to B$ με $f(x)$ η χώρα από την οποία προέρχεται ο $x \in A$. Επειδή $|A| = 16 \cdot |B| + 1$, από την γενικευμένη αρχή του περιστερεώνα (Πρόταση 2.12), υπάρχει τουλάχιστον ένα $y \in B$ ώστε $\left|f^{-1}(y)\right| \geq 16+1 = 17$, δηλαδή υπάρχει χώρα y από την οποία προέρχονται τουλάχιστον 17 άτομα. □

Παράδειγμα 2.3.13. *Σε κάποιο online διαγωνισμό τραγουδιού ψηφίζουν 10000 κριτές. Καθένας από αυτούς επιλέγει οκτώ (διαφορετικά) τραγούδια. Στο διαγωνισμό συμμετέχουν συνολικά 600 διαφορετικά τραγούδια. Να δειχθεί ότι υπάρχει τουλάχιστον ένα τραγούδι το οποίο έχει επιλεγεί από τουλάχιστον 134 κριτές.*

[3] $\lceil x \rceil$ είναι ο ελάχιστος ακέραιος, που είναι μεγαλύτερος ή ίσος του x, $x \in \mathbb{R}$.

Απόδειξη. Έστω A το σύνολο των ψήφων για όλα τα τραγούδια – προφανώς, κάθε τραγούδι εμφανίζεται τόσες φορές όσοι και οι κριτές που το επέλεξαν – και B το σύνολο όλων των τραγουδιών.

Ισχύει ότι $|A| = 10000 \cdot 8 = 80000$ και $|B| = 600$.

Αν $f : A \to B$ είναι η απεικόνιση που αντιστοιχίζει στην επιλογή κάθε κριτή το αντίστοιχο τραγούδι, τότε, από την γενικευμένη αρχή του περιστερεώνα (Πρόταση 2.12), υπάρχει κάποιο τραγούδι το οποίο έχει επιλεγεί από τουλάχιστον $\lceil \frac{80000}{600} \rceil = 134$ κριτές. □

Παράδειγμα 2.3.14. *Σε μια 5×5 σκακιέρα τοποθετούνται 11 πύργοι. Να δειχθεί ότι πάντα μπορούμε να επιλέξουμε 3 από αυτούς οι οποίοι δεν απειλούνται μεταξύ τους. (Δύο πύργοι απειλούνται αν και μόνο αν βρίσκονται στην ίδια γραμμή ή στην ίδια στήλη της σκακιέρας).*

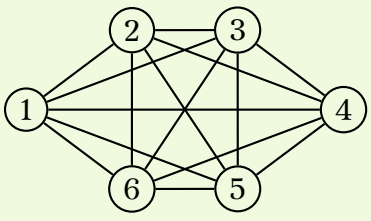
Λύση. Διαμερίζουμε τα τετράγωνα της 5×5 σκακιέρας σε 5 ομάδες όπως φαίνεται στο σχήμα.

1	**2**	**3**	**4**	**5**
2	**3**	**4**	**5**	**1**
3	**4**	**5**	**1**	**2**
4	**5**	**1**	**2**	**3**
5	**1**	**2**	**3**	**4**

Παρατηρούμε ότι όσοι πύργοι τοποθετηθούν στην ίδια ομάδα τετραγώνων δεν απειλούνται μεταξύ τους.

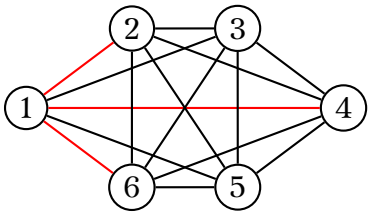
Έστω A το σύνολο των 11 πύργων και B το σύνολο των 5 ομάδων. Αν $f : A \to B$ είναι η απεικόνιση που αντιστοιχίζει σε κάθε πύργο την ομάδα τετραγώνων στην οποία τοποθετήθηκε τότε επειδή $|A| = 11$ και $|B| = 5$, από την γενικευμένη αρχή του περιστερεώνα (Πρόταση 2.12), υπάρχει κάποια ομάδα τετραγώνων στην οποία έχουν τοποθετηθεί τουλάχιστον $\lceil \frac{11}{5} \rceil = 3$ πύργοι. Άρα, υπάρχουν 3 πύργοι οι οποίοι δεν απειλούνται μεταξύ τους. □

Παράδειγμα 2.3.15. *Κάθε γραμμή του επόμενου σχήματος χρωματίζεται κόκκινη ή πράσινη. Να δειχθεί ότι σε κάθε χρωματισμό που θα προκύψει θα υπάρχει ένα κόκκινο τρίγωνο ή/και ένα πράσινο τρίγωνο.*

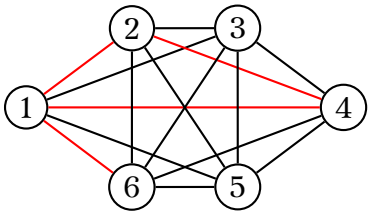


Λύση. Το σχήμα περιέχει $\binom{6}{2} = 15$ γραμμές και κάθε γραμμή έχει 2 τρόπους χρωματισμούς, άρα συνολικά υπάρχουν $2^{15} = 32768$ διαφορετικοί τρόποι χρωματισμού των γραμμών του.

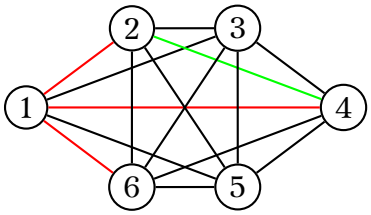
Επειδή η κορυφή 1 είναι άκρο 5 γραμμών και κάθε μία από τις 5 γραμμές χρωματίζεται κόκκινη ή πράσινη, από την γενικευμένη αρχή του περιστερεώνα έπεται ότι τουλάχιστον $\lceil \frac{5}{2} \rceil = 3$ από τις γραμμές της θα έχουν το ίδιο χρώμα. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι αυτές οι 3 γραμμές έχουν χρωματισθεί κόκκινες και συνδέουν την 1 με τις 2, 4 και 6.



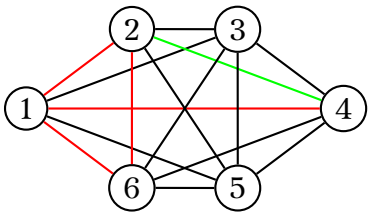
Διακρίνουμε τις παρακάτω **εμφωλευμένες** περιπτώσεις:
Αν η γραμμή 2 – 4 είναι κόκκινη, τότε υπάρχει το κόκκινο τρίγωνο 124.



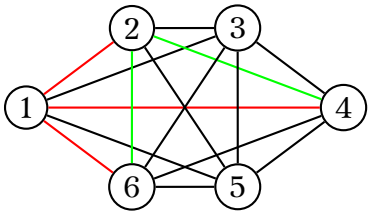
Αλλιώς, η γραμμή 2 – 4 είναι πράσινη.



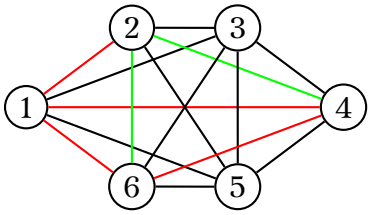
Αν η γραμμή 2 – 6 είναι κόκκινη, τότε υπάρχει το κόκκινο τρίγωνο 126.



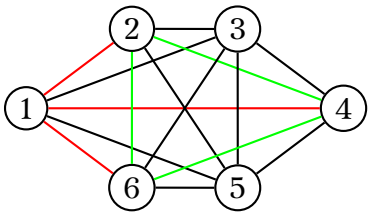
Αλλιώς, η γραμμή 2 – 6 είναι πράσινη.



Αν η γραμμή 4 – 6 είναι κόκκινη, τότε υπάρχει το κόκκινο τρίγωνο 146.



Αλλιώς, η γραμμή $4-6$ είναι πράσινη και τότε υπάρχει το πράσινο τρίγωνο 246.



Άρα, σε κάθε περίπτωση υπάρχει ένα κόκκινο ή/και πράσινο τρίγωνο. □

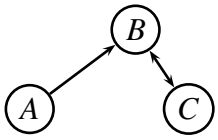
Παράδειγμα 2.3.16. *Ένα ad hoc ασύρματο δίκτυο αποτελείται από $n \geq 3$ αναμεταδότες και κάθε αναμεταδότης στέλνει την πληροφορία μόνο στον πλησιέστερο αναμεταδότη. Οι αποστάσεις μεταξύ των αναμεταδοτών είναι ανά δύο διαφορετικές. Να δειχθεί ότι αν το πλήθος των αναμεταδοτών είναι περιττός αριθμός, τότε κάποιος αναμεταδότης δεν λαμβάνει πληροφορία από κανέναν άλλο.*

Λύση. Προκειμένου όλοι να λαμβάνουν πληροφορία από κάποιον άλλο πρέπει να μην υπάρχει κάποιος αναμεταδότης που λαμβάνει πληροφορία από περισσότερους από έναν αναμεταδότη.

Επίσης, παρατηρούμε ότι επειδή οι αποστάσεις ανάμεσα στους αναμεταδότες είναι ανά δύο διαφορετικές έπεται ότι οι δύο κοντινότεροι αναμεταδότες θα στέλνουν την πληροφορία ο ένας στον άλλο.

Θα χρησιμοποιήσουμε επαγωγή ως προς τον αριθμό $2k+1$ των αναμεταδοτών.

Αν το δίκτυο αποτελείται από 3 αναμεταδότες, τότε οι δύο κοντινότεροι από αυτούς θα στέλνουν την πληροφορία ο ένας στον άλλο και ο τρίτος θα στέλνει την πληροφορία σε έναν από τους δύο κοντινότερους, οπότε ο ίδιος δεν θα λαμβάνει πληροφορία. Επομένως, το συμπέρασμα ισχύει για 3 αναμεταδότες.



Έστω ότι το συμπέρασμα ισχύει για κάθε δίκτυο με $2k+1 \geq 3$ αναμεταδότες.

Σε κάθε δίκτυο με $2(k+1)+1 = 2k+3$ αναμεταδότες, οι δύο κοντινότεροι θα στέλνουν την πληροφορία ο ένας στον άλλο.

Διακρίνουμε δύο περιπτώσεις:

Αν κάποιος από τους υπόλοιπους $2k+1$ στέλνει την πληροφορία σε έναν από τους δύο κοντινότερους, τότε τουλάχιστον ένας από αυτούς τους $2k+1$ δεν θα λαμβάνει πληροφορία από κανένα.

Αλλιώς, οι υπόλοιποι $2k+1$ αναμεταδότες αποτελούν ένα ad hoc ασύρματο δίκτυο με τις ίδιες ιδιότητες και άρα από την υπόθεση της επαγωγής υπάρχει τουλάχιστον ένας αναμεταδότης που δεν λαμβάνει πληροφορία από κανέναν άλλο. □

Αλγόριθμοι συμπίεσης αρχείων

Κάθε αρχείο είναι μια δυαδική λέξη, δηλαδή είναι μια λέξη που αποτελείται από τα ψηφία 0 ή 1. Ένα από τα βασικά χαρακτηριστικά ενός αρχείου είναι το μέγεθός του.

Έστω $\{0,1\}^*$ το σύνολο όλων των δυαδικών λέξεων (δηλαδή όλων των αρχείων).

$$\{0,1\}^* = \{0, 1, 00, 01, 10, 11, 000, \ldots\}.$$

Αν $\alpha \in \{0,1\}^*$, με $l(\alpha)$ συμβολίζουμε το μήκος της λέξης α, δηλαδή το πλήθος των γραμμάτων της.

Για παράδειγμα, $l(0) = l(1) = 1$, $l(01) = l(11) = 2$, $l(01110) = 5$.

Μια μέθοδος για την αποδοτικότερη αποθήκευση (και μεταφορά) αρχείων είναι η χρήση αλγορίθμων συμπίεσης αρχείων χωρίς απώλειες (lossless).

Ερώτηση. Τι είναι αλγόριθμος συμπίεσης χωρίς απώλειες;

Ένας **αλγόριθμος συμπίεσης αρχείων χωρίς απώλειες** μπορεί να περιγραφεί από μια απεικόνιση $f : \{0,1\}^* \to \{0,1\}^*$ η οποία ικανοποιεί τις εξής ιδιότητες:

1. f είναι 1–1,
2. υπάρχει τουλάχιστον ένα αρχείο $\alpha \in \{0,1\}^*$ με $l(f(\alpha)) < l(\alpha)$.

Η πρώτη ιδιότητα εκφράζει το γεγονός ότι σε κάθε συμπιεσμένο αρχείο αντιστοιχεί μοναδικό αρχικό αρχείο και επομένως επιτρέπει την δυνατότητα ανάκτησης του αρχικού αρχείου, δηλαδή επιτρέπει την αντιστροφή της διαδικασίας συμπίεσης.

Η δεύτερη ιδιότητα εκφράζει το γεγονός ότι υπάρχει ένα αρχείο το οποίο πράγματι συμπιέζεται από τον αλγόριθμο, δηλαδή του οποίου το μέγεθος μειώνεται.

Γνωστοί αλγόριθμοι συμπίεσης αρχείων, χωρίς απώλειες: zip, 7zip, rar, bzip2, ace, gzip, huffman.

Ερώτηση. Υπάρχει αλγόριθμος συμπίεσης αρχείων χωρίς απώλειες ο οποίος για κάθε αρχείο να παράγει συμπιεσμένα αρχεία με μέγεθος μικρότερο από το αρχικό;

Θα αποδείξουμε ότι η απάντηση είναι αρνητική. Για το σκοπό αυτό θα χρησιμοποιήσουμε την μέθοδο της εις άτοπον απαγωγής. Έστω ότι υπάρχει αλγόριθμος συμπίεσης χωρίς απώλειες ο οποίος για κάθε αρχείο παράγει συμπιεσμένα αρχεία με μέγεθος μικρότερο ή ίσο από το αρχικό.

Έστω $f : \{0,1\}^* \to \{0,1\}^*$ η απεικόνιση για την οποία $f(x)$ είναι το αποτέλεσμα της συμπίεσης της λέξης x από τον αλγόριθμο.

Από τον ορισμό υπάρχει τουλάχιστον μια λέξη $\alpha \in \{0,1\}^*$ με $l(f(\alpha)) < l(\alpha)$, δηλαδή η λέξη α να συμπιέζεται από την f.

Έστω ότι το μήκος του συμπιεσμένου αρχείου $f(\alpha)$ ισούται με n, δηλαδή $l(f(\alpha)) = n$· τότε $l(\alpha) > n$.

Θεωρούμε το σύνολο A_n όλων των δυαδικών λέξεων μήκους το πολύ n. Προφανώς, $f(a) \in A_n$.

Αν $l(f(x)) \leq l(x)$ για κάθε $x \in A_n$, έπεται ότι

$$f(x) \in A_n, \text{ για κάθε } x \in A_n.$$

Παρατηρούμε ότι επειδή $l(\alpha) > n$ ισχύει ότι $\alpha \notin A_n$.

Επειδή η f είναι 1-1 προκύπτει ότι

$$f(\alpha) \neq f(x) \text{ για κάθε } x \in A_n$$

και επομένως,

$$f(x) \in A_n \setminus \{f(\alpha)\} \text{ για κάθε } x \in A_n.$$

Θεωρώντας τον περιορισμό της f στο A_n θα έχουμε

$$f : A_n \to B_n = A_n \setminus \{f(\alpha)\},$$

το οποίο είναι άτοπο διότι

$$|A_n| > |A_n| - 1 = |A_n \setminus \{f(a)\}| = |B_n|.$$

Από τα παραπάνω προκύπτει η επόμενη πρόταση.

Πρόταση 2.13 (Συμπίεση χωρίς απώλειες και αρχή του περιστερεώνα). *Κάθε αλγόριθμος συμπίεσης χωρίς απώλειες αναγκαστικά παράγει κάποια αρχεία με μέγεθος μεγαλύτερο από το αρχικό τους.*

Το αποτελεσμα αυτό μοιάζει απογητευτικό για τους αλγόριθμους συμπίεσης χωρίς απώλειες, στην πράξη όμως αυτό που μας ενδιαφέρει είναι ένας αλγόριθμος να μειώνει το μέγεθος των αρχείων που εμφανίζονται συχνά, ακόμα και αν μεγαλώνει το μέγεθος κάποιων αρχείων που αν και περισσότερα δεν εμφανίζονται σχεδόν ποτέ ως είσοδος.

Αναζήτηση της χειρότερης περίπτωσης

Η αρχή του περιστερεώνα έχει εφαρμογές και στην εύρεση της χειρότερης περίπτωσης κατά την αναζήτηση στοιχείων με συγκεκριμένες ιδιότητες.

Πρόταση 2.14. *Έστω S ένα πεπερασμένο σύνολο με $|S| = n$ και $S_1, S_2, \ldots, S_k$ μια διαμέριση του S σε k υποσύνολα, όπου $k < n$. Να βρεθεί ο ελάχιστος αριθμός στοιχείων του S που πρέπει να επιλέξουμε, ώστε να εξασφαλίσουμε ότι*

i) δύο τουλάχιστον ανήκουν στο ίδιο υποσύνολο,

ii) δύο τουλάχιστον ανήκουν σε διαφορετικά υποσύνολα,

iii) ένα τουλάχιστον ανήκει στο υποσύνολο S_j, όπου $j \in [k]$,

iv) υπάρχουν στοιχεία από κάθε υποσύνολο,

v) r τουλάχιστον ανήκουν στο ίδιο σύνολο.

Λύση.

i) Επειδή $k < n$, από την αρχή του περιστερεώνα υπάρχει υποσύνολο της διαμέρισης με τουλάχιστον δύο στοιχεία. Αρκεί να επιλέξουμε $k+1$ στοιχεία από το S. Πράγματι, έστω A το σύνολο των $k+1$ στοιχείων και $f : A \to \{S_1, S_2, \ldots, S_k\}$, με $f(x)$ το υποσύνολο στο οποίο ανήκει το x. Επειδή $|A| = k+1 > k = |\{S_1, S_2, \ldots, S_k\}|$, από την αρχή του περιστερεώνα δύο τουλάχιστον στοιχεία θα ανήκουν στο ίδιο υποσύνολο.

ii) Αρκεί να επιλέξουμε $M+1$ στοιχεία από το S, όπου $M = \max\{|S_1|, |S_2|, \ldots, |S_k|\}$. Για να μην ανήκουν σε διαφορετικό υποσύνολο, θα ανήκουν στο ίδιο. Έστω λοιπόν ότι όλα ανήκουν στο S_j. Τότε

$$M + 1 \leq |S_j|,$$

άτοπο.

iii) Αρκεί να επιλέξουμε $n - |S_j| + 1$ στοιχεία από το S. Για να μην υπάρχουν στοιχεία από το υποσύνολο S_j, όλα τα στοιχεία θα ανήκουν στο σύνολο $S \setminus S_j$, οπότε

$$n - |S_j| + 1 \leq |S \setminus S_j|$$

$$n - |S_j| + 1 \leq |S| - |S_j|$$

$$n - |S_j| + 1 \leq n - |S_j|,$$

άτοπο.

iv) Αρκεί να επιλέξουμε $n - m + 1$ στοιχεία από το S, όπου $m = \min\{|S_1|, |S_2|, \ldots, |S_k|\}$. Για να μην υπάρχουν στοιχεία από κάθε υποσύνολο, αρκεί να μην υπάρχουν στοιχεία από κάποιο συγκεκριμένο υποσύνολο. Έστω λοιπόν ότι δεν υπάρχουν στοιχεία από το S_j. Τότε όλα τα στοιχεία θα ανήκουν στο σύνολο $S \setminus S_j$, οπότε

$$n - m + 1 \leq |S \setminus S_j|$$

$$n - m + 1 \leq |S| - |S_j|$$

$$n - m + 1 \leq n - |S_j|$$
$$|S_j| + 1 \leq m,$$

άτοπο.

ν) Αν $r > M$, όπου $M = \max\{|S_1|, |S_2|, \ldots, |S_k|\}$, τότε δεν υπάρχει τέτοια επιλογή.

Έστω $r \leq M$. Έστω $L = \bigcup S_i$ η ένωση των υποσυνόλων των S_i με $|S_i| < r$ και t ο αριθμός των υποσυνόλων S_i με τουλάχιστον r στοιχεία. Αρκεί να επιλέξουμε $|L| + t(r-1) + 1$ στοιχεία. (Γιατί;). □

Παράδειγμα 2.3.17. *Μια κληρωτίδα περιέχει 5 κόκκινα, 8 μπλε, 10 λευκά, 12 πράσινα και 7 κίτρινα σφαιρίδια. Να βρεθεί ο ελάχιστος αριθμός σφαιριδίων που πρέπει να κληρωθεί ώστε να εξασφαλίσουμε ότι θα υπάρχουν*

i) τουλάχιστον 2 σφαιρίδια του ίδιου χρώματος,

ii) τουλάχιστον 2 σφαιρίδια διαφορετικού χρώματος,

iii) τουλάχιστον 1 σφαιρίδιο από κάθε χρώμα,

iv) τουλάχιστον 4 σφαιρίδια του ίδιου χρώματος,

v) τουλάχιστον 6 σφαιρίδια του ίδιου χρώματος.

Λύση. Το σύνολο S είναι το σύνολο από σφαιρίδια, ενώ η διαμέριση του συνόλου γίνεται ως προς το χρώμα κάθε σφαιρίδιου, και υπάρχουν 5 σύνολα.

i) Αρκει να κληρωθούν $5 + 1 = 6$ σφαιρίδια.

ii) Αρκεί να κληρωθούν $12 + 1 = 13$ σφαιρίδια.

iii) Αρκεί να κληρωθούν $12 + 10 + 8 + 7 + 1 = 38$ σφαιρίδια.

iv) Αρκεί να κληρωθούν $3 + 3 + 3 + 3 + 3 + 1 = 16$ σφαιρίδια.

v) Αρκεί να κληρωθούν $5 + 5 + 5 + 5 + 5 + 1 = 26$ σφαιρίδια. □

2.3.1 Ασκήσεις προς επίλυση

1) Να δειχθεί ότι αν υπάρχουν n φωλιές για $kn+1$ περιστέρια, τότε τουλάχιστον μια φωλιά θα έχει τουλάχιστον $k+1$ περιστέρια.

2) (i) Έστω $f : A \to B$ με $|A| = mn$ και $|B| = m$, όπου $m, n \in \mathbb{N}^*$. Να δειχθεί ότι υπάρχει στοιχείο του B το οποίο είναι εικόνα τουλάχιστον n στοιχείων του A.

   (ii) Έστω $f : A \to B$ με $|A| = n$ και $|B| = m$, όπου $0 < m < n$. Να δειχθεί ότι υπάρχει στοιχείο του B το οποίο είναι εικόνα τουλάχιστον $\lceil \frac{n}{m} \rceil$ στοιχείων του A.

3) Πόσα άτομα χρειαζόμαστε για να είμαστε σίγουροι ότι τουλάχιστον 2 άτομα θα έχουν τουλάχιστον την ίδια μέρα γενέθλια; Το ίδιο πρόβλημα για 3 άτομα. Το ίδιο πρόβλημα για q άτομα.

4) Αν η Ελλάδα έχει πληθυσμό 11 εκατομυρίων, να δειχθεί ότι υπάρχει κάποια μέρα του χρόνου στην οποία έχουν γενέθλια τουλάχιστον 50 κάτοικοι της Ελλάδας και επιπλέον όλοι έχουν τα ίδια αρχικά γράμματα (ονόματος και επωνύμου).

5) Σε κάποιο Τμήμα Πληροφορικής υπάρχουν συνολικά 1000 φοιτητές. Σε κάθε εξάμηνο καθένας από αυτούς επιλέγει 8 μαθήματα από μια λίστα με 64 διαφορετικά μαθήματα. Ένας φοιτητής του μαθήματος των Μαθηματικών των Υπολογιστών όταν έμαθε ότι η μεγαλύτερη τάξη χωράει 124 φοιτητές κατάλαβε ότι υπάρχει πρόβλημα. Ποιό είναι το πρόβλημα;

6) Σε ένα τουρνουά συμμετέχουν n ομάδες. Κάθε ομάδα παίζει το πολύ μια φορά με κάθε άλλη ομάδα. Να αποδειχθεί ότι στο τέλος υπάρχουν τουλάχιστον 2 ομάδες που έχουν παίξει τον ίδιο αριθμό παιχνιδιών στο τουρνουά.

7) i) Να δειχθεί ότι κάθε ακολουθία από 10 διαφορετικούς φυσικούς αριθμούς έχει μια αύξουσα υπακολουθία μήκους 4, ή μια φθίνουσα υπακολουθία μήκους 4.

   ii) Κατασκευάστε μια ακολουθία από 9 διαφορετικούς φυσικούς αριθμούς που δεν έχει αύξουσα ή φθίνουσα υπακολουθία μήκους 4.

8) i) Να δειχθεί ότι μεταξύ 6 ατόμων υπάρχουν τουλάχιστον 3 άτομα που είτε γνωρίζονται ανά δύο μεταξύ τους είτε δεν γνωρίζονται καθόλου μεταξύ τους.

   ii) Να δοθεί ένα παράδειγμα με 5 άτομα μεταξύ των οποίων δεν υπάρχουν 3 άτομα τα οποία είτε γνωρίζονται ανά δύο μεταξύ τους είτε δεν γνωρίζονται καθόλου μεταξύ τους.

   iii) Να δειχθεί ότι μεταξύ 9 ατόμων υπάρχουν 3 που γνωρίζονται μεταξύ τους ή/και 4 που δεν γνωρίζονται μεταξύ τους.

9) Ένα συρτάρι περιέχει 6 ζευγάρια μαύρες κάλτσες, 5 ζευγάρια καφέ κάλτσες, 5 ζευγάρια άσπρες κάλτσες και 4 ζευγάρια πράσινες κάλτσες. Πόσες κάλτσες πρέπει να βγάλουμε από το συρτάρι (χωρίς να βλέπουμε) έτσι ώστε να έχουμε σίγουρα

   (i) 2 κάλτσες με το ίδιο χρώμα;

   (ii) 2 κάλτσες με διαφορετικό χρώμα;

   (iii) 3 κάλτσες με το ίδιο χρώμα;

   (iv) 3 κάλτσες με διαφορετικό χρώμα;

   (v) ένα ζευγάρι πράσινες κάλτσες;

   (vi) ένα ζευγάρι κάλτσες από κάθε χρώμα;

(vii) μια κάλτσα από κάθε χρώμα;

10) Μια κληρωτίδα περιέχει 4 κόκκινα, 7 μπλε, 12 λευκά, 11 πράσινα και 8 κίτρινα σφαιρίδια. Να βρεθεί ο ελάχιστος αριθμός σφαιριδίων που πρέπει να κληρωθεί ώστε να εξασφαλίσουμε ότι θα υπάρχουν

i) τουλάχιστον 2 σφαιρίδια του ίδιου χρώματος,

ii) τουλάχιστον 2 σφαιρίδια διαφορετικού χρώματος,

iii) τουλάχιστον 1 σφαιρίδιο από κάθε χρώμα,

iv) τουλάχιστον 4 σφαιρίδια του ίδιου χρώματος,

v) τουλάχιστον 6 σφαιρίδια του ίδιου χρώματος.

vi) τουλάχιστον 3 σφαιρίδια χρώματος μπλε.

Έστω x_1, x_2, x_3, x_4, x_5, x_6 οι αντίστοιχες απαντήσεις σε κάθε μια από τις παραπάνω ερωτήσεις. Να δειχθεί γιατί με $x_1 - 1$, $x_2 - 1$, $x_3 - 1$, $x_4 - 1$, $x_5 - 1$, $x_6 - 1$ σφαιρίδια δεν μπορούμε να εξασφαλίσουμε την απαίτηση κάθε ερώτησης αντίστοιχα.

11) Πόσοι αριθμοί πρέπει να επιλεγούν από το σύνολο $[10, 99] = \{10, 11, \ldots, 98, 99\}$ έτσι ώστε

(i) τουλάχιστον ένα πολλαπλάσιο του 3 να περιλαμβάνεται στην επιλογή;

(ii) τουλάχιστον δύο αριθμοί με το ίδιο πρώτο ψηφίο να περιλαμβάνονται στην επιλογή;

(iii) τουλάχιστον δύο αριθμοί χωρίς κοινό ψηφίο να περιλαμβάνονται στην επιλογή;

(iv) τουλάχιστον δύο αριθμοί με τουλάχιστον ένα κοινό ψηφίο να περιλαμβάνονται στην επιλογή;

12) Να δειχθεί ότι σε κάθε σύνολο n φυσικών αριθμών υπάρχουν k φυσικοί αριθμοί, όπου $1 \leq k \leq n$, των οποίων το άθροισμα είναι πολλαπλάσιο του n.

13) Από το σύνολο των αριθμών $\{1, 4, 7, 10, 13, \ldots, 100\}$ επιλέγονται 19 αριθμοί. Να δειχθεί ότι ανάμεσα στους 19 αριθμούς που επιλέχθηκαν υπάρχουν τουλάχιστον δύο με άθροισμα 104.

14) Από το σύνολο των αριθμών $\{1, 2, 3, \ldots, 126\}$ επιλέγονται 7 αριθμοί. Να δειχθεί ότι ανάμεσα στους 7 αριθμούς που επιλέχθηκαν υπάρχουν αριθμοί a, b με $b < a \leq 2b$.

15) Σε μια 10×10 σκακιέρα τοποθετούνται 41 πύργοι. Να δειχθεί ότι πάντα μπορούμε να επιλέξουμε 5 από αυτούς οι οποίοι δεν απειλούνται μεταξύ τους. (Δύο πύργοι απειλούνται αν και μόνο αν βρίσκονται στην ίδια γραμμή ή στην ίδια στήλη της σκακιέρας).

16) Να δειχθεί ότι μεταξύ 9 (διαφορετικών) πραγματικών αριθμών υπάρχουν δύο αριθμοί x, y ώστε $0 < (a - b)/(1 + ab) < \sqrt{2} - 1$.

17) i) Να δειχθεί ότι αν επιλέξουμε $n+2$ αριθμούς από το σύνολο $\{1, 2, 3, \ldots, 2n+1\}$ τότε μεταξύ αυτών υπάρχουν δύο αριθμοί των οποίων το άθροισμα ισούται με έναν άλλο από τους επιλεγμενους αριθμούς.

ii) Να βρεθεί ένα υποσύνολο του $[2n + 1]$ με $n + 1$ στοιχεία στο οποίο δεν υπάρχουν δύο αριθμοί των οποίων το άθροισμα να ισούται με έναν άλλο αριθμό του υποσυνόλου.

18) Κάποια επιτροπή συνεδρίασε 40 φορές. Σε κάθε συνεδρίαση παρευρίσκονταν ακριβώς 10 μέλη της. Έστω ότι κάθε ζεύγος μελών της επιτροπής δεν συνεδρίασε μαζί περισσότερο από μια φορά.

   i) Αν ο αριθμός των μελών της επιτροπής είναι μικρότερος ή ίσος από 60, να δειχθεί ότι υπάρχει άτομο που συμμετείχε σε τουλάχιστον 7 συνεδριάσεις.

   ii) Να δειχθεί ότι τα μέλη της επιτροπής είναι περισσότερα από 60.

19) Να δειχθεί ότι 25 άτομα δεν είναι δυνατόν να συστήσουν περισσότερες από 30 επιτροπές των 5 ατόμων η καθεμία, τέτοιες ώστε οποιεσδήποτε δύο επιτροπές να μην έχουν περισσότερα από ένα κοινά μέλη.

20) Έστω ότι ένα περιδέραιο αποτελείται από 48 κομμάτια, 34 λευκά και 14 χρωματιστά. Να δειχθεί ότι υπάρχει ένα τμήμα του περιδέραιου από 7 διαδοχικά κομμάτια στο οποίο τουλάχιστον 3 είναι χρωματιστά.

21) Το παίχνιδι "Ναυμαχία" διεξάγεται σε ένα μια σκακιέρα 7×7.

   i) Να δειχθεί ότι 11 βολές δεν αρκούν προκειμένου να πληγεί σε τουλάχιστον ένα τετράγωνο, ένα συγκεκριμένο πολεμικό πλοίο το οποίο έχει τη μορφή $\square\square\square\square$.

   (Υπόδειξη: Να δειχθεί ότι στην 7×7 σκακιέρα μπορούν να τοποθετηθούν 12 μη επικαλυπτόμενα πλοία της παραπάνω μορφής.)

   ii) Να δειχθεί ότι 12 βολές αρκούν προκειμένου να πληγεί, σε τουλάχιστον ένα τετράγωνο, ένα συγκεκριμένο πολεμικό πλοίο το οποίο έχει τη μορφή $\square\square\square\square$.

   (Υπόδειξη: Να βρεθούν 12 τετράγωνα στην 7×7 σκακιέρα τα οποία έχουν μη κενή επικάλυψη με κάθε τετράδα τετραγώνων όμοια με τη μορφή του πλοίου.)

22) Να δειχθεί ότι για κάθε $a, b, c \in \mathbb{N}$, ο αριθμός $(a-b)(b-c)(a-c)$ είναι άρτιος.

23) Έστω $a_1, a_2, \ldots, a_n$ μια μετάθεση των αριθμών $1, 2, \ldots, n$. Να δειχθεί ότι αν ο n είναι περιττός, τότε το γινόμενο

$$(a_1 - 1)(a_2 - 2) \cdots (a_n - n)$$

είναι άρτιος.

24) Στο παιχνίδι "Λόττο", επιλέγονται 6 από τους αριθμούς $1, 2, \ldots, 49$. Υποθέστε ότι ένα βραβείο παρηγοριάς δίδεται επίσης στα δελτία που δεν περιέχουν κανέναν από τους 6 αριθμούς που κερδίζουν. Ποιός είναι ο ελάχιστος αριθμός δελτίων με 6 αριθμούς που πρέπει να συμπληρωθούν ώστε να εξασφαλίσουμε το βραβείο παρηγοριάς; Πώς θα συμπληρωθούν όλα αυτά τα δελτία;

25) Σε καθέναν από τους πλανήτες κάποιου συστήματος βρίσκεται ένας αστρονόμος ο οποίος παρατηρεί μόνο τον πλησιέστερο πλανήτη. Οι αποστάσεις μεταξύ των πλανητών είναι ανά δύο διαφορετικές. Να δειχθεί ότι, αν το πλήθος των πλανητών είναι περιττός αριθμός, τότε κάποιον πλανήτη δεν τον παρατηρεί κανένας.

26) i) Να δειχθεί ότι δεν είναι δυνατόν να τοποθετηθούν τα ψηφία 0, 1, ..., 9 στις κορυφές ενός 45-γωνου, έτσι ώστε για κάθε ζεύγος (διαφορετικών) ψηφίων να υπάρχει πλευρά του 45-γωνου με άκρα αυτά τα ψηφία.

   (Υπόδειξη: Να δειχθεί ότι κάθε ψηφίο πρέπει να εμφανίζεται σε 5 τουλάχιστον κορυφές.)

ii) Να βρεθεί ένας τρόπος τοποθέτησης των ψηφίων 0, 1, . . ., 8 στις κορυφές ενός 45-γωνου, έτσι ώστε για κάθε ζεύγος (διαφορετικών) ψηφίων να υπάρχει πλευρά του 45-γωνου με άκρα αυτά τα ψηφία.

27) Ένας σκακιστής θέλει να προετοιμασθεί για ένα αγώνα πρωταθλήματος παίζοντας μερικά παιχνίδια εξάσκησης σε 30 ημέρες. Θέλει να παίξει τουλάχιστον ένα παιχνίδι την ημέρα, αλλά όχι περισσότερα από 45 παιχνίδια συνολικά. Να δειχθεί ότι όπως και να προγραμματίσει τα παιχνίδια, υπάρχει μια περίοδος από συνεχόμενες ημέρες κατά την οποία παίζει *ακριβώς* 14 παιχνίδια.

28) Ένας άνδρας περπάτησε για 10 ώρες και κάλυψε μια συνολική απόσταση 45 χιλιομέτρων. Είναι γνωστό ότι περπάτησε 6 χιλιόμετρα την πρώτη ώρα και μόνο 3 χιλιόμετρα την τελευταία ώρα. Να αποδειχθεί ότι πρέπει να περπάτησε τουλάχιστον 9 χιλιόμετρα σε μια συγκεκριμένη περίοδο δύο συνεχόμενων ωρών.

29) Η περιφέρεια ενός τροχού ρουλέτας διαιρείται σε 36 τομείς στους οποίους εμφανίζονται οι αριθμοί $1, 2, \ldots, 36$ με κάποιον αυθαίρετο τρόπο. Δείξτε ότι υπάρχουν 3 συνεχόμενοι τομείς τέτοιοι, ώστε το άθροισμα των αριθμών που εμφανίζονται σ' αυτούς να είναι τουλάχιστον 56.

30) Δείξτε ότι για ένα αυθαίρετο ακέραιο n, υπάρχει ένα πολλαπλάσιο του το οποίο περιέχει μόνο τα ψηφία 0 και 7 ή μόνο το ψηφίο 7. (Για παράδειγμα για $n = 3$, έχουμε $3 \cdot 259 = 777$, για $n = 4$, έχουμε $4 \cdot 1295 = 7700$, για $n = 5$, έχουμε $5 \cdot 14 = 70$, για $n = 6$, έχουμε $6 \cdot 1295 = 7770$).

(Υπόδειξη: Θεωρείστε τα υπόλοιπα των διαιρέσεων με το n των παρακάτω φυσικών αριθμών: $7, 77, 777, 7777, \ldots, \underbrace{777\cdots77}_{n}$.)

31) Έστω 5 σημεία τα οποία βρίσκονται στην επιφάνεια μιας σφαίρας. Να δειχθεί ότι υπάρχει ημισφαίριο της σφαίρας το οποίο περιέχει τουλάχιστον τα 4 από τα 5 σημεία.

32) Να δειχθεί ότι για κάθε πραγματικό αριθμό x ένας τουλάχιστον από τους αριθμούς

$$x, 2x, 3x, \ldots, (n-1)x$$

απέχει το πολύ κατά $1/n$ από κάποιον ακέραιο.

Παράρτημα: Η αρχή του περιστερεώνα σε άπειρα σύνολα

Πρόταση 2.15. *Αν $f : A \to B$ όπου A είναι άπειρο σύνολο και B είναι πεπερασμένο σύνολο, τότε υπάρχει $b \in B$ ώστε $f^{-1}(b)$ είναι άπειρο σύνολο*

Παράδειγμα 2.3.18. *Σε κάθε άπειρη ακολουθία ακεραίων υπάρχουν άπειροι αριθμοί που αφήνουν το ίδιο υπόλοιπο με το 11.*

Λύση. Διαμερίζουμε τους αριθμούς της ακολουθίας με βάση τα υπόλοιπα με το 11. Σύμφωνα με την αρχή του περιστερεώνα τουλάχιστον ένα από τα παραπάνω σύνολα θα έχει άπειρο πληθάριθμο. □

2.4 Αρχή της διαγωνιοποίησης

Η **αρχή της διαγωνιοποίησης** εισήχθηκε από τον George Cantor (1845–1918) στην προσπάθειά του να ταξινομήσει τους πληθάριθμους των άπειρων συνόλων.

Η πρώτη εφαρμογή της αρχής έγινε για την απόδειξη της πρότασης (*i*) της παραγράφου 1.4.3, από όπου και πήρε το όνομά της.

Η αρχή της διαγωνιοποίησης δίδεται στην επόμενη πρόταση.

Πρόταση 2.16 (Αρχή της διαγωνιοποίησης). *Έστω R μια δυαδική σχέση σε ένα σύνολο $\mathcal{E}$ και $\Gamma(x) = \{y \in \mathcal{E} : xRy\}$. Για το σύνολο*

$$\Delta = \{x \in \mathcal{E} : x \not R x\}$$

ισχύει ότι

$$\Delta \neq \Gamma(x), \text{ για κάθε } x \in \mathcal{E}.$$

Απόδειξη. Έστω $x \in \mathcal{E}$.

Αν $x \in \Delta$ τότε $x \not R x$, άρα $x \notin \Gamma(x)$.

Αν $x \notin \Delta$ τότε xRx, άρα $x \in \Gamma(x)$.

Δηλαδή, το $\Delta \neq \Gamma(x)$ για κάθε $x \in \mathcal{E}$. □

Το σύνολο Δ ονομάζεται **διαγώνιο σύνολο** του $\mathcal{E}$.

Παραδείγματα

1. Αν $\mathcal{E} = \{0, 1, 2, 3, 4, 5\}$ και

$$xRy \Leftrightarrow x = y^2$$

τότε το διαγώνιο σύνολο του $\mathcal{E}$ είναι ίσο με

$$\Delta = \{2, 3, 4, 5\}.$$

2. Για την σχέση R που ορίζεται στον επόμενο πίνακα για το σύνολο $\mathcal{E} = \{x_1, x_2, x_3, x_4\}$,

R	x_1	x_2	x_3	x_4
x_1			★	
x_2		★		★
x_3			★	
x_4	★	★	★	

έχουμε $\Delta = \{x_1, x_4\}$, οπότε
$\Gamma(x_1) = \{x_3\} \neq \Delta$,
$\Gamma(x_2) = \{x_2, x_4\} \neq \Delta$,
$\Gamma(x_3) = \{x_3\} \neq \Delta$,
$\Gamma(x_4) = \{x_1, x_2, x_3\} \neq \Delta$,

επαληθεύοντας τη πρόταση.

3. Για κάθε πεπερασμένο σύνολο X ισχύει ότι

$$|X| < |\mathcal{P}(X)|,$$

και επιπλέον αν το σύνολο X είναι αριθμήσιμο, τότε το $\mathcal{P}(X)$ είναι υπεραριθμήσιμο.

Απόδειξη. Αρκεί να δειχθεί ότι κάθε $1-1$ απεικόνιση $f : X \to \mathcal{P}(X)$ δεν είναι επί, δηλαδή ότι υπάρχει στοιχείο Δ του $\mathcal{P}(X)$ το οποίο δεν είναι εικόνα κανενός στοιχείου του X.

Θα εφαρμόσουμε την αρχή της διαγωνιοποίησης για $\mathcal{E} = \mathcal{X}$ και R τη δυαδική σχέση στο $\mathcal{X}$ που ορίζεται ως εξής:

$$xRy \Leftrightarrow y \in f(x).$$

Τότε,

$$\Delta = \{x \in \mathcal{X} : x \not R x\} = \{x \in \mathcal{X} : x \notin f(x)\},$$

και

$$\Gamma(x) = \{y \in \mathcal{X} : xRy\} = \{y \in \mathcal{X} : y \in f(x)\} = f(x).$$

Αλλά, από την αρχή της διαγωνιοποίησης $\Delta \neq \Gamma(x)$. Άρα, το Δ διαφέρει από κάθε σύνολο $f(x)$, για κάθε $x \in \mathcal{X}$. Δηλαδή το Δ δεν είναι εικόνα κανενός στοιχείου του $\mathcal{X}$ μέσω της f, οπότε η f δεν είναι επί. □

Παρατήρηση. Άμεση συνέπεια του Παραδείγματος 3 είναι ότι το σύνολο $\mathcal{P}(\mathbb{N})$ είναι υπεραριθμήσιμο.

2.4.1 Ασκήσεις προς επίλυση

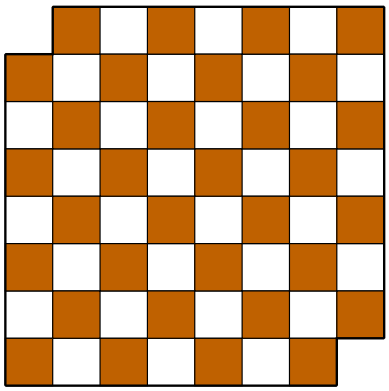
1) Αν R είναι η δυαδική σχέση στο $\mathbb{N}^2$ με $(x, y)R(x', y') \Leftrightarrow x = y' - 1$, να βρεθεί το διαγώνιο σύνολο Δ του συνόλου $\mathcal{E} = \{(1, 2),(1, 3),(2, 1),(0, 0),(5, 4),(6, 2),(6, 5),(9, 10),(11, 10)\}$.

∗2) Να δειχθεί ότι σύνολο $\mathbb{N}^{\mathbb{N}}$ είναι υπέραριθμήσιμο.

2.5 Παράρτημα: Αρχή της αρτιότητας

Τα επόμενα προβλήματα αντιμετωπίζονται με τη λεγόμενη **αρχή της αρτιότητας**.

Παράδειγμα 2.5.1. *Να δειχθεί ότι δεν μπορούμε να καλύψουμε με (μη επικαλυπτόμενα) ντόμινο μια σκακιέρα 8×8 από την οποία έχουμε αφαιρέσει το πάνω αριστερό και το κάτω δεξιό τετράγωνο.*



Λύση. Στη σκακιέρα έχουν απομείνει 30 λευκά και 32 σκούρα τετράγωνα. Παρατηρούμε ότι κάθε ντόμινο πρέπει να καλύπτει ένα λευκό και ένα σκούρο τετράγωνο. Άρα, η κάλυψη είναι αδύνατη. □

Παράδειγμα 2.5.2. *Να δειχθεί ότι δεν υπάρχει διαδρομή του ίππου που επισκέπτεται ακριβώς μια φορά όλα τα τετράγωνα μιας 8×8 σκακιέρας από την οποία έχουμε αφαιρέσει το πάνω αριστερό και το κάτω δεξιό τετράγωνο.*

Λύση. Ο ίππος σε κάθε βήμα αλλάζει χρώμα. Υπάρχουν 30 λευκά και 32 μαύρα τετράγωνα. Άρα, στο τέλος οποιασδήποτε διαδρομής θα υπάρχουν δύο μαύρα τετράγωνα τα οποία δεν θα έχει επισκεφθεί. □

Παράδειγμα 2.5.3. *Έστω ένα πολυώνυμο με ακέραιους συντελεστές τέτοιο ώστε $f(1) = 3$. Να δειχθεί ότι $f(3) \neq 0$.*

Λύση. Αφού $f(1) = 3$ έπεται ότι το άθροισμα όλων των συντελεστών του πολυωνύμου είναι περιττός. Παρατηρούμε ότι για κάθε όρο $a_i x^i$ του πολυωνύμου αν $x = 3$ ο όρος έχει την ίδια αρτιότητα με το a_i (δηλαδή, αν a_i είναι άρτιος, τότε $a_i 3^i$ πάλι είναι άρτιος, αν a_i είναι περιττός, τότε $a_i 3^i$ πάλι είναι περιττός) άρα το άθροισμα των όρων για $x = 3$ έχει την ίδια αρτιότητα με το $f(1)$ δηλαδή είναι περιττό. Άρα $f(3) \neq 0$. □

Παράδειγμα 2.5.4. *Να δειχθεί ότι για κάθε Πυθαγόρεια τριάδα (a, b, c) δηλαδή φυσικούς αριθμούς a, b, c ώστε $a^2 + b^2 = c^2$, ισχύει ότι abc είναι άρτιος.*

Λύση. Αν ο abc είναι περιττός, τότε οι a, b, c πρέπει να είναι και οι τρεις περιττοί. Τότε όμως καταλήγουμε σε άτοπο, αφού το $a^2 + b^2$ θα είναι άρτιος, ως άθροισμα δύο περιττών αριθμών, ενώ το c^2 θα είναι περιττός. □

Παράδειγμα 2.5.5. *Από ένα βιβλίο μαθηματικών έχουν σκιστεί* 49 *φύλλα (όχι απαραίτητα διαδοχικά). Να δειχθεί ότι το άθροισμα των αριθμών των σελίδων αυτών των φύλλων δεν ισούται με* 2016*.*

Λύση. Το άθροισμα των αριθμών σελίδων σε ένα φύλλο είναι άρτιος + περιττός = περιττός. Τα 49 φύλλα θα έχουν συνολικό άθροισμα σελίδων το άθροισμα 49 περιττών, το οποίο είναι περιττός. □

Παράδειγμα 2.5.6. *Να δειχθεί ότι το σύνολο* $\{1, 2, 3, \ldots, 2n + 1\}$*,* $n \in \mathbb{N}$ *δεν διαμερίζεται σε δύο σύνολα με τον ίδιο πληθάριθμο.*

Λύση. Το σύνολο $[2n + 1]$ έχει περιττό πλήθος στοιχείων. □

Παράδειγμα 2.5.7.

i) Να δειχθεί ότι το σύνολο [10] *δεν διαμερίζεται σε δύο υποσύνολα με το ίδιο άθροισμα στοιχείων.*

ii) Να δειχθεί ότι το σύνολο [13] *δεν διαμερίζεται σε δύο υποσύνολα με το ίδιο άθροισμα στοιχείων.*

Λύση.

i) Το άθροισμα των στοιχείων του [10] είναι ίσο με $(10 * 11)/2 = 55$ (περιττός).

ii) Το άθροισμα των στοιχείων του [13] είναι ίσο με $(13 * 14)/2 = 91$ (περιττός). □

Παράδειγμα 2.5.8. *Έστω A το σύνολο των δυαδικών λέξεων με άρτιο αριθμό άσσων. Να δειχθεί ότι αν σε κάποια λέξη w του A αλλάξει οποιοδήποτε γράμμα της τότε η λέξη w′ που θα προκύψει δεν θα ανήκει στο A.*

Απόδειξη. Αν αλλάξει οποιοδήποτε γράμμα της λέξης ο αριθμός των άσσων της θα πάψει να είναι άρτιος. □

Παράδειγμα 2.5.9. *Μια κάλπη περιέχει 21 λευκές και 22 μαύρες σφαίρες. Επιλέγουμε τυχαία 2 σφαίρες.*

Αν και οι δύο είναι μαύρες, τότε ξαναρίχνουμε την μία στην κάλπη και απορρίπτουμε την άλλη.

Αν και οι δύο είναι λευκές, τότε απορρίπτουμε και τις δύο σφαίρες και εισάγουμε μια μαύρη σφαίρα στην κάλπη.

Αν η μία είναι λευκή και η άλλη είναι μαύρη, τότε ξαναρίχνουμε τη λευκή στην κάλπη και απορρίπτουμε την μαύρη.

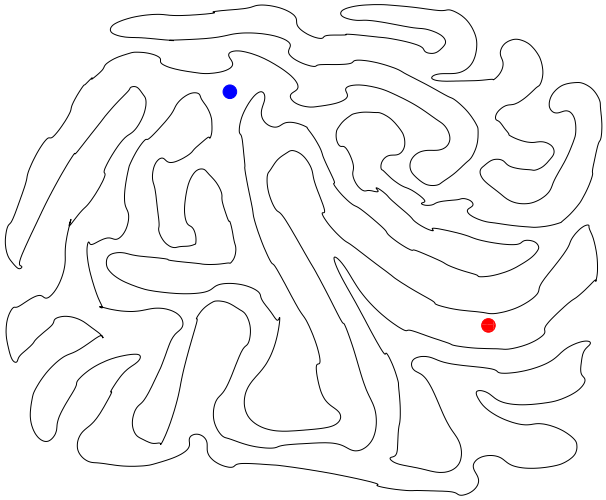
Τι χρώμα είναι τελευταία σφαίρα;

Λύση. Κάθε φορά ο αριθμός των σφαιρών στην κάλπη μειώνεται ακριβώς κατά 1. Ο αριθμός των λευκών σφαιρών μειώνεται μόνο κατά άρτιο αριθμό, άρα διατηρεί την αρτιότητά του. Επομένως, η τελευταία σφαίρα θα είναι σίγουρα λευκή. □

Παράδειγμα 2.5.10. *Να δειχθεί ότι η εξίσωση* $3x(x+1) = 5(2y+1)^3$ *δεν έχει θετικές ακέραιες λύσεις.*

Λύση. Ο αριθμός $3x(x+1)$ είναι άρτιος, ενώ το αριθμός $5(2y+1)^3$ είναι περιττός. □

Παράδειγμα 2.5.11. *Έστω μια απλή κλειστή καμπύλη στο επίπεδο, (η οποία χωρίζει το επίπεδο σε δύο περιοχές). Δίδονται δύο σημεία Α, Β τα οποία δεν ανήκουν στην καμπύλη. Να βρεθεί μια μέθοδος για να ελέγξουμε αν τα σημεία βρίσκονται στην ίδια περιοχή.*



Λύση. Κάθε απλή γραμμή που τέμνει την κλειστή καμπύλη αλλάζει περιοχή. Αν ενώσουμε με μια οποιαδήποτε (απλή) γραμμή τα δύο σημεία και μετρήσουμε τον αριθμό των τομών της γραμμής με την κλειστή καμπύλη τότε αν ο αριθμός αυτός είναι άρτιος τα σημεία βρίσκονται στο ίδια περιοχή, ενώ αν είναι περιττός τα σημεία βρίσκονται σε διαφορετικές περιοχές. □

2.5.1 Ασκήσεις προς επίλυση

1) Να δειχθεί ότι δεν μπορούμε να καλύψουμε με (μη επικαλυπτόμενα) 2×2 ντόμινο μια 8×8 από την οποία έχουμε αφαιρέσει το πάνω αριστερό και το κάτω δεξιό τετράγωνο.

2) Έστω ένα πολυώνυμο με ακέραιους συντελεστές τέτοιο ώστε $f(2) = 3$. Να δειχθεί ότι $f(4) \neq 0$.

3) i) Έστω $n \in \mathbb{N}^*$. Να δειχθεί ότι για κάθε τριάδα φυσικών αριθμών a, b, c ώστε $a^2+b^2 = c^2+2n$, ισχύει ότι abc είναι άρτιος.

   ii) Έστω $n \in \mathbb{N}^*$. Να δειχθεί ότι για κάθε τετράδα φυσικών αριθμών a, b, c, d ώστε $a^2+b^2+c^2 = d^2 + 2n + 1$, ισχύει ότι $abcd$ είναι άρτιος.

4) i) Να δειχθεί ότι το σύνολο [10] δεν διαμερίζεται σε τρία υποσύνολα με το ίδιο άθροισμα στοιχείων.

   ii) Να δειχθεί ότι το σύνολο [13] δεν διαμερίζεται σε τρία υποσύνολα με το ίδιο άθροισμα στοιχείων.

5) Να δειχθεί ότι η εξίσωση $5x(x+3)-3(y+5)(y-6) = 7(xy+2)$ δεν έχει θετικές ακέραιες περιττές λύσεις.

6) Έστω μια απλή κλειστή καμπύλη στο επίπεδο (η οποία χωρίζει το επίπεδο σε δύο περιοχές). Δίδεται ένα σημείο A το οποίο δεν ανήκει στην καμπύλη. Να βρεθεί μια μέθοδος για να ελέγξουμε αν το A είναι στο εσωτερικό της καμπύλης ή όχι.

7) Να δειχθεί ότι σε κάθε γράφημα δεσμών ο αριθμός των κορυφών με περιττό βαθμό είναι άρτιος.

∗8) Να δειχθεί ότι το 8-puzzle δεν έχει πάντα λύση.

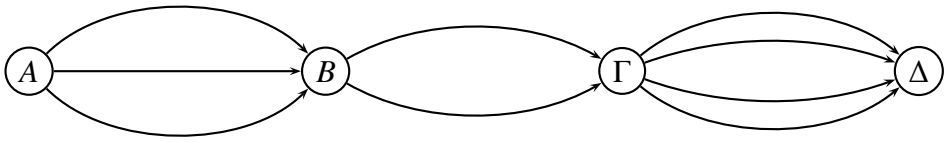
Κεφάλαιο 3

Διατάξεις, Συνδυασμοί

3.1 Πολλαπλασιαστική αρχή ή κανόνας γινομένου

Πρόταση 3.1 (Πολλαπλασιαστική αρχή). *Αν ένα αντικείμενο A μπορεί να επιλεγεί κατά m τρόπους και ένα αντικείμενο B κατά n τρόπους, τότε και τα δύο μαζί μπορούν να επιλεγούν κατά $m \cdot n$ τρόπους.*

Παράδειγμα. Αν από την πόλη A στην πόλη B υπάρχουν 3 διαφορετικοί δρόμοι, από την B στη Γ 2 δρόμοι και από τη Γ στη Δ 4 δρόμοι, πόσες διαδρομές υπάρχουν από την πόλη A στη Δ μέσω των πόλεων B και Γ;



Απάντηση. Υπάρχουν $3 \cdot 2 \cdot 4 = 24$ διαδρομές. □

3.2 Διατάξεις

Έστω E ένα πεπερασμένο σύνολο με n στοιχεία, δηλαδή $|E| = n$.

Κάθε διατεταγμένη m-άδα $(a_1, a_2, \ldots, a_m)$ με $a_i \in E$ για κάθε $i \in [m] = \{1, 2, \ldots, m\}$ ονομάζεται **διάταξη των n στοιχείων του E ανά m.**

Αν τα στοιχεία μιας διάταξης είναι διαφορετικά (δηλαδή $a_i \neq a_j$ για κάθε $i, j \in [m]$ με $i \neq j$) τότε αυτή ονομάζεται **απλή διάταξη** (ή **διάταξη**), ενώ αν τα στοιχεία της δεν είναι κατ' ανάγκη διαφορετικά τότε αυτή ονομάζεται **επαναληπτική διάταξη** ή **διάταξη με επανάληψη**.

Αν $n = m$, τότε η διάταξη n ανά n ονομάζεται **μετάθεση n στοιχείων**.

Μια επαναληπτική μετάθεση στην οποία εμφανίζονται k διαφορετικά στοιχεία ονομάζεται **μετάθεση k ειδών στοιχείων**.

Παραδείγματα

1. Έστω $E = \{\alpha, \beta, \gamma, \delta\}$.

   Οι (απλές) διατάξεις των 4 στοιχείων του E ανά 2 είναι οι εξής:
   $$(\alpha,\beta),\quad (\alpha,\gamma),\quad (\alpha,\delta),\quad (\beta,\gamma),\quad (\beta,\delta),\quad (\gamma,\delta),$$
   $$(\beta,\alpha),\quad (\gamma,\alpha),\quad (\delta,\alpha),\quad (\gamma,\beta),\quad (\delta,\beta),\quad (\delta,\gamma),$$
   ενώ οι διατάξεις με επανάληψη των 4 στοιχείων του E ανά 2 είναι οι **προηγούμενες** και **επιπλέον** οι ακόλουθες:
   $$(\alpha,\alpha),\quad (\beta,\beta),\quad (\gamma,\gamma),\quad (\delta,\delta).$$

2. Οι μεταθέσεις των 3 στοιχείων α, β, γ είναι οι εξής:
   $$(\alpha,\beta,\gamma),\quad (\alpha,\gamma,\beta),\quad (\beta,\alpha,\gamma),$$
   $$(\beta,\gamma,\alpha),\quad (\gamma,\alpha,\beta),\quad (\gamma,\beta,\alpha).$$

3. Οι μεταθέσεις 3 ειδών στοιχείων α, β, γ όπου το α εμφανίζεται 2 φορές και τα β, γ από μία φορά είναι οι εξής:
   $$(\alpha,\alpha,\beta,\gamma),\quad (\alpha,\alpha,\gamma,\beta),\quad (\alpha,\beta,\alpha,\gamma),\quad (\alpha,\beta,\gamma,\alpha),$$
   $$(\alpha,\gamma,\alpha,\beta),\quad (\alpha,\gamma,\beta,\alpha)\quad (\beta,\alpha,\alpha,\gamma),\quad (\beta,\alpha,\gamma,\alpha)$$
   $$(\beta,\gamma,\alpha,\alpha),\quad (\gamma,\alpha,\alpha,\beta),\quad (\gamma,\alpha,\beta,\alpha),\quad (\gamma,\beta,\alpha,\alpha).$$

Εφαρμογή 3.2.1. *Να δειχθεί ότι το πλήθος των $1-1$ απεικονίσων από το A στο B, όπου $A = \{\alpha,\beta,\gamma,\delta\}$ και $B = \{1,2,3,4,5,6,7\}$ είναι ίσο με το πλήθος των διατάξεων των 7 ανά 4.*

Απόδειξη. Για κάθε $1-1$ απεικόνιση $f : A \to B$ ορίζουμε μια διάταξη των 7 στοιχείων του B ανά 4:

Για παράδειγμα, αν $f(\alpha) = 5$, $f(\beta) = 3$, $f(\gamma) = 1$ και $f(\delta) = 4$, τότε η ζητούμενη διάταξη είναι η $(5, 3, 1, 4)$.

Αντίστροφα, για κάθε διάταξη των 7 στοιχείων του B ανά 4 ορίζουμε μια $1-1$ απεικόνιση $f : A \to B$:

Η διάταξη $(3, 5, 6, 7)$ για παράδειγμα, ορίζει την απεικόνιση $f : A \to B$ με

$$f(\alpha) = 3,\ f(\beta) = 5,\ f(\gamma) = 6,\ f(\delta) = 7.$$ □

Πλήθος διατάξεων

Πρόταση 3.2 (Πλήθος διατάξεων). *Το πλήθος $P(n,m)$ ή A_n^m των διατάξεων n στοιχείων ανά m δίδεται από τον τύπο*
$$P(n,m) = \frac{n!}{(n-m)!}.$$

Απόδειξη. Έστω $|E| = n$. Τα στοιχεία μιας οποιασδήποτε διάταξης $(a_1, a_2, \ldots, a_m)$ επιλέγονται ως εξής:

a_1	επιλέγεται από το	$E_1 = E$
a_2	$\cdots$	$E_2 = E \setminus \{a_1\}$
a_3	$\cdots$	$E_3 = E \setminus \{a_1, a_2\}$
$\vdots$	$\vdots$	$\vdots$
a_m	επιλέγεται από το	$E_m = E \setminus \{a_1, a_2, \ldots, a_{m-1}\}$.

Έτσι η διάταξη $(a_1, a_2, \ldots, a_m)$ επιλέγεται από το σύνολο $E_1 \times E_2 \times \cdots \times E_m$.

Άρα,

$$\begin{aligned} P(n,m) &= |E_1 \times E_2 \times \cdots \times E_m| \\ &= |E_1||E_2| \cdots |E_m| \\ &= n(n-1)\cdots(n-(m-1)) \\ &= n(n-1)\cdots(n-m+1) \\ &= \frac{n(n-1)\cdots(n-m+1)(n-m)(n-m-1)\cdots 2\cdot 1}{(n-m)(n-m-1)\cdots 2\cdot 1} \\ &= \frac{n!}{(n-m)!}. \end{aligned}$$

□

Πλήθος μεταθέσεων

Πρόταση 3.3 (Πλήθος μεταθέσεων). *Το πλήθος P_n των μεταθέσεων n στοιχείων δίδεται από τον τύπο*

$$P_n = n!.$$

Απόδειξη. Ισχύει ότι $P_n = P(n,n) = \frac{n!}{(n-n)!} = n!$ □

Πλήθος επαναληπτικών διατάξεων

Πρόταση 3.4 (Πλήθος επαναληπτικών διατάξεων). *Το πλήθος $U(n,m)$ των επαναληπτικών διατάξεων n στοιχείων ανά m δίδεται από τον τύπο*

$$U(n,m) = n^m.$$

Απόδειξη. Έστω $|E| = n$. Τα στοιχεία μιας οποιασδήποτε επαναληπτικής διάταξης $(a_1, a_2, \ldots, a_m)$ επιλέγονται ως εξής:

$$\begin{array}{lcl} a_1 & \text{επιλέγεται από το} & E_1 = E \\ a_2 & \cdots & E_2 = E \\ a_3 & \cdots & E_3 = E \\ \vdots & \vdots & \vdots \\ a_m & \text{επιλέγεται από το} & E_m = E. \end{array}$$

Έτσι η επαναληπτική διάταξη $(a_1, a_2, \ldots, a_m)$ επιλέγεται από το σύνολο $E_1 \times E_1 \times \cdots \times E_m = E^m$. Άρα,

$$U(n,m) = |E^m| = \underbrace{|E| \cdot |E| \cdots |E|}_{m \text{ φορές}} = |E|^m.$$

□

Αναγωγική εξίσωση διατάξεων

Πρόταση 3.5 (Αναγωγική εξίσωση διατάξεων). *Για κάθε $m, n \in \mathbb{N}$ ισχύει η αναγωγική εξίσωση*

$$P(n,m) = P(n-1,m) + mP(n-1,m-1),$$

όπου $P(n,0) = 1$ για κάθε $n \in \mathbb{N}$.

Απόδειξη. Δίδεται μια απόδειξη της πρότασης η οποία ονομάζεται **συνδυαστική απόδειξη**.

Έστω ένα σύνολο E με $|E| = n$, $n \in \mathbb{N}^*$ και $\Delta_m(E)$ το σύνολο όλων των διατάξεων των n στοιχείων του E ανά m. Ισχύει ότι $|\Delta_m(E)| = P(n, m)$.

Θεωρούμε $\beta \in E$ και ορίζουμε τα εξής υποσύνολα του $\Delta_m(E)$:

$$A = \{(a_1, a_2, \ldots, a_m) \in \Delta_m(E) : a_i \neq \beta \text{ για κάθε } i \in [m]\}$$

(δηλαδή το A περιέχει όλες τις διατάξεις των n στοιχείων του E ανα m που δεν περιέχουν το στοιχείο β), και για κάθε $i \in [m]$ ορίζουμε τα σύνολα

$$B_i = \{(a_1, a_2, \ldots, a_m) \in \Delta_m(E) : a_i = \beta\}$$

(δηλαδή το B_i περιέχει όλες τις διατάξεις των n στοιχείων του E ανά m που περιέχουν το στοιχείο β στη θέση i).

Τα σύνολα $A, B_1, B_2, \ldots, B_m$ αποτελούν μια διαμέριση του $\Delta_m(E)$, αφού σε μια (απλή) διάταξη των n στοιχείων του E ανά m είτε δεν θα εμφανίζεται το στοιχείο β, είτε θα εμφανίζεται στη θέση 1, είτε θα εμφανίζεται στη θέση 2, ..., είτε θα εμφανίζεται στη θέση m. Επομένως, ισχύει ότι

$$|\Delta_m(E)| = |A| + \sum_{i=1}^{m} |B_i|. \tag{3.1}$$

Παρατηρούμε ότι $A = \Delta_m(E \setminus \{\beta\})$, επομένως

$$|A| = |\Delta_m(E \setminus \{\beta\}| = P(n-1, m). \tag{3.2}$$

Επιπλέον, επειδή κάθε στοιχείο του B_i έχει σταθερή την i συντεταγμένη (ίση με β) προκύπτει ότι η απεικόνιση

$$\phi_i : B_i \to \Delta_{m-1}(E \setminus \{\beta\}), \text{ με}$$

$$\phi((a_1, a_2, \ldots, a_{i-1}, \beta, a_{i+1}, \ldots, a_m)) = (a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_m))$$

είναι αμφιμονοσήμαντη. Οπότε

$$B_i \sim \Delta_{m-1}(E \setminus \{\beta\}),$$

και επομένως

$$|B_i| = |\Delta_{m-1}(E \setminus \{\beta\})| = P(n-1, m-1), \text{ για κάθε } i \in [m]. \tag{3.3}$$

Από τις σχέσεις (3.1), (3.2), (3.3) προκύπτει ότι

$$\begin{aligned} P(n, m) &= P(n-1, m) + \sum_{i=1}^{m} P(n-1, m-1) \\ &= P(n-1, m) + mP(n-1, m-1). \end{aligned}$$

□

3.3 Συνδυασμοί

Έστω ένα σύνολο E με $|E| = n$.

Κάθε οικογένεια που αποτελείται από m στοιχεία του E ονομάζεται **συνδυασμός των n στοιχείων του E ανά m.**

Αν τα στοιχεία ενός συνδυασμού είναι διαφορετικά, τότε αυτός ονομάζεται **απλός συνδυασμός** (ή **συνδυασμός**), ενώ αν τα στοιχεία του δεν είναι κατ' ανάγκη διαφορετικά, τότε αυτός ονομάζεται **επαναληπτικός συνδυασμός** ή **συνδυασμός με επανάληψη**.

Παράδειγμα. Εστω $E = \{\alpha, \beta, \gamma, \delta\}$.

Οι συνδυασμοί των 4 στοιχείων του E ανά 2 είναι οι εξής:

$$\{\alpha,\beta\}, \{\alpha,\gamma\}, \{\alpha,\delta\}, \{\beta,\gamma\}, \{\beta,\delta\}, \{\gamma,\delta\},$$

ενώ οι επαναληπτικοί συνδυασμοί των 4 στοιχείων του E ανά 2 είναι οι ακόλουθοι:

$$\alpha\alpha, \beta\beta, \gamma\gamma, \delta\delta, \alpha\beta, \alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta, \gamma\delta.$$

Ουσιαστικά *κάθε απλός συνδυασμός των n στοιχείων του E ανά m είναι ένα υποσύνολο του E με m στοιχεία.*

Η διαφορά συνδυασμών και διατάξεων είναι ότι στους συνδυασμούς δεν παίζει ρόλο η σειρά των στοιχείων.

Πλήθος συνδυασμών

Πρόταση 3.6 (Πλήθος συνδυασμών). *Το πλήθος $\binom{n}{m}$ ή $C(n,m)$ ή C_n^m των συνδυασμών n στοιχείων ανά m δίδεται από τον τύπο*

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}.$$

Απόδειξη. Θα δοθεί μια συνδυαστική απόδειξη της πρότασης.

Έστω ένα σύνολο E με $|E| = n$.

Συμβολίζουμε με $\Delta_m(E)$ και $\Sigma_m(E)$ τα σύνολα των διατάξεων και συνδυασμών αντίστοιχα των n στοιχείων του E ανά m.

Για κάθε συνδυασμό $\sigma = \{a_1, a_2, \ldots, a_m\}$ στο $\Sigma_m(E)$, συμβολίζουμε με A_σ το σύνολο όλων των διατάξεων στο $\Delta_m(E)$ των οποίων τα στοιχεία είναι τα $a_1, a_2, \ldots, a_m$.

Προφανώς, $|A_\sigma| = m!$ (το πλήθος των μεταθέσεων των στοιχείων $a_1, a_2, \ldots, a_m$) και ισχύει ότι η οικογένεια $\{A_\sigma\}$ όπου $\sigma \in \Sigma_m(E)$ είναι μια διαμέριση του $\Delta_m(E)$.

Άρα, είναι

$$\begin{aligned} |\Delta_m(E)| &= |\bigcup \{A_\sigma : \sigma \in \Sigma_m(E)\}| \\ &= \sum_{\sigma \in \Sigma_m(E)} |A_\sigma| \\ &= m!|\Sigma_m(E)|. \end{aligned}$$

Άρα,

$$|\Sigma_m(E)| = \frac{|\Delta_m(E)|}{m!} \Leftrightarrow \binom{n}{m} = \frac{n!}{m!(n-m)!}.$$

□

Παρατήρηση. Προφανώς, ισχύει ότι

$$\binom{n}{m} = \binom{n}{n-m}.$$

Αναγωγικές εξισώσεις συνδυασμών

Πρόταση 3.7 (Τρίγωνο του Pascal). *Ισχύει ότι*

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1},$$

όπου $m \leq n$ *με* $\binom{n}{0} = 1$ *για κάθε* $n \in \mathbb{N}$, *και* $\binom{n}{m} = 0$ *αν* $m > n$.

Απόδειξη. Δίδεται μια συνδυαστική απόδειξη.

Έστω ένα σύνολο E με $|E| = n$ και $\beta \in E$.

Διαμερίζουμε το σύνολο $\Sigma_m(E)$ των συνδυασμών των n στοιχείων του E ανά m σε δύο σύνολα A, B ως εξής :

A: το σύνολο όλων των συνδυασμών στο $\Sigma_m(E)$ *που δεν περιέχουν* το β, και

B: το σύνολο όλων των συνδυασμών στο $\Sigma_m(E)$ *που περιέχουν* το β.

Προφανώς,

$$|\Sigma_m(E)| = \binom{n}{m}$$

και

$$|\Sigma_m(E)| = |A| + |B|.$$

Επίσης, ισχύει ότι

$$A = \Sigma_m(E \setminus \{\beta\}),$$

δηλαδή A είναι το σύνολο των συνδυασμών των $n-1$ στοιχείων του $E \setminus \{\beta\}$ ανά m, οπότε

$$|A| = |\Sigma_m(E \setminus \{\beta\})| = \binom{n-1}{m}.$$

Από την άλλη, κάθε συνδυασμός $\sigma \in B$ περιέχει το β, οπότε γράφεται

$$\sigma = \{a_1, a_2, \ldots, a_{m-1}, \beta\}$$

όπου $a_i \in E \setminus \{\beta\}$ για κάθε $i \in [m-1]$.

Τότε ο συνδυασμός

$$\sigma' = \{a_1, a_2, \ldots, a_{m-1}\}$$

ανήκει στο σύνολο $\Sigma_{m-1}(E \setminus \{\beta\})$.

Επειδή η απεικόνιση $\sigma \to \sigma'$ από το B στο $\Sigma_{m-1}(E \setminus \{\beta\})$ είναι αμφιμονοσήμαντη, προκύπτει ότι

$$|B| = |\Sigma_{m-1}(E \setminus \{\beta\})| = \binom{n-1}{m-1}.$$

Άρα, τελικά

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}.$$ □

Πρόταση 3.8 (Κατακόρυφη αναγωγική εξίσωση). *Ισχύει ότι*

$$\binom{n}{m} = \binom{m-1}{m-1} + \binom{m}{m-1} + \cdots + \binom{n-1}{m-1} = \sum_{\nu=m}^{n} \binom{\nu-1}{m-1}.$$

Απόδειξη. Εφαρμόζοντας το τρίγωνο του Pascal για κάθε $\nu \in \{n, n-1, \ldots, m+1, m\}$ αντί n προκύπτουν οι ισότητες:

$$\begin{aligned}
\binom{n}{m} &= \binom{n-1}{m} + \binom{n-1}{m-1} \\
\binom{n-1}{m} &= \binom{n-2}{m} + \binom{n-2}{m-1} \\
\binom{n-2}{m} &= \binom{n-3}{m} + \binom{n-3}{m-1} \\
&\vdots \\
\binom{m+1}{m} &= \binom{m}{m} + \binom{m}{m-1} \\
\binom{m}{m} &= \binom{m-1}{m} + \binom{m-1}{m-1}
\end{aligned}$$

Προσθέτοντας κατά μέλη τις παραπάνω ισότητες έχουμε ότι

$$\binom{n}{m} = \binom{m-1}{m-1} + \binom{m}{m-1} + \cdots + \binom{n-3}{m-1} + \binom{n-2}{m-1} + \binom{n-1}{m-1}$$ □

Πρόταση 3.9 (Οριζόντια αναγωγική εξίσωση). *Ισχύει ότι*

$$\binom{n}{m} = (-1)^m \binom{n+1}{0} + (-1)^{m-1} \binom{n+1}{1} + \cdots + (-1)^{m-m} \binom{n+1}{m} = \sum_{\nu=0}^{m} (-1)^{m-\nu} \binom{n+1}{\nu}.$$

Απόδειξη. Άσκηση (Εφαρμογή της πρότασης 3.7 για $n+1$ αντί n και $\nu = 1, 2, \ldots, m$ αντί m.) □

Τρίγωνο του Pascal

Οι αριθμοί $\binom{n}{m}$ (για $n, m \leq 7$) δίδονται στο παρακάτω τρίγωνο το οποίο ονομάζεται τρίγωνο του Pascal.

n \ m	0	1	2	3	4	5	6	7
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Αριθμός επαναληπτικών συνδυασμών

Πρόταση 3.10 (Αριθμός επαναληπτικών συνδυασμών). *Ο αριθμός* $\left[\begin{matrix} n \\ m \end{matrix}\right]$ *ή* $E(n,m)$ *των επαναληπτικών συνδυασμών* n *στοιχείων ανά* m *ισούται με*

$$\left[\begin{matrix} n \\ m \end{matrix}\right] = \binom{n+m-1}{m}.$$

Απόδειξη. Δίδεται μια συνδυαστική απόδειξη.

Θεωρούμε τα σύνολα

$$E = \{x_1, x_2, \ldots, x_n\},$$

και

$$T = \{x_1, x_2, \ldots, x_n, x_{n+1}, \ldots, x_{n+m-1}\}.$$

Έστω $E_m(E)$ το σύνολο των επαναληπτικών συνδυασμών των n στοιχείων του E ανά m και $\Sigma_m(T)$ το σύνολο των συνδυασμών των $n+m-1$ στοιχείων του T ανά m.

Ισχύει ότι $|E_m(E)| = \left[\begin{matrix} n \\ m \end{matrix}\right]$ και $\Sigma_m(T) = \binom{n+m-1}{m}$.

Θα κατασκευασθεί μια αμφιμονοσήμαντη απεικόνιση μεταξύ των συνόλων $E_m(E)$ και $\Sigma_m(T)$.

Επειδή και στους επαναληπτικούς συνδυασμούς δεν παίζει ρόλο η σειρά, τα στοιχεία του $E_m(E)$ μπορούν να γραφούν υπό την μορφή:

$$\sigma = x_{i_1} x_{i_2} \cdots x_{i_k} \cdots x_{i_m}$$

όπου $i_1 \le i_2 \le \cdots \le i_m \le n$.

Για κάθε $\sigma \in E_m(E)$ ορίζουμε

$$\sigma' = x_{j_1} x_{j_2} \cdots x_{j_k} \cdots x_{j_m}$$

όπου

$$j_k = i_k + k - 1, \text{ για κάθε } k \in [m]$$

(δηλαδή "δείκτης" + "θέση" − 1).

Προφανώς για κάθε $k \in [m]$ ισχύουν:

$$j_k \le (m-1) + n = m + n - 1$$

και

$$j_1 < j_2 < \cdots < j_m,$$

δηλαδή τα στοιχεία του σ' είναι διακεκριμένα και επομένως $\sigma' \in \Sigma_m(T)$.
(Παράδειγμα, για $n = 8$ και $m = 5$:

$$E = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$$

$$T = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}\}.$$

Έστω σ ένας επαναληπτικός συνδυασμός του E, π.χ.

$$\sigma = x_2 x_7 x_2 x_5 x_7.$$

Επειδή και στους επαναληπτικούς συνδυασμούς δεν παίζει ρόλο η σειρά μπορούμε να γράφουμε:

$$\sigma = x_2 x_2 x_5 x_7 x_7.$$

Τότε, ο (απλός) συνδυασμός

$$\sigma' = x_2x_3x_7x_{10}x_{11}$$

είναι ένας συνδυασμός του T.)

Η απεικόνιση $\sigma \to \sigma'$ ειναι μια αμφιμονοσήμαντη απεικόνιση μεταξύ των συνόλων $E_m(E)$ και $\Sigma_m(T)$, οπότε είναι

$$|E_m(E)| = |\Sigma_m(T)| \Leftrightarrow \left[\!\!\binom{n}{m}\!\!\right] = \binom{n+m-1}{m}. \qquad \square$$

Αριθμός μεταθέσεων k ειδών στοιχείων με $n_1, n_2, \ldots, n_k$ στοιχεία αντίστοιχα

Πρόταση 3.11 (Αριθμός μεταθέσεων k ειδών στοιχείων). *Ο αριθμός $M(n_1, n_2, \ldots, n_k)$ των μεταθέσεων k ειδών στοιχείων με $n_1, n_2, \ldots, n_k$ στοιχεία αντίστοιχα δίδεται από τον τύπο*

$$M(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1!n_2!\cdots n_k!},$$

όπου $n = n_1 + n_2 \cdots n_k$.

Απόδειξη. Κάθε μετάθεση σ, k ειδών από τα οποία n_1 συμπίπτουν με a_1, n_2 συμπίπτουν με a_2, …, n_k συμπίπτουν με a_k μπορεί να κατασκευασθεί ως εξής:

Αρχικά τοποθετούμε τα n_1 (τα οποία είναι a_1 σε πλήθος) σε n_1 από τις n θέσεις:

σ _ _ $\underline{\alpha_1}$ _ _ $\underline{\alpha_1}$ _ _ $\underline{\alpha_1}$ _ _ _ _

Αυτό γίνεται με $\binom{n}{n_1}$ τρόπους.

Έπειτα τοποθετούμε τα n_2 (τα οποία είναι a_2 σε πλήθος) σε n_2 από τις $n - n_1$ θέσεις που περίσσεψαν:

σ _ $\underline{\alpha_2}$ $\underline{\alpha_1}$ $\underline{\alpha_2}$ _ $\underline{\alpha_1}$ _ _ $\underline{\alpha_1}$ $\underline{\alpha_2}$ _ $\underline{\alpha_2}$ _

Αυτό γίνεται με $\binom{n-n_1}{n_2}$ τρόπους.

Έπειτα τοποθετούμε τα n_3 (τα οποία είναι a_3 σε πλήθος) με $\binom{n-n_1-n_2}{n_3}$ τρόπους, κ.ο.κ.

Άρα, τελικά, για να κατασκευάσουμε όλες αυτές τις μεταθέσεις των k ειδών υπάρχουν

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}$$

τρόποι.

Έτσι,

$$\begin{aligned} M(n_1, n_2, \ldots, n_k) &= \frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdot\frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!}\cdots\frac{n_k!}{n_k!0!} \\ &= \frac{n!}{n_1!n_2!\cdots n_k!}. \end{aligned} \qquad \square$$

Ακέραιες Λύσεις Γραμμικής Εξίσωσης

Έστω $m, n \in \mathbb{N}^*$. Στην επόμενη πρόταση υπολογίζεται ο αριθμός των μη αρνητικών ακέραιων λύσεων της γραμμικής διοφαντικής εξίσωσης

$$x_1 + x_2 \cdots + x_n = m.$$

Οι λύσεις της εξίσωσης είναι διατεταγμένες n-άδες μη αρνητικών ακεραίων $(x_1, x_2, \ldots, x_n)$ με $x_1 + x_2 + \cdots + x_n = m$.

Στην περίπτωση όπου $x_i \in \{0, 1\}$ για κάθε $i \in [n]$, η αντίστοιχη λύση ονομάζεται $\{0,1\}$-**λύση**.

Στην περίπτωση όπου $x_i \in \mathbb{N}^*$ (αντ. $x_i \in \mathbb{N}$) για κάθε $i \in [n]$, έχουμε μια **θετική** (αντ. **μη αρνητική**) **ακέραια λύση**.

Πρόταση 3.12 (Αριθμός ακέραιων λύσεων γραμμικής εξίσωσης). *Έστω η γραμμική εξίσωση*

$$x_1 + x_2 \cdots + x_n = m \tag{3.4}$$

όπου $m, n \in \mathbb{N}^*$ και $x_i \in \mathbb{N}$ για κάθε $i \in [n]$. Τότε

i) Ο αριθμός των $\{0,1\}$-λύσεων της εξίσωσης (3.4), ισούται με $\binom{n}{m}$.

ii) Ο αριθμός των μη αρνητικών ακέραιων λύσεων της εξίσωσης (3.4) ισούται με $\left[\!\binom{n}{m}\!\right] = \binom{n+m-1}{m}$.

iii) Ο αριθμός των θετικών ακέραιων λύσεων της εξίσωσης (3.4) ισούται με $\binom{m-1}{n-1}$.

Απόδειξη. Θα δοθούν συνδυαστικές αποδείξεις.

i) Αρκεί να κατασκευασθεί μια αμφιμονοσήμαντη απεικόνιση f μεταξύ του συνόλου όλων των $\{0,1\}$-λύσεων $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ της εξίσωσης (3.4) και του συνόλου όλων των υποσυνόλων A του $[n]$ με $|A| = m$.

Πράγματι, θέτουμε

$$f(\mathbf{x}) = A_{\mathbf{x}} = \{i \in [n] : x_i = 1\}.$$

Αρκεί τώρα να δειχθεί ότι η f είναι καλά ορισμένη (δηλαδή ότι ισχύει $|A_{\mathbf{x}}| = m$) και ότι η f είναι $1-1$ και επί, με $f^{-1}(A) = (\mu_A(1), \mu_A(2), \ldots, \mu_A(n))$ για κάθε $A \subseteq [n]$ με $|A| = m$, όπου μ_A είναι η χαρακτηριστική συνάρτηση του A. (Άσκηση.)

ii) Αρκεί να κατασκευασθεί μια αμφιμονοσήμαντη απεικόνιση g μεταξύ του συνόλου όλων των μη αρνητικών ακέραιων λύσεων της εξίσωσης (3.4) και του συνόλου όλων των $\{0,1\}$-λύσεων

$$\mathbf{y} = (y_1, y_2, \ldots, y_{n+m-1})$$

της εξίσωσης

$$y_1 + y_2 + \cdots + y_{n+m-1} = m. \tag{3.5}$$

Αν $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ είναι μια λύση της εξίσωσης (3.4), τότε θέτουμε

$$\mathbf{y} = (\underbrace{1, 1, \ldots, 1}_{x_1 \text{ φορές}}, 0, \underbrace{1, 1, \ldots, 1}_{x_2 \text{ φορές}}, 0, \ldots, \underbrace{1, 1, \ldots, 1}_{x_{n-1} \text{ φορές}}, 0, \underbrace{1, 1, \ldots, 1}_{x_n \text{ φορές}}).$$

Το πλήθος των στοιχείων του $\mathbf{y}$ είναι $n + m - 1$ διότι $x_1 + x_2 + \cdots + x_n = m$ (πλήθος μονάδων) και το πλήθος των μηδενικών είναι $n - 1$.

Επειδή το άθροισμα των στοιχείων της $\mathbf{y}$ είναι m έπεται ότι $\mathbf{y}$ ειναι λύση της εξίσωσης (3.5).

Με άλλα λόγια, ορίζουμε $g(\mathbf{x}) = \mathbf{y}$ με

$$y_t = \begin{cases} 0, & \text{αν } t = x_1 + x_2 + \cdots + x_i + i \\ 1, & \text{αν } t \neq x_1 + x_2 + \cdots + x_i + i \end{cases}$$

όπου $i \in [n-1]$ και $t \in [n+m-1]$.

Αντίστροφα, αν $y = (y_1, y_2, \ldots, y_{n+m-1})$ είναι μια $\{0,1\}$-λύση της εξίσωσης (3.5) τότε υπάρχουν ακριβώς $n-1$ το πλήθος $t \in [n+m-1]$ με $y_t = 0$.

Τότε, για κάθε $i \in [n]$ ορίζουμε x_i το πλήθος μονάδων που περιέχονται μεταξύ του $(i-1)$-στού και i-στού μηδενικού. (Αν $i = 1$ θεωρούμε ένα φανταστικό 0 στην αρχή.)

Αρκεί τώρα να δειχθεί ότι η $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ είναι η μοναδική λύση της έξισωσης (3.5) με $g^{-1}(\mathbf{y}) = \mathbf{x}$. (Άσκηση.)

iii) Κάθε θετική ακέραια λύση της γραμμικής εξίσωσης

$$x_1 + x_2 + \cdots + x_n = m$$

αντιστοιχεί σε μια μη αρνητική ακέραια λύση της γραμμικής εξίσωσης

$$y_1 + y_2 + \cdots + y_n = m - n$$

όπου $y_1, y_2, \ldots, y_n \geq 0$ και $y_i = x_i - 1$ για κάθε $i \in [n]$.

Επομένως, ο αριθμός των θετικών ακέραιων λύσεων της γραμμικής εξίσωσης $x_1 + x_2 + \cdots + x_n = m$ ισούται με τον αριθμό των μη αρνητικών ακέραιων λύσεων της εξίσωσης $y_1 + y_2 + \cdots + y_n = m - n$, δηλαδή είναι ίσος με $\left[\begin{matrix} n \\ m-n \end{matrix}\right] = \binom{n + (m-n) - 1}{m-n} = \binom{m-1}{m-n} = \binom{m-1}{n-1}$. □

Παράδειγμα.

Η μη αρνητική ακέραια λύση

$$\mathbf{x} = (2, 0, 3, 1, 2)$$

της εξίσωσης

$$x_1 + x_2 + x_3 + x_4 + x_5 = 8$$

απεικονίζεται στην $\{0,1\}$-λύση

$$\mathbf{y} = (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$$

της εξίσωσης

$$y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} + y_{12} = 8$$

και στη θετική ακέραια λύση

$$\mathbf{z} = (3, 1, 4, 2, 3)$$

της εξίσωσης

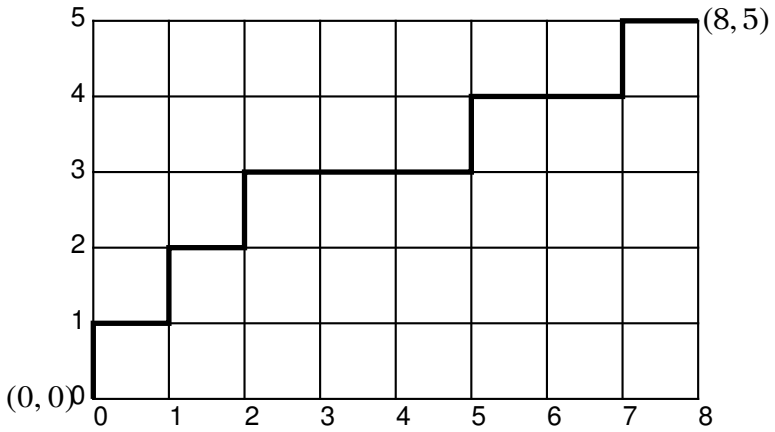
$$z_1 + z_2 + z_3 + z_4 + z_5 = 13.$$

Μονοπάτια

Θα ασχοληθούμε τώρα με **μονοπάτια** που βρίσκονται στο πρώτο τεταρτημόριο του Καρτεσιανού επιπέδου και ενώνουν το $(0,0)$ με κάποιο σημείο (n,m) χρησιμοποιώντας μόνο **βήματα** της μορφής $V = (0,1)$ (**κατακόρυφο βήμα**) και $H = (1,0)$ (**οριζόντιο βήμα**). Θα ταυτίζουμε, κάθε τέτοιο μονοπάτι με την αντίστοιχη ακολουθία με στοιχεία από το σύνολο $\{V,H\}$.

Παράδειγμα.

Το μονοπάτι $P = V\ H\ V\ H\ V\ H\ H\ H\ V\ H\ H\ V\ H$ ενώνει το $(0,0)$ με το $(8,5)$, όπως φαίνεται στο παρακάτω σχήμα.



Το **μήκος** (δηλαδή ο αριθμός των βημάτων) ενός μονοπατιού που ενώνει τα σημεία $(0,0)$ και (n,m) είναι ίσο με $n+m$. Συγκεκριμένα το μονοπάτι έχει n ορίζόντια και m κατακόρυφα βήματα.

Πρόταση 3.13 (**Αριθμός μονοπατιών**). *Το πλήθος των μονοπατιών που ενώνουν τα σημεία* $(0,0)$ *και* (n,m) *είναι ίσο με* $\binom{n+m}{n}$.

Αντιστοιχία μονοπατιών και μη αρνητικών ακέραιων λύσεων εξίσωσης

Κάθε μονοπάτι που ενώνει τα σημεία $(0,0)$ και $(n-1,m)$ αντιστοιχεί σε μια μη αρνητική και ακέραια λύση της εξίσωσης

$$x_1 + x_2 \cdots + x_n = m,$$

και αντιστρόφως.

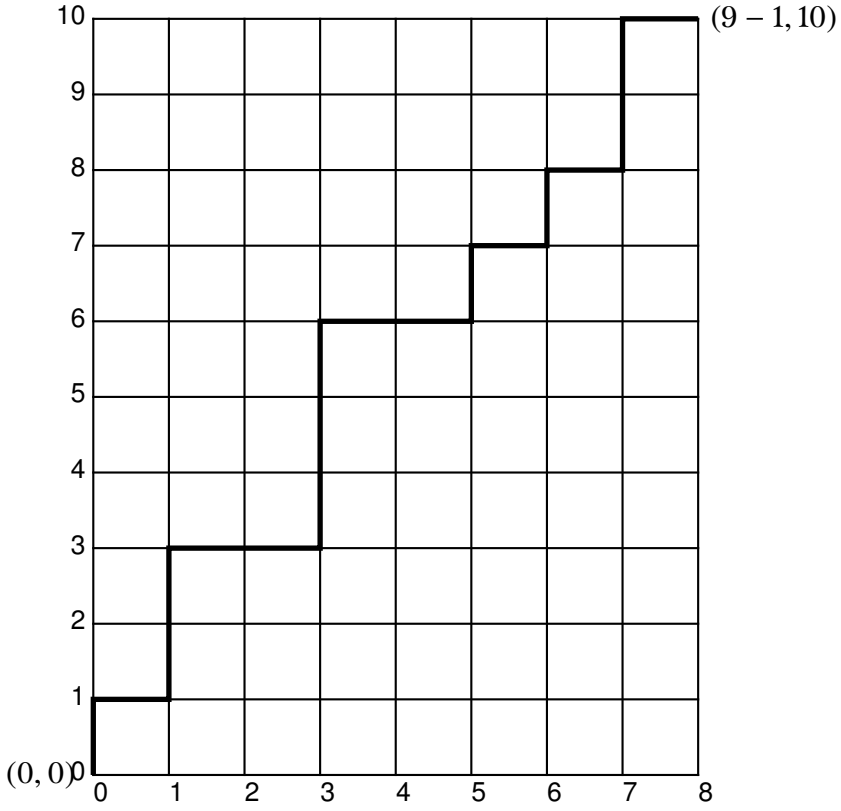
Πράγματι, το μονοπάτι P γράφεται μονοσήμαντα στη μορφή

$$P = V^{x_1} H V^{x_2} H V^{x_3} \cdots V^{x_{n-1}} H V^{x_n}$$

όπου x_{i+1}, $i \in [n-2]$, είναι το πλήθος των κατακόρυφων βημάτων μεταξύ του i-στού και $(i+1)$-οστού οριζόντιου βήματος, και x_1 (αντ. x_n) είναι το πλήθος των κατακόρυφων βημάτων πρίν (αντ. μετά) από το πρώτο (αντ. τελευταίο) οριζόντιο βήμα.

Το μονοπάτι P αντιστοιχεί στη λύση $(x_1, x_2, \ldots, x_n)$ της εξίσωσης $x_1 + x_2 + \cdots + x_n = m$.

Παράδειγμα.



Το μονοπάτι P γράφεται μονοσήμαντα στη μορφή

$$P = V^1\ H\ V^2 H\ V^0\ H\ V^3\ H\ V^0\ H\ V^1 H\ V^1 H\ V^2 H\ V^0$$

και αντιστοιχεί στην λύση

$$(1, 2, 0, 3, 0, 1, 1, 2, 0)$$

της εξίσωσης

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 10.$$

Από τα προηγούμενα συνάγεται το επόμενο αποτέλεσμα:

Πρόταση 3.14. *Το πλήθος των μη αρνητικών και ακέραιων λύσεων της εξίσωσης*

$$x_1 + x_2 + \cdots + x_n = m$$

είναι ίσο με το πλήθος των μονοπατιών που ενώνουν τα σημεία $(0, 0)$ *και* $(n - 1, m)$*, δηλαδή ίσο με*

$$\binom{n + m - 1}{n - 1} = \left[\begin{matrix} n \\ m \end{matrix}\right].$$

3.4 Συνδυαστικά μοντέλα και συνδυαστικές αποδείξεις

Σημείωση. Η ενότητα αυτή είναι καλύτερο να μελετηθεί αφού προηγηθεί η εξοικείωση με τις βασικές έννοιες μέσα από την μελέτη των λυμένων ασκήσεων 3.1 μέχρι και 3.26.

Στο κεφάλαιο αυτό συναντήσαμε πολλές φορές την έννοια της **συνδυαστικής απόδειξης**.

Η κεντρική ιδέα αυτής της μεθόδου απόδειξης είναι η εξής: Μπορούμε να αποδείξουμε ότι ισχύει ένας τύπος *ερμηνεύοντας* κάθε μέλος του τύπου ως απάντηση στο ίδιο πρόβλημα απαρίθμησης κάποιων κατάλληλα επιλεγμένων αντικειμένων.

Παράδειγμα. Για να αποδείξουμε ότι ισχύει ο τύπος

$$\binom{n}{k} = \binom{n}{n-k} \text{ για κάθε } n, k \in \mathbb{N} \text{ με } k \leq n,$$

μπορούμε να θεωρήσουμε το πρόβλημα της επιλογής ενός υποσυνόλου k στοιχείων από το σύνολο $[n] = \{1, 2, 3, \ldots, n\}$.

Από τη μία, μπορούμε να καθορίσουμε το ζητούμενο υποσύνολο επιλέγοντας με $\binom{n}{k}$ τρόπους τα k από τα n στοιχεία του.

Από την άλλη, μπορούμε να καθορίσουμε το ζητούμενο υποσύνολο επιλέγοντας τα $n-k$ στοιχεία του $[n]$ που **δεν** θα περιληφθούν σε αυτό (και άρα θα περιληφθούν τα υπόλοιπα k από τα στοιχεία του n). Αυτό μπορεί να γίνει με $\binom{n}{n-k}$ τρόπους.

Επειδή και οι δύο προσεγγίσεις απαντούν σωστά στο ίδιο πρόβλημα, έπεται ότι οι δύο λύσεις είναι ίσες. Άρα,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Λέμε ότι τα υποσύνολα του $[n]$ με k στοιχεία αποτελούν ένα **συνδυαστικό μοντέλο** για την παραπάνω ισότητα, διότι η απαρίθμησή τους με δύο διαφορετικές προσεγγίσεις αποδεικνύει **γιατί ισχύει** η ισότητα. Στην περίπτωση αυτή λέμε ότι αυτό το συνδυαστικό μοντέλο **ερμηνεύει** την ισότητα.

Παράδειγμα. Για να αποδείξουμε ότι ισχύει ο τύπος

$$k\binom{n}{k} = n\binom{n-1}{k-1}, \text{ για κάθε } n, k \in \mathbb{N}^* \text{ με } k \leq n,$$

μπορούμε να θεωρήσουμε το πρόβλημα συγκρότησης μιας k-μελούς επιτροπής από ένα σύνολο n υποψηφίων, στην οποία κάποιο μέλος της θα είναι ο πρόεδρος της επιτροπής.

Αφενός, ο καθορισμός της επιτροπής μπορεί να γίνει επιλέγοντας αρχικά τα k μέλη της με $\binom{n}{k}$ τρόπους και στη συνέχεια εκλέγοντας τον πρόεδρο αυτής μεταξύ των k επιλεγμένων μελών της με $\binom{k}{1} = k$ τρόπους. Άρα, συνολικά υπάρχουν $k\binom{n}{k}$ τρόποι καθορισμού της.

Αφετέρου, η επιτροπή μπορεί να συγκροτηθεί επιλέγοντας αρχικά τον πρόεδρο αυτής με $\binom{n}{1} = n$ τρόπους και στη συνέχεια τα υπόλοιπα $k-1$ μέλη της από τους εναπομείναντες $n-1$ υποψήφιους. Αυτό μπορεί να γίνει με $\binom{n-1}{k-1}$ τρόπους. Άρα, συνολικά υπάρχουν $n\binom{n-1}{k-1}$ τρόποι καθορισμού της.

Επειδή, και οι δύο μέθοδοι δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι οι αριθμοί που βρήκαμε είναι ίσοι. Άρα,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Οι k-μελείς επιτροπές με πρόεδρο από ένα σύνολο $[n]$ υποψηφίων αποτελούν ένα **συνδυαστικό μοντέλο** για την παραπάνω ισότητα, διότι η απαρίθμησή τους **ερμηνεύει** την ισότητα.

Για κάθε τύπο μπορούν να υπάρχουν **άπειρα** συνδυαστικά μοντέλα που τον ερμηνεύουν. Στην ενότητα αυτή θα δούμε ορισμένα απλά βασικά συνδυαστικά μοντέλα που ερμηνεύουν πολλούς τύπους.

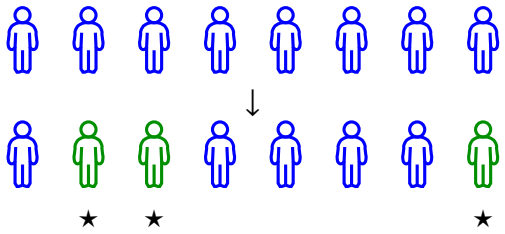
3.4.1 Το συνδυαστικό μοντέλο των επιτροπών

Το συνδυαστικό μοντέλο των επιτροπών αναφέρεται σε προβλήματα συγκρότητησης μιας ή περισσοτέρων επιτροπών από ένα σύνολο n υποψηφίων λαμβάνοντας υπόψη διάφορους περιορισμούς, π.χ. οι επιτροπές να έχουν πρόεδρο, να έχουν και γραμματέα, να περιλαμβάνουν άτομα του ίδιου φύλου κ.ο.κ.

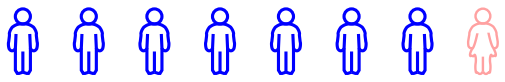
Παράδειγμα 3.4.1. *Να αποδειχθεί ότι* $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, *για κάθε* $n, k \in \mathbb{N}^*$ *με* $n \leq k$.

Λύση. Προκειμένου να ερμηνεύσουμε συνδυαστικά τα δύο μέλη θεωρούμε το πρόβλημα της συγκρότησης μιας k-μελούς επιτροπής από ένα σύνολο n υποψηφίων εκ των οποίων $n-1$ είναι άνδρες και μια είναι γυναίκα.

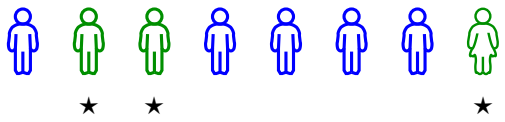
(*1η προσέγγιση.*) Ο αριθμός $\binom{n}{k}$ ισούται με τον αριθμό των τρόπων συγκρότητησης της k-μελούς επιτροπής από το σύνολο των n υποψηφίων, χωρίς να λάβουμε υπόψη αν επιλέγουμε άνδρες ή γυναίκες.



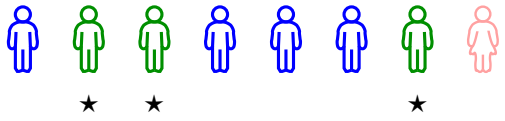
(*2η προσέγγιση.*) Προκειμένου να ερμηνεύσουμε συνδυαστικά το άθροισμα του δευτέρου μέλους παρατηρούμε ότι οι επιτροπές χωρίζονται σε δύο κατηγορίες: Σε αυτές που περιέχουν την γυναίκα και σε αυτές που αποτελούνται μόνο από άνδρες.



Στην πρώτη περίπτωση υπάρχουν $\binom{n-1}{k-1}$ τρόποι επιλογής των υπολοίπων $k-1$ μελών από τους $n-1$ άνδρες υποψηφίους.



Στην δεύτερη περίπτωση υπάρχουν $\binom{n-1}{k}$ τρόποι επιλογής των k ανδρών από τους $n-1$ άνδρες υποψηφίους.



Άρα, συνολικά, υπάρχουν $\binom{n-1}{k} + \binom{n-1}{k-1}$ τρόποι συγκρότησης της k-μελούς επιτροπής.

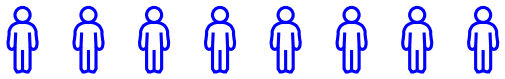
Επειδή, οι δύο προσεγγίσεις δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι είναι ίσες. Άρα,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

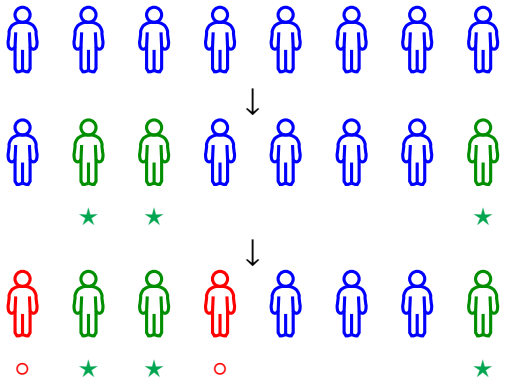
□

Παράδειγμα 3.4.2. *Να αποδειχθεί ότι* $\binom{n}{k}\binom{n-k}{\lambda} = \binom{n}{\lambda}\binom{n-\lambda}{k}$, *για κάθε* $n \in \mathbb{N}^*$, $k, \lambda \in \mathbb{N}$ *με* $k + \lambda \leq n$.

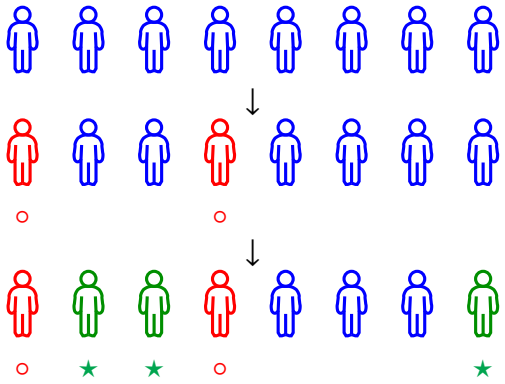
Λύση. Θεωρούμε το πρόβλημα συγκρότησης δύο ξένων μεταξύ τους διαφορετικών επιτροπών με k και λ μέλη αντίστοιχα από ένα σύνολο n υποψηφίων.



(*1η προσέγγιση.*) Η πρώτη επιτροπή καθορίζεται αν επιλέξουμε τα k μέλη της με $\binom{n}{k}$ τρόπους. Η δεύτερη επιτροπή μπορεί να σχηματισθεί επιλέγοντας λ από τους υπόλοιπους $n-k$ υποψηφίους με $\binom{n-k}{\lambda}$ τρόπους. Άρα, υπάρχουν $\binom{n}{k}\binom{n-k}{\lambda}$ τρόποι συγκρότησης των δύο επιτροπών.



(*2η προσέγγιση.*) Μπορούμε να αρχίσουμε τον καθορισμό των επιτροπών από τη δεύτερη. Η δεύτερη επιτροπή καθορίζεται με $\binom{n}{\lambda}$ τρόπους, ενώ η πρώτη επιλέγοντας k από τους εναπομείναντες $n-\lambda$ υποψηφίους με $\binom{n-\lambda}{k}$ τρόπους. Άρα, υπάρχουν $\binom{n}{\lambda}\binom{n-\lambda}{k}$ τρόποι συγκρότησης των δύο επιτροπών.



Επειδή, οι δύο προσεγγίσεις δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι είναι ίσες. Άρα,

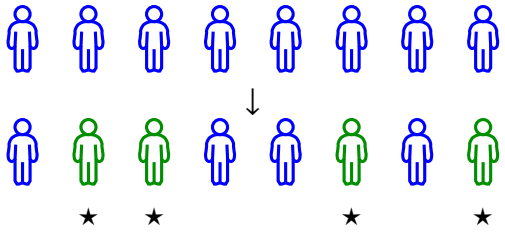
$$\binom{n}{k}\binom{n-k}{\lambda} = \binom{n}{\lambda}\binom{n-\lambda}{k}.$$

□

Παράδειγμα 3.4.3. *Να αποδειχθεί ότι* $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$, *για κάθε* $n \in \mathbb{N}^*$.

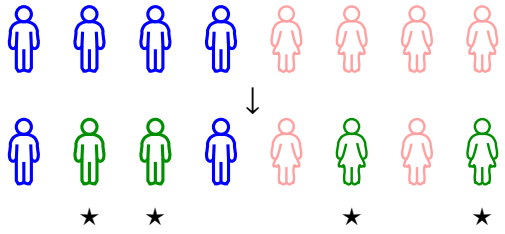
Λύση. Θεωρούμε το πρόβλημα της συγκρότησης μιας n-μελούς επιτροπής από ένα σύνολο $2n$ υποψήφιων που αποτελείται από n άνδρες και n γυναίκες.

(*1n προσέγγιση.*) Ο αριθμός $\binom{2n}{n}$ ισούται με τον αριθμό των τρόπων συγκρότησης μιας n-μελούς επιτροπής από το σύνολο των $2n$ υποψηφίων χωρίς να λαμβάνουμε υπόψη αν επιλέγεται άνδρας ή γυναίκα.



(*2n προσέγγιση.*) Διακρίνουμε περιπτώσεις ως προς τον αριθμό k των ανδρών που συμμετέχουν στην επιτροπή.

Υπάρχουν $\binom{n}{k}$ τρόποι για να επιλέξουμε k από τους n άνδρες και $\binom{n}{n-k}$ τρόποι για να επιλέξουμε τα υπόλοιπα $n-k$ μέλη της επιτροπής από τις n γυναίκες. Επομένως, στην περίπτωση αυτή υπάρχουν $\binom{n}{k}\binom{n}{n-k}$ τρόποι συγκρότησης της επιτροπής. Για να βρούμε το συνολικό πλήθος των τρόπων πρέπει να αθροίσουμε για κάθε $k = 0, 1, 2, \ldots, n$, οπότε προκύπτει ότι ο ζητούμενος αριθμός ισούται με $\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$.



Επειδή, οι δύο προσεγγίσεις δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι είναι ίσες. Άρα,

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}.$$

□

3.4.2 Το συνδυαστικό μοντέλο των λέξεων

Το συνδυαστικό μοντέλο των λέξεων αναφέρεται σε προβλήματα κατασκευής λέξεων με γράμματα από ένα καθορισμένο αλφάβητο λαμβάνοντας υπόψη διάφορους περιορισμούς ή ιδιότητες, π.χ. οι λέξεις πρέπει να αρχίζουν από ένα συγκεκριμένο γράμμα, να μην περιέχουν διαδοχικά δύο ίδια γράμματα, κ.ο.κ.

Παράδειγμα 3.4.4. *Να δειχθεί ότι* $3^n = 3^{n-1} + 3^{n-1} + 3^{n-1}$, *για κάθε* $n \in \mathbb{N}^*$.

Λύση. Θεωρούμε το σύνολο των λέξεων μήκους n που κατασκευάζονται από τα σύμβολα A, B, C (και στις οποίες επιτρέπονται επαναλήψεις).

(*1η προσέγγιση.*) Για κάθε ένα από τα n γράμματα της λέξης υπάρχουν 3 επιλογές. Άρα, συνολικά υπάρχουν 3^n διαφορετικές λέξεις.

(*2η προσέγγιση.*) Οι λέξεις αυτές χωρίζονται σε 3 κατηγορίες σε αυτές που αρχίζουν με A, σε αυτές που αρχίζουν με B και σε αυτές που αρχίζουν με C. Σε κάθε μια από τις 3 περιπτώσεις, οι λέξη που ακολουθεί μετά το πρώτο γράμμα αποτελείται από $n-1$ γράμματα, κάθε ένα από τα οποία έχει 3 επιλογές. Άρα υπάρχουν, για κάθε περίπτωση, 3^{n-1} λέξεις. Άρα, συνολικά, $3^{n-1} + 3^{n-1} + 3^{n-1}$ λέξεις.

Επειδή, οι δύο προσεγγίσεις δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι είναι ίσες. Άρα,

$$3^n = 3^{n-1} + 3^{n-1} + 3^{n-1}.$$ □

Παράδειγμα 3.4.5. *Να δειχθεί ότι* $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$.

Απόδειξη. Θεωρούμε τα σύνολα των λέξεων μήκους $2n$ που κατασκευάζονται από τα σύμβολα 0 και 1 και περιέχουν ίσο αριθμό 0 και 1.

(*1η προσέγγιση.*) Κάθε λέξη με αυτές τις ιδιότητες καθορίζεται από τις θέσεις των 0 (αφού στις υπόλοιπες θέσεις θα υπάρχουν υποχρεωτικά 1). Υπάρχουν $\binom{2n}{n}$ τρόποι να επιλέξουμε τις n θέσεις των 0 από τις $2n$ διαθέσιμες θέσεις. Άρα, το πλήθος αυτών των λέξεων είναι $\binom{2n}{n}$.

(*2η προσέγγιση.*) Οι λέξεις αυτές διαμερίζονται σε κατηγορίες με βάση τον αριθμό k των 0 που βρίσκονται στις πρώτες n θέσεις της λέξης.

Αν μια λέξη περιέχει ακριβώς k 0 στις πρώτες n θέσεις της, τότε θα περιέχει $n-k$ 0 στις υπόλοιπες n θέσεις της. Υπάρχουν $\binom{n}{k}$ τρόποι επιλογής των k 0 στις πρώτες n θέσεις και $\binom{n}{n-k}$ τρόποι επιλογής των $n-k$ 0 στις υπόλοιπες n θέσεις της. Αρα, σ' αυτή την περίπτωση, υπάρχουν $\binom{n}{k}\binom{n}{n-k}$ λέξεις.

Για να βρούμε το συνολικό πλήθος των λέξεων πρέπει να αθροίσουμε για κάθε $k = 0, 1, 2, \ldots, n$, οπότε προκύπτει ότι ο ζητούμενος αριθμός ισούται με $\sum_{k=0}^{n} \binom{n}{k} 2^{n-k}$.

Επειδή, οι δύο προσεγγίσεις δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι είναι ίσες. Άρα,

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}.$$ □

Παράδειγμα 3.4.6. *Να δειχθεί ότι* $3^n = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}$, *για κάθε* $n \in \mathbb{N}^*$.

Λύση. Θεωρούμε το σύνολο των λέξεων μήκους n που κατασκευάζονται από τα σύμβολα A, B, C (και στις οποίες επιτρέπονται επαναλήψεις).

(*1η προσέγγιση.*) Για κάθε ένα από τα n γράμματα της λέξης υπάρχουν 3 επιλογές. Άρα, συνολικά υπάρχουν 3^n διαφορετικές λέξεις.

(*2n προσέγγιση.*) Οι λέξεις αυτές διαμερίζονται σε κατηγορίες με βάση τον αριθμό k των A που περιέχουν.

Αν μια λέξη περιέχει ακριβώς k A υπάρχουν $\binom{n}{k}$ τρόποι να επιλεγούν οι θέσεις των k A από τις n διαθέσιμες θέσεις. Στις υπόλοιπες $n-k$ θέσεις πρέπει υποχρεωτικά να τοποθετηθούν B ή C. Για κάθε μια από αυτές τις $n-k$ θέσεις υπάρχουν 2 επιλογές, άρα υπάρχουν 2^{n-k} τρόποι συμπλήρωσης. Συνολικά, σ' αυτή την περίπτωση, υπάρχουν $\binom{n}{k}2^{n-k}$ λέξεις.

Για να βρούμε το συνολικό πλήθος των λέξεων πρέπει να αθροίσουμε για κάθε $k = 0, 1, 2, \ldots, n$, οπότε προκύπτει ότι ο ζητούμενος αριθμός ισούται με $\sum_{k=0}^{n} \binom{n}{k}2^{n-k}$.

Επειδή, οι δύο προσεγγίσεις δίνουν την σωστή απάντηση στο ίδιο πρόβλημα απαρίθμησης, έπεται ότι είναι ίσες. Άρα,

$$3^n = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}. \qquad \square$$

3.5 Λυμένες ασκήσεις

Άσκηση 3.1. *Από μια κληρωτίδα που περιέχει 100 λαχνούς αριθμημένους από το 1 μέχρι το 100 κληρώνονται διαδοχικά 5 λαχνοί, χωρίς μετά από κάθε κλήρωση να επανατοποθετούνται στη κληρωτίδα. Ο πρώτος λαχνός που κληρώνεται κερδίζει 10000 ευρώ, ο δεύτερος 5000 ευρώ, ο τρίτος 3000 ευρώ, ο τέταρτος 2000 ευρώ και ο πέμπτος 1000 ευρώ. Να βρεθεί το πλήθος των δυνατών αποτελεσμάτων της κλήρωσης.*

Λύση. Για τον υπολογισμό των δυνατών αποτελεσμάτων παρατηρούμε ότι η σειρά με την οποία εξάγονται οι αριθμοί είναι σημαντική λόγω του διαφορετικού ποσού που κερδίζεται σε κάθε κλήρωση. Έτσι ο ζητούμενος αριθμός θα είναι ίσος με τον αριθμό των διατάξεων των 100 ανά 5 δηλαδή

$$P(100,5) = \frac{100!}{(100-5)!} = 100 \cdot 99 \cdot 98 \cdot 97 \cdot 96 = 9034502400. \qquad \square$$

Άσκηση 3.2. *Να βρεθεί ο αριθμός των τρόπων αποστολής* 10 *διαφορετικών μηνυμάτων σε* 10 *διαφορετικούς παραλήπτες.*

Λύση. Για το πρώτο μήνυμα υπάρχουν 10 επιλογές αποστολής. Για το δεύτερο μήνυμα υπάρχουν 9 επιλογές, κ.ο.κ. Επομένως, ο ζητούμενος αριθμός ισούται με τον αριθμό των μεταθέσεων των 10 μηνυμάτων, δηλαδή ισούται με $10! = 3628800$. $\square$

Άσκηση 3.3. *Να βρεθεί ο αριθμός των διαφορετικών συνθηματικών μήκους* 10 *τα οποία κατασκευάζονται από τα γράμματα του αγγλικού αλφαβήτου (τα οποία διακρίνονται σε κεφαλαία και πεζά) και τους* 23 *επιπλέον χαρακτήρες* $\sim$, !, @, #, \$, %, ^, &, $*$, (,), $-$, $+$, $=$, _(*underscore*), |, .(*fullstop*), ,(*comma*), ?, >, <, \, /.

Λύση. Για κάθε ένα από τους 10 χαρακτήρες του συνθηματικού υπάρχουν 26+26+23 = 75 επιλογές. Επειδή επιτρέπονται επαναλήψεις, ο ζητούμενος αριθμός ισούται με τον αριθμό των επαναληπτικών διατάξεων 75 στοιχείων ανά 10, δηλαδή ισούται με $U(75,10) = 75^{10} = 5631351470947265625$. $\square$

Άσκηση 3.4. *Πόσους τετραψήφιους φυσικούς αριθμούς μπορούμε να κατασκευάσουμε με τα ψηφία 1, 2, 3, 4, 5, 6, 7*

(i) όταν όλα τα ψηφία τους είναι διαφορετικά,

(ii) όταν τα ψηφία τους μπορεί να επαναλαμβάνονται,

(iii) όταν πρέπει να είναι περιττοί και τα ψηφία τους μπορεί να επαναλαμβάνονται,

(iv) όταν το άθροισμα του δεύτερου και τέταρτου ψηφίου τους είναι ίσο με 9 και τα ψηφία τους να είναι διαφορετικά.

Λύση. Επειδή στην κατασκευή των αριθμών αυτών παίζει ρόλο η σειρά των ψηφίων τους, πρόκειται για διατάξεις στο (i) και για επαναληπτικές διατάξεις στο (ii) των 7 ψηφίων ανά 4. Έτσι μπορούμε να κατασκευάσουμε:

(i) $P(7,4) = \frac{7!}{(7-4)!} = \frac{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7}{1\cdot2\cdot3} = 840$ φυσικούς αριθμούς με διαφορετικά ψηφία.

(ii) $U(7,4) = 7^4 = 2401$ φυσικούς αριθμούς με ψηφία που μπορεί να επαναλαμβάνονται.

(iii) Επειδή θέλουμε οι αριθμοί που κατασκευάζουμε να είναι περιττοί θα υπάρχουν 4 διαφορετικές επιλογές για το τελευταίο ψηφίο τους (1 ή 3 ή 5 ή 7). Για τα υπόλοιπα 3 φηφία τους υπάρχουν 7 επιλογές (διότι τα ψηφία τους μπορεί να επαναλαμβάνονται). Έτσι εδώ μπορούμε να κατασκευάσουμε $4 \cdot 7^3 = 1372$ τέτοιους αριθμούς.

(iv) Έστω $xyzw$ ένας τέτοιος αριθμός. Πρέπει να ισχύει $y + w = 9$ οπότε υπάρχουν 6 επιλογές για το ζευγάρι (y, w):

$$(2,7), (7,2), (3,6), (6,3), (4,5) \text{ και } (5,4).$$

Αφού έχουμε διαλέξει το ζευγάρι (y, w), το ζευγάρι (x, z) θα επιλέγεται μεταξύ των διατάξεων του συνόλου $[7] \setminus \{y, w\}$, δηλαδή θα επιλέγεται με $P(5,2)$ τρόπους.

Άρα σύμφωνα με τον κανόνα του γινομένου, μπορούμε να κατασκευάσουμε $6 \cdot P(5,2) = 6\frac{5!}{(5-2)!} = 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$ διαφορετικούς αριθμούς. □

Άσκηση 3.5. *Να βρεθεί ο αριθμός των διαφορετικών τυχερών εξάδων που μπορούν να κληρωθούν στο παιχνίδι "Λόττο".*

Λύση. Κάθε τυχερή εξάδα αντιστοιχεί σε ένα υποσύνολο έξι στοιχείων από το σύνολο $[49] = \{1, 2, \ldots, 49\}$. (Δεν έχει σημασία η σειρά με την οποία κληρώνονται οι αριθμοί.) Επομένως, ο ζητούμενος αριθμός ισούται με τον αριθμό των συνδυασμών των 49 στοιχείων ανά 6, δηλαδή ισούται με $\binom{49}{6} = 13983816$. □

Άσκηση 3.6. *Κατά πόσους τρόπους μπορεί να σχηματισθεί μια τετραμελής Πανεπιστημιακή επιτροπή από 4 φοιτητές, 3 λέκτορες και 2 καθηγητές*

(i) αν όλοι είναι εξίσου εκλέξιμοι,

(ii) αν η επιτροπή δεν περιέχει κανένα φοιτητή,

(iii) αν η επιτροπή περιέχει ακριβώς ένα φοιτητή,

(iv) αν η επιτροπή περιέχει τουλάχιστον ένα φοιτητή,

(v) αν η επιτροπή περιέχει το πολύ ένα λέκτορα,

(vi) αν η επιτροπή πρεπει να περιέχει 1 καθηγητή, 1 λέκτορα και 2 φοιτητές.

Λύση. Επειδή στο σχηματισμό της επιτροπής τα μέλη της έχουν ισότιμο ρόλο, πρόκειται για συνδυασμούς.

Έτσι,

(i) Ο ζητούμενος αριθμός ισούται με τον αριθμό των συνδυασμών των $4 + 3 + 2 = 9$ ατόμων ανά 4, δηλαδή

$$\binom{9}{4} = \frac{9!}{4!(9-4)!} = \frac{6 \cdot 7 \cdot 8 \cdot 9}{1 \cdot 2 \cdot 3 \cdot 4} = 126.$$

(ii) Ο ζητούμενος αριθμός ισούται με τον αριθμό των συνδυασμών των $3 + 2 = 5$ (εξαιρούνται οι φοιτητές) ανά 4, δηλαδή

$$\binom{5}{4} = \frac{5!}{4!(5-4)!} = 5.$$

(iii) Για τον φοιτητή που θα επιλεγεί υπάρχουν $\binom{4}{1} = 4$ τρόποι. Για τα υπόλοιπα 3 μέλη της επιτροπής υπάρχουν $\binom{3+2}{3} = \binom{5}{3} = 10$ τρόποι. Έτσι, σύμφωνα με την πολλαπλασιαστική αρχή ο ζητούμενος αριθμός ισούται με $4 \cdot 10 = 40$.

(iv) Ο αριθμός των επιτροπών που περιέχουν τουλάχιστον ένα φοιτητή ισούται με τη διαφορά του αριθμού των επιτροπών όπου όλοι είναι εξίσου εκλέξιμοι και του αριθμού των επιτροπών που δεν περιέχουν κανένα φοιτητή, δηλαδή

$$\binom{9}{4} - \binom{5}{4} = 126 - 5 = 121.$$

(v) Ο αριθμός των επιτροπών που περιέχουν το πολύ ένα λέκτορα ισούται με το άθροισμα του αριθμού των επιτροπών που δεν περιέχουν *κανένα* λέκτορα και του αριθμού των επιτροπών που περιέχουν *ακριβώς ένα* λέκτορα.

Ο πρώτος αριθμός ισούται με $\binom{4+2}{4} = \binom{6}{4} = 15$.

Ο δεύτερος αριθμός ισούται με $\binom{3}{1}\binom{6}{3} = 3 \cdot 20 = 60$.

Επομένως, ο ζητούμενος αριθμός ισούται με $15 + 60 = 75$.

(vi) Για κάθε καθηγητή που θα εκλεγεί υπάρχουν $\binom{2}{1} = 2$ τρόποι, για τον λέκτορα $\binom{3}{1} = 3$ τρόποι, ενω για τους 2 φοιτητές $\binom{4}{2} = 6$ τρόποι. Έτσι, σύμφωνα με την πολλαπλασιαστική αρχή ο ζητούμενος αριθμός θα είναι ίσος με $2 \cdot 3 \cdot 6 = 36$. □

Άσκηση 3.7. *Να βρεθεί με πόσους τρόπους μπορούμε να επιλέξουμε τρεις διαφορετικούς αριθμούς από το σύνολο* [90] *ώστε το άθροισμά τους να είναι πολλαπλάσιο του* 3.

Λύση. Το άθροισμα τριών θετικών ακεραίων είναι πολλαπλάσιο του 3 στις παρακάτω 4 περιπτώσεις:

(i) Και οι τρεις αριθμοί είναι πολλαπλάσια του 3.

(ii) Και οι τρεις αριθμοί αφήνουν υπόλοιπο 1 όταν διαιρεθούν με το 3.

(iii) Και οι τρεις αριθμοί αφήνουν υπόλοιπο 2 όταν διαιρεθούν με το 3.

(iv) Οι τρεις αριθμοί αφήνουν διαφορετικό υπόλοιπο ο καθένας όταν διαιρεθεί με το 3 (δηλαδή αφήνουν υπόλοιπα 0, 1 και 2 αντίστοιχα).

Μεταξύ των αριθμών του συνόλου [90] υπάρχουν ακριβώς 30 αριθμοί που αφήνουν υπόλοιπο 0 όταν διαιρεθούν με το 3 (δηλαδή, είναι πολλαπλάσια του 3), υπάρχουν 30 αριθμοί που αφήνουν υπόλοιπο 1 και 30 αριθμοί που αφήνουν υπόλοιπο 2.

Επομένως, στην πρώτη περίπτωση υπάρχουν $\binom{30}{3}$ τρόποι επιλογής, στη δεύτερη περίπτωση υπάρχουν άλλοι $\binom{30}{3}$ τρόποι και επιπλέον $\binom{30}{3}$ τρόποι για την τρίτη περίπτωση. Τέλος, στη τέταρτη περίπτωση υπάρχουν $\binom{30}{1}\binom{30}{1}\binom{30}{1}$ τρόποι επιλογής των τριών αριθμών.

Άρα, συνολικά υπάρχουν $3\binom{30}{3} + \binom{30}{1}^3 = 15 \cdot 29 \cdot 28 + 30^3 = 39180$ τρόποι επιλογής των τριών αριθμών. □

Άσκηση 3.8. *Με πόσους τρόπους μπορεί από 12 ανδρόγυνα να επιλεγεί μια εξαμελής επιτροπή:*

(i) Χωρίς περιορισμό.

(ii) Η επιτροπή δεν μπορεί να περιέχει κάποιο ανδρόγυνο.

(iii) Η επιτροπή αποτελείται από πρόεδρο, αντιπρόεδρο, γραμματέα και τρία μέλη.

(iv) Η επιτροπή αποτελείται από πρόεδρο και γραμματέα οι οποίοι είναι άνδρες, από δύο αντιπρόεδρους οι οποίες είναι γυναίκες και από δύο μέλη διαφορετικού φύλου.

Λύση.

(i) Ο ζητούμενος αριθμός ισούται με τον αριθμό των συνδυασμών των 24 ατόμων ανά 6, δηλαδή

$$\binom{24}{6} = 134596.$$

(ii) Από κάθε ανδρόγυνο μπορεί να συμμετέχει το πολύ ένα άτομο.

Αρχικά επιλέγουμε ποια ανδρόγυνα θα εκπροσωπηθούν στην επιτροπή. Η επιλογή αυτή μπορεί να γίνει με $\binom{12}{6}$ τρόπους.

Για κάθε ένα από τα 6 ανδρόγυνα που επιλέχθηκαν υπάρχουν 2 επιλογές για το ποιος από τους δύο θα είναι στην επιτροπή.

Άρα, συνολικά, υπάρχουν $\binom{12}{6} \cdot 2^6 = 59136$ τρόποι σχηματισμού της επιτροπής.

(iii) Για το σχηματισμό της επιτροπής λαμβάνουμε υπόψη τους διακριτούς ρόλους του προέδρου, αντιπροέδρου, γραμματέα και απλού μέλους.

(1ος τρόπος)

Για την εκλογή του προέδρου υπάρχουν 24 επιλογές.

Για την εκλογή του αντιπροέδρου υπάρχουν 23 επιλογές.

Για την εκλογή του γραμματέα υπάρχουν 22 επιλογές.

Για τα τρία (απλά) μέλη υπάρχουν $\binom{21}{3}$ επιλογές.

Άρα, συνολικά, υπάρχουν $24 \cdot 23 \cdot 22 \cdot \binom{21}{3} = 16151520$ τρόποι σχηματισμού της επιτροπής.

(2ος τρόπος)

Αρχικά επιλέγουμε τα άτομα που θα συμμετέχουν στην επιτροπή και στη συνέχεια τους αναθέτουμε ρόλους.

Για την εκλογή των 6 μελών υπάρχουν $\binom{24}{6}$ επιλογές.

Για την εκλογή του προέδρου υπάρχουν 6 επιλογές.

Για την εκλογή του αντιπροέδρου υπάρχουν 5 επιλογές.

Για την εκλογή του γραμματέα υπάρχουν 4 επιλογές.

Άρα, συνολικά, υπάρχουν $\binom{24}{6} \cdot 6 \cdot 5 \cdot 4 = 16151520$ τρόποι σχηματισμού της επιτροπής.

(iv) (1ος τρόπος)

Για την εκλογή του άνδρα προέδρου υπάρχουν 12 επιλογές.

Για την εκλογή του άνδρα γραμματέα υπάρχουν 11 επιλογές.

Για την εκλογή των δύο γυναικών αντιπροέδρων υπάρχουν $\binom{12}{2}$ επιλογές.

Για τα δύο μέλη διαφορετικού φύλλου έχουμε $10 \cdot 10$ επιλογές.

Άρα, συνολικά, υπάρχουν $12 \cdot 11 \cdot \binom{12}{2} \cdot 10 \cdot 10 = 871200$ τρόποι σχηματισμού της επιτροπής.

(2ος τρόπος)

Πρώτα επιλέγουμε τα άτομα που θα συμμετέχουν και έπειτα τους αναθέτουμε ρόλους. Η επιτροπή θα αποτελείται από 3 άνδρες και 3 γυναίκες.

Για τους 3 άνδρες υπάρχουν $\binom{12}{3}$ επιλογές.

Για την εκλογή του άνδρα προέδρου υπάρχουν 3 επιλογές.

Για την εκλογή του άνδρα γραμματέα υπάρχουν 2 επιλογές.

Για τις 3 γυναίκες υπάρχουν $\binom{12}{3}$ επιλογές.

Για την εκλογή των δύο γυναικών αντιπροέδρων υπάρχουν $\binom{3}{2}$ επιλογές.

Άρα, συνολικά, υπάρχουν $\binom{12}{3} \cdot 3 \cdot 2 \cdot \binom{12}{3} \cdot \binom{3}{2} = 871200$ τρόποι σχηματισμού της επιτροπής. □

Άσκηση 3.9. *Να βρεθεί με πόσους τρόπους μπορούν να επιλεγούν, μεταξύ των μελών ενός ομίλου που αποτελείται από 20 μέλη, δύο επιτροπές, η μια εκ των οποίων να αποτελείται από πρόεδρο, αντιπρόεδρο, ταμία και γραμματέα, ενώ η άλλη από 3 μέλη.*

(i) Όταν οι δύο επιτροπές μπορούν να έχουν κοινά μέλη.

(ii) Όταν οι δύο επιτροπές δεν έχουν κοινά μέλη.

(iii) Όταν ο πρόεδρος είναι το μοναδικό κοινό μέλος των δύο επιτροπών.

Λύση.

(i) Για την επιτροπή που έχει πρόεδρο έχουμε τις εξής επιλογές:

Για την εκλογή του προέδρου υπάρχουν 20 επιλογές.

Για την εκλογή του αντιπροέδρου υπάρχουν 19 επιλογές.

Για την εκλογή του ταμία υπάρχουν 18 επιλογές.

Για την εκλογή του γραμματέα υπάρχουν 17 επιλογές.

Άρα, για την σύνθεση αυτής της επιτροπής υπάρχουν $20 \cdot 19 \cdot 18 \cdot 17$ τρόποι.

Για την επιτροπή με τα τρία μέλη υπάρχουν $\binom{20}{3}$ τρόποι επιλογής.

Άρα, συνολικά, για τις δύο επιτροπές υπάρχουν $20 \cdot 19 \cdot 18 \cdot 17 \cdot \binom{20}{3}$ τρόποι σχηματισμού.

(ii) Στην περίπτωση όπου οι δύο επιτροπές δεν έχουν κοινά μέλη, για τον σχηματισμό της επιτροπής που έχει πρόεδρο υπάρχουν $20 \cdot 19 \cdot 18 \cdot 17$ τρόποι. Ενώ, για το σχηματισμό της επιτροπής με τα 3 μέλη υπάρχουν $\binom{16}{3}$ επιλογές.

Άρα, συνολικά, για τις δύο επιτροπές υπάρχουν $20 \cdot 19 \cdot 18 \cdot 17 \cdot \binom{16}{3}$ τρόποι σχηματισμού.

(iii) Στην περίπτωση όπου οι δύο επιτροπές έχουν ως κοινό μέλος τον πρόεδρο, για τον σχηματισμό της επιτροπής που έχει πρόεδρο υπάρχουν $20 \cdot 19 \cdot 18 \cdot 17$ τρόποι. Ενώ, για το σχηματισμό της επιτροπής με τα 3 μέλη υπάρχουν $\binom{16}{2}$ επιλογές (αφού το τρίτο μέλος της είναι ο πρόεδρος της άλλης επιτροπής).

Άρα, συνολικά, για τις δύο επιτροπές υπάρχουν $20 \cdot 19 \cdot 18 \cdot 17 \cdot \binom{16}{2}$ τρόποι σχηματισμού. □

Άσκηση 3.10.

(i) Να βρεθεί ο αριθμός των τρόπων τοποθέτησης 10 *διαφορετικών αντικείμενων* $O_1, O_2, \ldots, O_{10}$ *σε* 3 *διαφορετικά κουτιά* A, B, C.

(ii) Να βρεθεί ο αριθμός των τρόπων τοποθέτησης 10 *όμοιων αντικειμένων σε* 3 *διαφορετικά κουτιά* A, B, C.

(iii) Να βρεθεί ο αριθμός των τρόπων τοποθέτησης 10 *όμοιων αντικειμένων σε* 3 *διαφορετικά κουτιά* A, B, C, *έτσι ώστε κανένα κουτί να μην μείνει άδειο.*

Λύση.

(i) Για κάθε ένα από τα 10 αντικείμενα υπάρχουν 3 διαφορετικές επιλογές. Επομένως, ο ζητούμενος αριθμός είναι ίσος με τον αριθμό των επαναληπτικών διατάξεων των 3 στοιχείων A, B, C ανά 10, δηλαδή ισούται με $U(3, 10) = 3^{10}$.

(ii) Κάθε τοποθέτηση των 10 όμοιων αντικειμένων στα 3 κουτιά A, B, C αντιστοιχεί σε μια μη αρνητική ακέραια λύση της γραμμικής εξίσωσης

$$x_A + x_B + x_C = 10.$$

Επομένως, ο ζητούμενος αριθμός ισούται με $\left[\begin{smallmatrix}3\\10\end{smallmatrix}\right] = \binom{3+10-1}{10} = \binom{12}{10} = 66$.

(iii) Κάθε τοποθέτηση των 10 όμοιων αντικειμένων στα 3 κουτιά A, B, C έτσι ώστε κανένα κουτί να μην μείνει άδειο αντιστοιχεί σε μια ακέραια λύση της γραμμικής εξίσωσης

$$x_A + x_B + x_C = 10,$$

όπου $x_A, x_B, x_C \geq 1$.

Αν τεθεί $y_A = x_A - 1$, $y_B = x_B - 1$, $y_C = x_C - 1$, τότε κάθε λύση της παραπάνω εξίσωσης αντιστοιχεί σε μια μη αρνητική ακέραια λύση της γραμμικής εξίσωσης

$$y_A + y_B + y_C = 7.$$

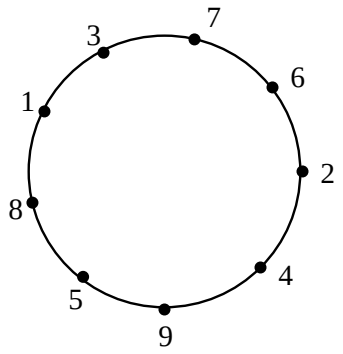
Επομένως, ο ζητούμενος αριθμός ισούται με $\left[\begin{smallmatrix}3\\7\end{smallmatrix}\right] = \binom{3+7-1}{7} = \binom{9}{7} = 36$. □

Άσκηση 3.11. *Πόσες είναι οι μεταθέσεις των γραμμάτων της λέξης :*
Μ Α Θ Η Μ Α Τ Ι Κ Α

Λύση. Το πλήθος των μεταθέσεων των γραμμάτων της δοσμένης λέξης ισούται με τον αριθμό των μεταθέσεων 7 ειδών (όσων δηλαδή είναι τα διαφορετικά γράμματά της) δηλαδή,

$$M(2, 3, 1, 1, 1, 1, 1) = \frac{10!}{2!3!1!1!1!1!1!} = 302400.$$ □

Άσκηση 3.12. *Να βρεθεί με πόσους τρόπους μπορούν να καθίσουν σε ένα στρογγυλό τραπέζι με 9 όμοιες θέσεις 9 άτομα.*



Λύση. Σε κάθε τρόπο τοποθέτησης των 9 ατόμων στο τραπέζι αντιστοιχούν 9 μεταθέσεις του συνόλου [9] προκύπτουν με κυκλική εναλλαγή των στοιχείων τους. Έτσι για παράδειγμα για τον τρόπο τοποθέτησης του παραπάνω σχήματος προκύπτουν οι μεταθέσεις:

$$\begin{array}{lll}(1,3,7,6,2,4,9,5,8), & (3,7,6,2,4,9,5,8,1), & (7,6,2,4,9,5,8,1,3),\\ (6,2,4,9,5,8,1,3,7), & (2,4,9,5,8,1,3,7,6), & (4,9,5,8,1,3,7,6,2),\\ (9,5,8,1,3,7,6,2,4), & (5,8,1,3,7,6,2,4,9), & (8,1,3,7,6,2,4,9,5).\end{array}$$

Αν $\mathcal{K}$ είναι το σύνολο όλων των τρόπων τοποθέτησης των 9 ατόμων στο τραπέζι και $\mathcal{S}$ το σύνολο όλων των μεταθέσεων του [9] τότε ορίζουμε C_i, $i \in \mathcal{K}$, το σύνολο όλων των μεταθέσεων του $\mathcal{S}$ που προκύπτουν από το i. Προφανώς, η οικογένεια $(C_i)_{i\in\mathcal{K}}$ είναι μια διαμέριση του $\mathcal{S}$ και $|C_i| = 9$, για κάθε $i \in \mathcal{K}$. Οπότε προκύπτει ότι :

$$|\mathcal{S}| = \sum_{i\in\mathcal{K}} |C_i| \Leftrightarrow$$

$$9! = \underbrace{9 + 9 + \cdots + 9}_{|\mathcal{K}| \text{ φορές}} \Leftrightarrow$$

$$9! = |\mathcal{K}| \cdot 9 \Rightarrow |\mathcal{K}| = \frac{9!}{9} = 8!.$$ □

Άσκηση 3.13. *Να βρεθεί ο αριθμός των μη αρνητικών ακέραιων λύσεων της ανίσωσης*

$$x_1 + x_2 + x_3 + x_4 < 12.$$

Λύση. Επειδή τα x_i, $i \in [4]$ είναι ακέραιοι ισχύει

$$x_1 + x_2 + x_3 + x_4 < 12 \Leftrightarrow x_1 + x_2 + x_3 + x_4 \leq 11$$

Αν τεθεί

$$x_5 = 11 - x_1 - x_2 - x_3 - x_4$$

τότε $x_5 \geq 0$ και η παραπάνω ανίσωση είναι ισοδύναμη με την εξίσωση

$$x_1 + x_2 + x_3 + x_4 + x_5 = 11$$

Άρα, ο αριθμός των λύσεων της αρχικής ανίσωσης είναι ίσος με τον αριθμό των μη αρνητικών ακέραιων λύσεων της εξίσωσης

$$x_1 + x_2 + x_3 + x_4 + x_5 = 11$$

δηλαδή είναι ίσος με $\left[\begin{smallmatrix}5\\11\end{smallmatrix}\right] = \binom{5+11-1}{11} = \binom{15}{11}$. □

Άσκηση 3.14. *Να βρεθεί ο αριθμός των μη αρνητικών ακέραιων λύσεων της εξίσωσης*

$$x_1 + x_2 + x_3 + 5x_4 = 16.$$

Λύση. Παρατηρούμε ότι για κάθε λύση της εξίσωσης ισχύει ότι $0 \leq x_4 \leq 3$.

Διακρίνουμε περιπτώσεις για την τιμή του x_4.

Αν $x_4 = 0$, ο ζητούμενος αριθμός ισούται με τον αριθμό των μη αρνητικών ακέραιων λύσεων της εξίσωσης

$$x_1 + x_2 + x_3 = 16,$$

δηλαδή είναι ίσος με $\left[\begin{smallmatrix}3\\16\end{smallmatrix}\right] = \binom{18}{16}$.

Αν $x_4 = 1$, ο ζητούμενος αριθμός ισούται με τον αριθμό των μη αρνητικών ακέραιων λύσεων της εξίσωσης

$$x_1 + x_2 + x_3 = 11,$$

δηλαδή είναι ίσος με $\left[\begin{smallmatrix}3\\11\end{smallmatrix}\right] = \binom{13}{11}$.

Αν $x_4 = 2$, ο ζητούμενος αριθμός ισούται με τον αριθμό των μη αρνητικών ακέραιων λύσεων της εξίσωσης

$$x_1 + x_2 + x_3 = 6,$$

δηλαδή είναι ίσος με $\left[\begin{smallmatrix}3\\6\end{smallmatrix}\right] = \binom{8}{6}$.

Τέλος, αν $x_4 = 3$, ο ζητούμενος αριθμός ισούται με τον αριθμό των μη αρνητικών ακέραιων λύσεων της εξίσωσης

$$x_1 + x_2 + x_3 = 1,$$

δηλαδή είναι ίσος με $\left[\begin{smallmatrix}3\\1\end{smallmatrix}\right] = \binom{3}{1}$.

Αρα, ο συνολικός αριθμός των λύσεων της εξίσωσης ισούται με $\binom{18}{2} + \binom{13}{2} + \binom{8}{2} + \binom{3}{2}$. □

Άσκηση 3.15. *Δίνονται $m, n \in \mathbb{N}^*$ και οι ακέραιοι αριθμοί s_i, όπου $i \in [n]$, με*

$$s = s_1 + s_2 + \cdots + s_n \leq m.$$

Να δειχθεί ότι ο αριθμός των ακέραιων (όχι κατ' ανάγκη μη αρνητικών) λύσεων της εξίσωσης

$$x_1 + x_2 + \cdots x_n = m \tag{3.6}$$

με τους περιορισμούς $x_i \geq s_i$ για κάθε $i \in [n]$ ισούται με

$$\binom{n + m - s - 1}{n - 1}.$$

Λύση. Αν $(x_1, x_2, \ldots, x_n)$ είναι μια λύση της (3.6) με $x_i \geq s_i$, για κάθε $i \in [n]$ τότε θέτουμε $y_i = x_i - s_i$ για κάθε $i \in [n]$. Εύκολα προκύπτει ότι $y_i \in \mathbb{N}$ για κάθε $i \in [n]$ και

$$y_1 + y_2 + \cdots + y_n = m - s. \tag{3.7}$$

Αντίστροφα, αν $(x_1, x_2, \ldots, x_n)$ είναι μια μη αρνητική λύση της εξίσωσης (3.7), τότε αν θέσουμε $x_i = y_i + s_i$ για κάθε $i \in [n]$ προκύπτει ότι $x_i \geq s_i$ για κάθε $i \in [n]$ και $(x_1, x_2, \ldots, x_n)$ είναι λύση της εξίσωσης (3.6).

Κατόπιν τούτων προκύπτει ότι υπάρχει μια αμφιμονοσήμαντη απεικόνιση μεταξύ των ακεραίων λύσεων της εξίσωσης (3.6) με $x_i \geq s_i$ για κάθε $i \in [n]$ και των μη αρνητικών λύσεων της εξίσωσης (3.7).

Έτσι, ο ζητούμενος αριθμός θα είναι ίσος με τον αριθμό των μη αρνητικών λύσεων της (3.7), δηλαδή

$$\binom{n+m-s-1}{m-s} = \binom{n+m-s-1}{n-1}. \qquad \square$$

Άσκηση 3.16.

(i) Να δειχθεί ότι ο αριθμός των k-άδων ακεραίων $a_1, a_2, \ldots, a_k$ με

$$1 \leq a_1 < a_2 < \cdots < a_k \leq n$$

ισούται με $\binom{n}{k}$.

Λύση. Κάθε συνδυασμός k αριθμών από το σύνολο $[n]$ αντιστοιχεί σε μια ακριβώς ακολουθία $a_1, a_2, \ldots, a_k$ με $1 \leq a_1 < a_2 < \cdots < a_k \leq n$ και αντιστρόφως. Επομένως, ο αριθμός όλων των ακολουθιών ισούται με $\binom{n}{k}$. $\square$

(ii) Να δειχθεί ότι ο αριθμός των k-άδων ακεραίων $a_1, a_2, \ldots, a_k$ με

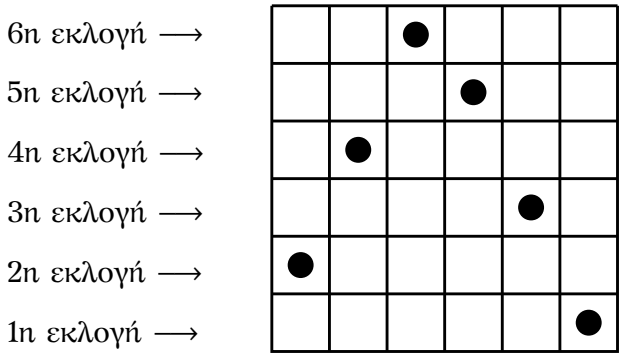
$$1 \leq a_1 \leq a_2 \leq \cdots \leq a_k \leq n$$

ισούται με $\left[\begin{matrix} n \\ k \end{matrix}\right]$.

Λύση. Κάθε επαναληπτικός συνδυασμός k αριθμών από το σύνολο $[n]$ αντιστοιχεί σε μια ακριβώς ακολουθία $a_1, a_2, \ldots, a_k$ με $1 \leq a_1 \leq a_2 < \cdots \leq a_k \leq n$ και αντιστρόφως. Επομένως, ο αριθμός όλων των ακολουθιών ισούται με $\left[\begin{matrix} n \\ k \end{matrix}\right]$. $\square$

Άσκηση 3.17. *Να βρεθεί με πόσους τρόπους μπορούν να τοποθετηθούν 6 πιόνια στα τετράγωνα μιας 6×6 σκακιέρας ώστε να μην υπάρχουν δύο ή περισσότερα πιόνια στην ίδια γραμμή ή στήλη.*

Λύση. (1ος τρόπος)



Το πρώτο πιόνι τοποθετείται στην πρώτη γραμμή με 6 διαφορετικούς τρόπους. Για το δεύτερο πιόνι υπάρχουν 5 διαφορετικοί τρόποι (εξαιρείται το τετράγωνο της δεύτερης γραμμής στην στήλη του οποίου έχουμε βάλει στην πρώτη γραμμή το πρώτο πιόνι). Για το τρίτο πιόνι υπάρχουν 4 διαφορετικοί τρόποι (εξαιρούνται τα τετράγωνα της τρίτης γραμμής στις στήλες των οποίων έχουμε ήδη βάλει τα δυο προηγούμενα πιόνια). Συνεχίζοντας με αυτό τον τρόπο (βλέπε προηγούμενο σχήμα) για το τέταρτο πιόνι υπάρχουν 3 τρόποι, για το πέμπτο 2 τρόποι και για το έκτο ένας μόνο τρόπος τοποθέτησής του.

Έτσι σύμφωνα με την πολλαπλασιαστική αρχή για να τοποθετήσουμε και τα 6 πιόνια στην σκακιέρα θα υπάρχουν

$$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6! = 720 \text{ τρόποι.}$$

(2ος τρόπος) Για το πρώτο πιόνι υπάρχουν 36 τετράγωνα για να τοποθετηθεί. Για το δεύτερο πιόνι υπάρχουν 36-11=25 τετράγωνα για να τοποθετηθεί (αφαιρούνται από τις επιλογές τα 5 τετράγωνα της γραμμής που βρίσκεται το πρώτο πιόνι, τα 5 τετράγωνα της στήλης του πρώτου πιονιού και το 1 τετράγωνο που καταλαμβάνει το πρώτο πιόνι). Για το τρίτο πιόνι υπάρχουν 25-9=16 επιλογές (αφαιρούνται από τις επιλογές τα 4 - και όχι 5 - τετράγωνα της γραμμής που βρίσκεται το δεύτερο πιόνι - αφού ήδη ένα από αυτά τα τετράγωνα έχει αφαιρεθεί προηγουμένως - τα 4 τετράγωνα της γραμμής που βρίσκεται το τρίτο πιόνι και το 1 τετράγωνο που καταλαμβάνει το δεύτερο πιόνι). Συνεχίζοντας με αυτόν τον τρόπο, υπάρχουν 9 τρόποι για το τέταρτο πιόνι, 4 τρόποι για το πέμπτο και 1 τρόπος για το έκτο.

Έτσι σύμφωνα με την πολλαπλασιαστική αρχή υπάρχουν

$$36 \cdot 25 \cdot 16 \cdot 9 \cdot 4 \cdot 1 = (6!)^2$$

τρόποι επιλογής των τετραγώνων τοποθέτησης των έξι πιονιών.

Κατά την εφαρμογή του τρόπου αυτού όμως, κάθε αποτέλεσμα επαναλαμβάνεται πολλές φορές. Αυτό οφείλεται στο γεγονός ότι οποιαδήποτε έξι συγκεκριμένα τετράγωνα καλύπτονται, μπορούν να καλυφθούν με διαφορετική σειρά τοποθέτησης των πιονιών. Δεδομένου ότι η διαδοχική τοποθέτηση των 6 πιονιών γίνεται προφανώς με 6! τρόπους πρέπει να διαιρέσουμε το $(6!)^2$ που ήδη υπολογίσαμε με 6!.

Επομένως, τελικά υπάρχουν

$$\frac{(6!)^2}{6!} = 6!$$

διαφορετικοί τρόποι τοποθέτησης. □

Άσκηση 3.18. *Να βρεθεί με πόσους τρόπους μπορούν να τοποθετηθούν 6 πιόνια στα τετράγωνα μιας 8×10 σκακιέρας ώστε να μην υπάρχουν δύο ή περισσότερα πιόνια στην ίδια γραμμή ή στήλη.*

Λύση. Οι 6 γραμμές στις οποίες θα βρίσκονται τα 6 πιόνια μπορούν να επιλεγούν με $\binom{8}{6}$ τρόπους. Αντίστοιχα, οι 6 στήλες στις οποίες θα βρίσκονται τα 6 πιόνια μπορούν να επιλεγούν με $\binom{10}{6}$ τρόπους. Επομένως, από την πολλαπλασιαστική αρχή, υπάρχουν $\binom{8}{6}\binom{10}{6}$ τρόποι για να επιλέξουμε τις 6 γραμμές και στήλες. Η τομή αυτών των 6 γραμμών και 6 στηλών σχηματίζει μια σκακιέρα 6×6 με 36 τετράγωνα, επομένως ο αριθμός των τρόπων τοποθέτησης των 6 πιονιών σ' αυτή τη σκακιέρα ισούται με 6!. Άρα, τελικά, από την πολλαπλασιαστική αρχή υπάρχουν $\binom{8}{6}\binom{10}{6}6!$ τρόποι τοποθέτησης των 6 πιονιών. □

Άσκηση 3.19. *Να υπολογισθεί ο αριθμός των τρόπων που n ανδρόγυνα μπορούν να καθίσουν στη μία πλευρά ενός τραπεζιού έτσι ώστε σε k καθορισμένα ανδρόγυνα οι σύζυγοι να κάθονται ο ένας δίπλα στον άλλο.*

Λύση. Θεωρούμε ότι κάθε ένα από τα k καθορισμένα ανδρόγυνα είναι ένα αδιαίρετο στοιχείο οπότε το πλήθος των στοιχείων που πρέπει να τοποθετήσουμε στον ευθύγραμμο τραπέζι είναι ίσο με με $2n-k$.

Το πλήθος των ▮ είναι k και το πλήθος των ▮ είναι $2n-2k$.

Επομένως θα υπάρχουν $(2n-k)!$ τρόποι τοποθέτησης. Σε κάθε ένα από αυτούς τους τρόπους τοποθέτησης υπάρχουν δύο επιλογές τοποθέτησης καθενός από τα k καθορισμένα ζευγάρια (δηλαδή ο άνδρας να προηγείται ή να έπεται της γυναίκας). Άρα ο ζητούμενος αριθμός θα είναι ίσος με

$$\underbrace{2\cdot 2\cdots 2}_{k\ \text{φορές}}\,(2n-k)! = 2^k(2n-k)!.$$

□

Άσκηση 3.20. *Να υπολογισθεί ο αριθμός των διαφόρων τρόπων που μπορούν να διαταχθούν σε μια σειρά n αγόρια και k κορίτσια, $k\le n+1$, έτσι ώστε να μην υπάρχουν δυο κορίτσια που να βρίσκονται το ένα δίπλα στο άλλο.*

Λύση. Καταρχήν διατάσσουμε τα αγόρια. Ο αριθμός των διατάξεων των αγοριών είναι ίσος με με τον αριθμό των μεταθέσεων των n αγοριών δηλαδή $n!$.

Για κάθε μετάθεση $(a_1,a_2,\ldots,a_n)$ του συνόλου των αγοριών υπάρχουν $n+1$ επιτρεπτές θέσεις για τα κορίτσια. Έτσι ο αριθμός των τρόπων που μπορούν να τοποθετηθούν τα k κορίτσια, για τη μετάθεση αυτή των αγοριών, ισούται με τον αριθμό των διατάξεων των $n+1$ ανά k δηλαδή $P(n+1,k)$.

Άρα, σύμφωνα με την πολλαπλασιαστική αρχή ο ζητούμενος αριθμός θα είναι ίσος με

$$n!P(n+1,k) = \frac{n!(n+1)!}{(n+1-k)!}.$$

□

Άσκηση 3.21. *Έστω a_n το πλήθος των λέξεων μήκους n που κατασκευάζονται από τα ψηφία $\{0,1,2,3\}$ και οι οποίες περιέχουν άρτιο αριθμό εμφανίσεων του 0. Να δειχθεί ότι $a_{n+1} = 2a_n + 4^n$.*

Λύση. Οι λέξεις μήκους n που κατασκευάζονται από τα ψηφία $\{0,1,2,3\}$ είναι 4^n.

Από αυτές, ονομάζουμε *έγκυρες* τις λέξεις που έχουν άρτιο αριθμό εμφανίσεων 0. Επομένως, ο αριθμός των έγκυρων λέξεων μήκους n ισούται με a_n και ο αριθμός των μή έγκυρων λέξεων μήκους n ισούται με $4^n - a_n$.

Έστω μια έγκυρη λέξη μήκους $n+1$. Η λέξη αρχίζει είτε με 0, είτε με $1,2,3$.

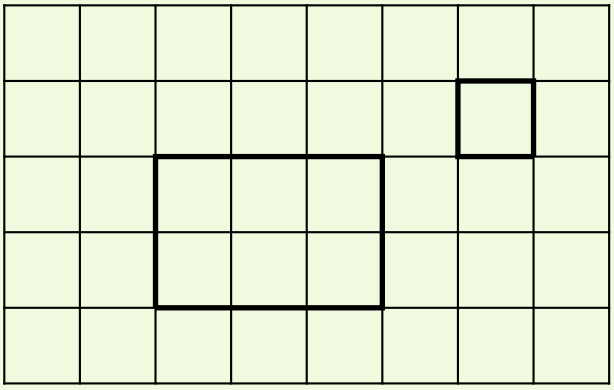
Στην πρώτη περίπτωση, τα υπόλοιπα n στοιχεία της λέξης αποτελούν μια μη έγκυρη λέξη μήκους n, άρα υπάρχουν $1 \cdot (4^n - a_n)$ έγκυρες λέξεις μήκους $n+1$ που αρχίζουν με 0.

Στις υπόλοιπες περιπτώσεις, τα υπόλοιπα n στοιχεία της λέξης αποτελούν μια έγκυρη λέξη μήκους n, άρα υπάρχουν $3 \cdot a_n$ έγκυρες λέξεις μήκους $n+1$ που αρχίζουν με 1, ή 2, ή 3.

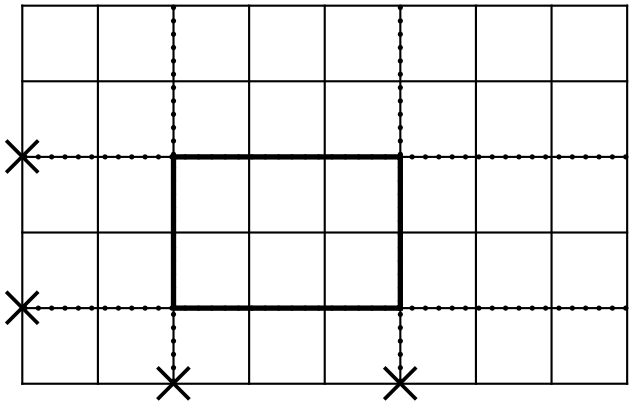
Άρα, από τον κανόνα του αθροίσματος ισχύει ότι

$$a_{n+1} = 1 \cdot (4^n - a_n) + 3 \cdot a_n = 2a_n + 4^n. \qquad \square$$

Άσκηση 3.22. *Να βρεθεί ο αριθμός των ορθογωνίων με κορυφές τα σημεία και πλευρές τα ευθύγραμμα τμήματα μιας $n \times m$ σκακιέρας.*



Λύση. Κάθε ορθογώνιο προσδιορίζεται μονοσήμαντα επιλέγοντας 2 σημεία στην κάτω πλευρά της σκακιέρας και 2 σημεία στην αριστερή πλευρά της σκακιέρας.



Υπάρχουν $\binom{m+1}{2}$ τρόποι για να επιλέξουμε 2 σημεία στη κάτω πλευρά.

Υπάρχουν $\binom{n+1}{2}$ τρόποι για να επιλέξουμε 2 σημεία στην αριστερή πλευρά.

Από την πολλαπλασιαστική αρχή υπάρχουν $\binom{m+1}{2}\binom{n+1}{2}$ επιλογές. $\square$

Άσκηση 3.23.

i) Έστω w μια k-αδική λέξη μήκους n (δηλαδή μια λέξη που τα ψηφία της μπορούν να λαμβάνουν k διαφορετικές τιμές). Να δειχθεί ότι ο αριθμός των k-αδικών λέξεων μήκους n που διαφέρουν από τη w το πολύ σε d θέσεις ισούται με $\sum_{j=0}^{d} \binom{n}{j}(k-1)^j$.

ii) Να βρεθεί ο αριθμός των 3-αδικών λέξεων μήκους 3 με ψηφία $\{0,1,2\}$ οι οποίες διαφέρουν το πολύ σε 2 θέσεις από τη λέξη $w = 011$.

Λύση.

i) Οι k-αδικές λέξεις που διαφέρουν από την w το πολύ σε d θέσεις διαμερίζονται σε $d+1$ σύνολα με βάση τον ακριβή αριθμό j των θέσεων στις οποίες διαφέρουν. Οι δυνατές τιμές του j είναι 0, 1, 2, …, $d-1$, d.

Το πλήθος των λέξεων u οι οποίες διαφέρουν σε ακριβώς j θέσεις με την w υπολογίζεται ως εξής:

Υπάρχουν $\binom{n}{j}$ διαφορετικές j-άδες θέσεων στις οποίες n u μπορεί να διαφέρει από την w.

Επίσης, σε κάθε μια από αυτές τις j θέσεις της u πρέπει να βρίσκεται διαφορετικό στοιχείο από αυτό που υπάρχει στην αντίστοιχη θέση στη w, οπότε υπάρχουν $k-1$ επιλογές για το αντίστοιχο ψηφίο. Επομένως, συνολικά για τις j θέσεις υπάρχουν $(k-1)^j$ επιλογές.

Για τις υπόλοιπες $n-j$ θέσεις της u υπάρχει μόνο μια επιλογή, αφού σε αυτές οι λέξεις u και w δεν διαφέρουν.

Άρα, από την πολλαπλασιαστική αρχή, υπάρχουν $\binom{n}{j}(k-1)^j$ λέξεις που διαφέρουν ακριβώς σε j θέσεις με την w.

Συνολικά, αθροίζοντας όλες τις περιπτώσεις, υπάρχουν $\sum_{j=0}^{d} \binom{n}{j}(k-1)^j$ λέξεις που διαφέρουν το πολύ σε d θέσεις με την w.

ii) Ο ζητούμενος αριθμός ισούται με

$$\sum_{j=0}^{2} \binom{3}{j} 2^j = \binom{3}{0} \cdot 2^0 + \binom{3}{1} \cdot 2^1 + \binom{3}{2} \cdot 2^2 = 1 + 6 + 12 = 19.$$

Δηλαδή, υπάρχουν 19 τριαδικές λέξεις που διαφέρουν το πολύ σε 2 θέσεις από τη λέξη 011. Πράγματι,

Λέξεις που διαφέρουν από την 011 σε 0 θέσεις: 011.

Λέξεις που διαφέρουν από την 011 σε 1 θέση: 111, 211, 001, 021, 010, 012,

Λέξεις που διαφέρουν από την 011 σε 2 θέσεις: 101, 121, 201, 221, 110, 112, 210, 212, 000, 002, 020, 022. □

Άσκηση 3.24. *Να δειχθεί ότι ο αριθμός των τρόπων διαμέρισης n διαφορετικών ατόμων σε k διαφορετικές ομάδες με $n_1, n_2, \ldots, n_k$ μέλη αντίστοιχα είναι ίσος με* $\dfrac{n!}{n_1!n_2!\cdots n_k!}$.

Λύση. Για την πρώτη ομάδα υπάρχουν $\binom{n}{n_1}$ επιλογές, για την δεύτερη ομάδα υπάρχουν $\binom{n-n_1}{n_2}$ επιλογές, για την τρίτη ομάδα υπάρχουν $\binom{n-n_1-n_2}{n_3}$ επιλογές, κ.ο.κ, για την k-οστή ομάδα υπάρχουν $\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}$ επιλογές. Άρα, το πλήθος των τρόπων διαμέρισης ισούται με

$$\begin{aligned}
&\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_k}{n_k}\\
&= \frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!}\cdots\frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!(n-n_1-n_2-\cdots-n_k)!}\\
&= \frac{n!}{n_1!n_2!\cdots n_k!}.
\end{aligned}$$

□

Άσκηση 3.25. *Να βρεθεί η τιμή της μεταβλητής m μετά την εκτέλεση του επόμενου τμήματος κώδικα.*

```
m = 0;
for(i=1; i<=10; i++){
  for(j=1; j<=i; j++){
    for(k=1; k<=j; k++){
      m++;
    }
  }
}
```

Λύση. Η εντολή m++ εκτελείται για τα i, j, k για τα οποία ισχύουν οι ανισότητες $1 \le k \le j \le i \le 10$. Κάθε τριάδα (i, j, k) με αυτές τις ιδιότητες αντιστοιχεί σε ένα επαναληπτικό συνδυασμό των 10 στοιχείων ανά 3 (γιατί;). Επομένως, η εντολή m++ εκτελείται $\left[\binom{10}{3}\right] = \binom{10+3-1}{3} = \binom{12}{3}$ φορές, δηλαδή η m θα έχει την τιμή $m = 220$. □

Άσκηση 3.26. *Να υπολογισθεί το άθροισμα*

$$S_n = \sum_{i=s}^{k}(-1)^i\binom{n}{i}$$

όπου $n \in \mathbb{N}^*$, και $k, s \in \mathbb{N}^*$ με $s \le k$.

Λύση. Χρησιμοποιώντας το τρίγωνο του Pascal για κάθε $i = s, s+1, \ldots, k$ προκύπτουν οι σχέσεις:

$$\begin{aligned}
(-1)^s\binom{n}{s} &= (-1)^s\binom{n-1}{s} + (-1)^s\binom{n-1}{s-1}\\
(-1)^{s+1}\binom{n}{s+1} &= (-1)^{s+1}\binom{n-1}{s+1} + (-1)^{s+1}\binom{n-1}{s}\\
(-1)^{s+2}\binom{n}{s+2} &= (-1)^{s+2}\binom{n-1}{s+2} + (-1)^{s+2}\binom{n-1}{s+1}\\
&\vdots\\
(-1)^{k-2}\binom{n}{k-2} &= (-1)^{k-2}\binom{n-1}{k-2} + (-1)^{k-2}\binom{n-1}{k-3}\\
(-1)^{k-1}\binom{n}{k-1} &= (-1)^{k-1}\binom{n-1}{k-1} + (-1)^{k-1}\binom{n-1}{k-2}\\
(-1)^{k}\binom{n}{k} &= (-1)^{k}\binom{n-1}{k} + (-1)^{k}\binom{n-1}{k-1}.
\end{aligned}$$

Προσθέτοντας κατά μέλη τις παραπάνω ισότητες προκύπτει ότι

$$S_n = (-1)^s\binom{n-1}{s-1} + (-1)^k\binom{n-1}{k}.$$ □

Παρατήρηση. Στις επόμενες ασκήσεις οι λύσεις δίδονται χρησιμοποιώντας συνδυαστικές αποδείξεις. Για συντομία, θα χρησιμοποιήσουμε την εξής ορολογία: Ένα πεπερασμένο σύνολο (αντ. υποσύνολο) με k στοιχεία θα ονομάζεται και k-σύνολο (αντ. k-υποσύνολο).

Άσκηση 3.27. *Να δειχθεί ότι οι αριθμοί* $\dfrac{(4n)!}{(3n)!n!}$ *και* $\dfrac{(4n)!}{2^{3n}3^n}$ *είναι ακέραιοι.*

Λύση. Ο αριθμός των τρόπων διάταξης του αντικειμένου A το οποίο εμφανίζεται $3n$ φορές και του αντικειμένου B το οποίο εμφανίζεται n φορές, ισούται με τον αριθμό των μεταθέσεων 2 ειδών στοιχείων με $3n$ και n στοιχεία αντίστοιχα, δηλαδή είναι ίσος με $\dfrac{(3n+n)!}{(3n)!n!} = \dfrac{(4n)!}{(3n)!n!}$. Επομένως, ο πρώτος αριθμός είναι ακέραιος αφού μετράει μεταθέσεις αντικειμένων.

Ο αριθμός των τρόπων διάταξης των αντικειμένων A_1, A_2, …, A_n, τα οποία εμφανίζονται 4 φορές το καθένα ισούται με τον αριθμό των μεταθέσεων n ειδών στοιχείων με 4, 4, …, 4 στοιχεία αντίστοιχα, δηλαδή είναι ίσος με $\dfrac{(4+4+\cdots+4)!}{4!4!\cdots4!} = \dfrac{(4n)!}{(4!)^n} = \dfrac{(4n)!}{4^n3^n2^n} = \dfrac{(4n)!}{2^{2n}3^n2^n} = \dfrac{(4n)!}{2^{3n}3^n}$. Επομένως, ο δεύτερος αριθμός είναι ακέραιος αφού μετράει μεταθέσεις αντικειμένων. □

Άσκηση 3.28. *Να δοθεί μια συνδυαστική απόδειξη της ταυτότητας* $\binom{2n}{2} = 2\binom{n}{2} + n^2$.

Λύση. Έστω n ανδρόγυνα από τα οποία θέλουμε να επιλέξουμε 2 άτομα.

Ο αριθμός των διαφορετικών τρόπων επιλογής των 2 ατόμων ισούται με τον αριθμό των συνδυασμών $2n$ στοιχείων ανά 2, δηλαδή είναι ίσος με $\binom{2n}{2}$.

Μπορούμε να υπολογίσουμε τον ίδιο αριθμό διακρίνοντας δύο περιπτώσεις ως προς το φύλο των ατόμων που επιλέγονται.

(i) Τα 2 άτομα είναι του ιδίου φύλου. Τότε υπάρχουν 2 επιλογές για το φύλο και έπειτα $\binom{n}{2}$ επιλογές για τα δύο άτομα του ιδίου φύλου. Άρα, από τον κανόνα του γινομένου υπάρχουν $2\binom{n}{2}$ τρόποι επιλογής τους.

(ii) Τα 2 άτομα είναι διαφορετικού φύλου. Τότε υπάρχουν $\binom{n}{1} = n$ τρόποι να επιλέξουμε μια γυναίκα και $\binom{n}{1} = n$ τρόποι να επιλέξουμε έναν άνδρα. Άρα, από τον κανόνα του γινομένου υπάρχουν n^2 τρόποι επιλογής τους.

Άρα, συνολικά, υπάρχουν $2\binom{n}{2} + n^2$ τρόποι επιλογής των 2 ατόμων.

Επειδή, τόσο με τον πρώτο όσο και με τον δεύτερο τρόπο μετράμε τους ίδιους τρόπους επιλογής, έπεται ότι $\binom{2n}{2} = 2\binom{n}{2} + n^2$. □

Άσκηση 3.29. *Έστω E ένα σύνολο με n στοιχεία.*

(i) Να δειχθεί ότι ο αριθμός των k-υποσυνόλων του E ισούται με $\binom{n}{k}$.

(ii) Να δειχθεί ότι ο αριθμός των k-υποσυνόλων του E ισούται με τον αριθμό των $(n-k)$-υποσυνόλων του E.

(iii) Να δειχθεί ότι $\binom{n}{k} = \binom{n}{n-k}$, για κάθε $n, k \in \mathbb{N}$.

Λύση. Κάθε υποσύνολο A του E προσδιορίζεται μονοσήμαντα από τα στοιχεία του.

(i) Αν $|A| = k$ τότε το k-υποσύνολο A προσδιορίζεται μονοσήμαντα από τα k στοιχεία του. Υπάρχουν $\binom{n}{k}$ διαφορετικοί τρόποι να επιλέξουμε k στοιχεία από τα n στοιχεία. Άρα, υπάρχουν $\binom{n}{k}$ διαφορετικά k-υποσύνολα του E.

(ii) Αν A είναι k-υποσύνολο του E τότε το σύνολο $E \setminus A$ (δηλαδή το συμπλήρωμα του A) είναι $(n-k)$-υποσύνολο του E. Αντιστρόφως, αν B είναι $(n-k)$-υποσύνολο του E τότε το σύνολο $E \setminus B$ είναι k-υποσύνολο του E. Επιπλέον, αν $B = X \setminus A$ τότε $X \setminus B = A$.

Επομένως, σε κάθε k-υποσύνολο του E αντιστοιχεί ένα και μοναδικό $(n-k)$-υποσύνολο του E και αντιστρόφως, άρα ο αριθμός των k-υποσυνόλων του E ισούται με τον αριθμό των $(n-k)$-υποσυνόλων του E.

(iii) Από το ερώτημα (i) προκύπτει ότι $\binom{n}{k}$ είναι ο αριθμός των k-υποσυνόλων του E, ενώ $\binom{n}{n-k}$ είναι ο αριθμός των $(n-k)$-υποσυνόλων του E. Από το ερώτημα (ii) έπεται ότι οι δύο αριθμοί είναι ίσοι. □

Άσκηση 3.30.

(i) Να δειχθεί ότι ο αριθμός των δυαδικών λέξεων μήκους n ισούται με 2^n.

(ii) Να δειχθεί ότι ο αριθμός των δυαδικών λέξεων μήκους n που περιέχουν ακριβώς k άσσους ισούται με $\binom{n}{k}$.

(iii) Να δειχθεί ότι ο αριθμός των δυαδικών λέξεων μήκους n που περιέχουν ακριβώς k άσσους ισούται με τον αριθμό των δυαδικών λέξεων μήκους n που περιέχουν ακριβώς $n-k$ άσσους.

(iv) Να δειχθεί ότι $\binom{n}{k} = \binom{n}{n-k}$, για κάθε $n, k \in \mathbb{N}$.

(v) Να δειχθεί ότι $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

Λύση.

(i) Κάθε δυαδική λέξη μήκους n προσδιορίζεται μοναδικά από τα n ψηφία της. Για κάθε ψηφίο υπάρχουν 2 επιλογές (0 ή 1), επομένως από τον κανόνα του γινομένου για τα n ψηφία υπάρχουν $\underbrace{2 \cdot 2 \cdots 2}_{n \text{ φορές}} = 2^n$ διαφορετικές επιλογές.

(ii) Παρατηρούμε ότι κάθε δυαδική λέξη μήκους n με ακριβώς k άσσους προσδιορίζεται μοναδικά αν γνωρίζουμε τις θέσεις των k άσσων της (αφού στις υπόλοιπες $n-k$ θέσεις τα ψηφία θα είναι υποχρεωτικά 0). Υπάρχουν $\binom{n}{k}$ διαφορετικοί τρόποι να επιλέξουμε τις k θέσεις των άσσων σε μια λέξη, άρα υπάρχουν $\binom{n}{k}$ διαφορετικές δυαδικές λέξεις μήκους n με k άσσους.

(iii) Αν w είναι μια δυαδική λέξη μήκους n με k άσσους (και $n-k$ μηδενικά) τότε το συμπλήρωμα της w (δηλαδή η δυαδική λέξη που προκύπτει αν αλλάξουμε κάθε μηδενικό ψηφίο της w σε άσσο και κάθε άσσο σε μηδέν) είναι μια δυαδική λέξη w' μήκους n με $n-k$ άσσους (και k μηδενικά). Αντίστροφα, αν v είναι μια δυαδική λέξη μήκους n με $n-k$ άσσους (και k μηδενικά) τότε το συμπλήρωμα της v είναι μια δυαδική λέξη v' μήκους n με k άσσους (και $n-k$ μηδενικά). Επιπλέον, το συμπλήρωμα της w' είναι η λέξη w.

Επομένως, σε κάθε δυαδική λέξη μήκους n με k άσσους αντιστοιχεί μια και μοναδική δυαδική λέξη μήκους n με $n-k$ άσσους και αντιστρόφως, άρα ο αριθμός των δυαδικών λέξεων μήκους n με k άσσους ισούται με τον αριθμό των δυαδικών λέξεων μήκους n με $n-k$ άσσους.

(iv) Από το ερώτημα (ii) προκύπτει ότι $\binom{n}{k}$ είναι ο αριθμός των δυαδικών λέξεων μήκους n με k άσσους, ενώ $\binom{n}{n-k}$ είναι ο αριθμός των δυαδικών λέξεων μήκους n με $n-k$ άσσους, Από το ερώτημα (iii) έπεται ότι οι δύο αριθμοί είναι ίσοι.

(v) Το σύνολο B_n όλων των δυαδικών λέξεων μήκους n διαμερίζεται σε $n+1$ υποσύνολα με βάση τον αριθμό των άσσων που περιέχονται σε κάθε δυαδική λέξη.

Αν συμβολίσουμε με $B_{n,k}$ το σύνολο των δυαδικών λέξεων μήκους n με ακριβώς k άσσους, τότε τα $n+1$ σύνολα $B_{n,0}$, $B_{n,1}$, $B_{n,2}$, …, $B_{n,n}$ αποτελούν διαμέριση του B_n και όπως είδαμε στα ερωτήματα (i) και (ii) ισχύει ότι $|B_n| = 2^n$ και $|B_{n,k}| = \binom{n}{k}$ για κάθε $k = 0, 1, 2, \ldots, n$.

Από την ισότητα $B_n = B_{n,0} \cup B_{n,1} \cup B_{n,2} \cup \cdots \cup B_{n,n}$ και δεδομένου ότι τα $B_{n,0}$, …, $B_{n,n}$ είναι ανά δύο ξένα, έπεται ότι

$$|B_n| = |B_{n,0}| + |B_{n,1}| + \cdots + |B_{n,n}|$$

ή, ισοδύναμα

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

□

Άσκηση 3.31. *Έστω E ένα σύνολο με n στοιχεία.*

(i) Να δειχθεί ότι ο αριθμός των υποσυνόλων του E ισούται με 2^n.

(ii) Να δειχθεί ότι $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

(iii) Να δειχθεί ότι $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ για κάθε $n, k \in \mathbb{N}^*$.

Λύση.

(i) (1ος τρόπος) Κάθε υποσύνολο A του E καθορίζεται από τα στοιχεία του. Ένα στοιχείο x του E είτε ανήκει στο A είτε δεν ανήκει στο A. Άρα, για κάθε στοιχείο x του E, υπάρχουν 2 επιλογές που καθορίζουν ένα διαφορετικό υποσύνολο A. Από τον κανόνα του γινομένου για τα n στοιχεία του E υπάρχουν $\underbrace{2 \cdot 2 \cdots 2}_{n \text{ φορές}} = 2^n$ διαφορετικές επιλογές, άρα 2^n διαφορετικά υποσύνολα του E.

(2ος τρόπος) Αν θεωρήσουμε μια αρίθμηση στα στοιχεία του E, τότε σε κάθε υποσύνολο A του E μπορούμε να αντιστοιχίσουμε μια δυαδική λέξη $w = w_1 w_2 \cdots w_n$ μήκους n ως εξής: Το i-οστό ψηφίο της λέξης w (δηλαδή το w_i) ισούται με 1 αν το i-οστό στοιχείο του E (με την παραπάνω αρίθμηση) ανήκει στο σύνολο A και $w_i = 0$ αν το i-οστό στοιχείο του E δεν ανήκει στο σύνολο A. Προφανώς σε κάθε υποσύνολο A ανήκει μια μοναδική δυαδική λέξη w μήκους n. Αντίστροφα, σε κάθε δυαδική λέξη μήκους n αντιστοιχεί ένα και μοναδικό υποσύνολο του E. Όπως είδαμε σε προηγούμενη άσκηση, ο αριθμός των δυαδικών λέξεων μήκους n ισούται με 2^n, από όπου προκύπτει το ζητούμενο.

(ii) Το δυναμοσύνολο του E διαμερίζεται σε $n+1$ υποσύνολα με βάση τον αριθμό των στοιχείων που περιέχονται σε κάθε υποσυνόλο του E.

Πιο συγκεκριμένα, το δυναμοσύνολο $\mathcal{P}(E)$ του E είναι ένωση όλων των k-υποσυνόλων του E για $k = 0, 1, 2, \ldots, n$. Όπως είδαμε, ο αριθμός των k υποσυνόλων του E ισούται με $\binom{n}{k}$, ενώ $|\mathcal{P}(E)| = 2^n$. Επειδή τα σύνολα των k-υποσυνόλων του E για $k = 0, 1, \ldots, n$ αποτελούν διαμέριση του $\mathcal{P}(E)$, έπεται ότι $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

(iii) Όπως δείξαμε στην άσκηση 3.29, ο αριθμός των k-υποσυνόλων του E ισούται με $\binom{n}{k}$.

Έστω x ένα στοιχείο του E. Υπάρχουν δύο περιπτώσεις για το x όσον αφορά τα k-υποσύνολα του E: Είτε το x θα ανήκει σε ένα k-υποσύνολο του E, είτε το x δεν θα ανήκει σε ένα k-υποσύνολο του E.

Τα k-υποσύνολα του E που περιέχουν το x, καθορίζονται από τα $k-1$ επιπλέον στοιχεία που επιλέγονται από το σύνολο $E \setminus \{x\}$, δηλαδή με $\binom{n-1}{k-1}$ τρόπους.

Εξάλλου, τα k-υποσύνολα του E που δεν περιέχουν το x, καθορίζονται από τα k στοιχεία που επιλέγονται από το σύνολο $E \setminus \{x\}$, δηλαδή με $\binom{n-1}{k}$ τρόπους.

Επομένως, αφού τα δύο προηγούμενα σύνολα k-υποσύνολων αποτελούν διαμέριση των k-υποσυνόλων του E, έπεται ότι $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. □

3.6 Ασκήσεις προς επίλυση

1. Να βρεθεί ο μέγιστος αριθμός των διαφορετικών ελληνικών πινακίδων των ιδιωτικών αυτοκινήτων όταν είναι γνωστό ότι σχηματίζονται από τρία γραμματα από το σύνολο

$$\{A, B, E, Z, H, I, K, M, N, O, P, T, Y, X\}$$

(με δυνατότητα επαναλήψεων) ακολουθούμενα από 4 ψηφία τα οποία σχηματίζουν τετραψήφιο αριθμό.

Ποιος θα ήταν ο μέγιστος αριθμός αν χρησιμοποιούνταν μόνο 2 γράμματα αντί για 3;

Ποιος θα ήταν ο μέγιστος αριθμός αν δεν επιτρεπόταν να χρησιμοποιηθούν ταυτόχρονα το γράμμα Ο και το ψηφίο 0;

2. Πόσους πενταψήφιους αριθμούς μπορούμε να κατασκευάσουμε με τα ψηφία $1, 2, 3, 4, 5, 6, 7, 8, 9$

   (i) αν πρέπει να έχουν τα ψηφία τους διαφορετικά,

   (ii) αν τα ψηφία τους μπορεί να επαναλαμβάνονται,

   (iii) αν δεν περιέχουν δύο ίδια ψηφία σε διαδοχικές θέσεις,

   (iv) αν πρέπει να είναι άρτιοι αριθμοί και τα ψηφία τους να είναι διαφορετικά,

   (v) αν τα δύο πρώτα ψηφία τους είναι άρτια και τα δύο τελευταία ψηφία τους περιττά,

   (vi) αν το άθροισμα του πρώτου και του τελευταίου ψηφίου τους είναι ίσο με 4 και τα ψηφία τους μπορούν να επαναλαμβάνονται,

   (vii) αν το άθροισμα του πρώτου και του δεύτερου ψηφίου τους είναι ίσο με 8 και τα ψηφία τους είναι διαφορετικά,

   (viii) αν πρέπει να είναι περιττοί και το πρώτο και το τρίτο ψηφίο τους είναι ίσα,

   (ix) αν διαβάζονται το ίδιο από τα αριστερά προς τα δεξιά και από τα δεξιά προς τα αριστερά,

   (x) αν τα ψηφία τους είναι σε γνησίως αύξουσα σειρά (δηλαδή, το πρώτο μικρότερο του δευτέρου, το δεύτερο του τρίτου και το τρίτο του τέταρτου),

   (xi) αν το άθροισμα του πρώτου και του δεύτερου ψηφίου τους είναι ίσο με το τρίτο ψηφίο τους και τα ψηφία τους είναι διαφορετικά,

   (xii) αν περιέχουν ακριβώς μια φορά το ψηφίο 7,

   (xiii) αν περιέχουν τουλάχιστον δύο ίδια ψηφία.

3. Σε ένα κώδικα χρησιμοποιούνται δεκαεξαδικές λέξεις (δηλαδή λέξεις που σχηματίζονται από τα ψηφία 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) μήκους n.

   Να βρεθεί η ελάχιστη τιμή του n όταν ο κώδικας πρέπει

   (i) να περιέχει τουλάχιστον 10^6 διαφορετικές λέξεις,

   (ii) να περιέχει τουλάχιστον m διαφορετικές λέξεις,

   (iii) να περιέχει τουλάχιστον 10^6 διαφορετικές λέξεις, οι οποίες διαβάζονται το ίδιο από αριστερά προς τα δεξιά και από τα δεξιά προς τα αριστερά,

   (iv) να περιέχει τουλάχιστον m διαφορετικές λέξεις, οι οποίες διαβάζονται το ίδιο από αριστερά προς τα δεξιά και από τα δεξιά προς τα αριστερά.

4. Να δειχθεί ότι το συνολικό πλήθος των θετικών φυσικών αριθμών που δεν έχουν επαναλήψεις στα ψηφία τους είναι ίσο με 8877690.

5. Πόσες λέξεις μπορούν να κατασκευασθούν χρησιμοποιώντας όλα τα γράμματα της λέξης Ε Φ Α Ρ Μ Ο Γ Η και πόσες από αυτές έχουν τα γράμματα Α και Ρ διαδοχικά; Σε πόσες από αυτές περιέχονται ακριβώς δύο άλλα γράμματα μεταξύ των Α και Ρ;

6. Να βρεθεί ο αριθμός των τρόπων που μπορούμε να διατάξουμε τους αριθμούς $1, 2, 3, \ldots, 24$ έτσι ώστε να υπάρχουν ακριβώς 7 αριθμοί μεταξύ των 1 και 2.

7. Να δειχθεί ότι ο αριθμός των δυαδικών λέξεων μήκους n με άρτιο αριθμό άσσων ισούται με 2^{n-1}, για κάθε $n \geq 1$.

8. Πόσες είναι οι μεταθέσεις των γραμμάτων των παρακάτω λέξεων

   (i) Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Υ Π Ο Λ Η

   (ii) Σ Ι Δ Η Ρ Ο Δ Ρ Ο Μ Ο Σ

9. (i) Με πόσους τρόπους μπορούμε να διατάξουμε δύο A, τέσσερα B και τρία C στη σειρά έτσι ώστε τα δύο A να είναι διαδοχικά;

   (ii) Με πόσους τρόπους μπορούμε να διατάξουμε δέκα A, έξι B και πέντε C στη σειρά έτσι ώστε να μην υπάρχουν δύο B σε διαδοχικές θέσεις;

10. Κατά πόσους τρόπους μπορούν να διαταχθούν 4 λευκές, 5 κίτρινες και 9 μαύρες μπάλες

    (i) χωρίς περιορισμό,

    (ii) αν κάθε διάταξή τους αρχίζει με λευκή και τελειώνει με μαύρη μπάλα,

    (iii) αν δεν επιτρέπεται δύο λευκές μπάλες να είναι διαδοχικές,

    (iv) αν οι μπάλες με το ίδιο χρώμα είναι όλες διαδοχικές.

11. Με πόσους τρόπους μπορούν να καθίσουν σε μια πλευρά ενός τραπεζιού n ανδρόγυνα όταν

    (i) δεν υπάρχουν άλλοι περιορισμοί,

    (ii) οι άνδρες και οι γυναίκες πρέπει να κάθονται εναλλάξ,

    $*$(iii) δεν υπάρχουν ανδρόγυνα που ο άνδρας κάθεται δίπλα στη γυναίκα του.

12. Να βρεθεί με πόσους τρόπους μπορούν να καθίσουν σε μια πλευρά ενός τραπεζιού 4 ποδοσφαιριστές, 3 κολυμβητές και 5 σκιέρ έτσι ώστε τα άτομα του ίδιου αθλήματος να κάθονται το ένα πλάϊ στο άλλο.

13. Να βρεθεί με πόσους τρόπους μπορούν να τοποθετηθούν k πιόνια στα τετράγωνα μιας $m \times n$ σκακιέρας ώστε να μην υπάρχουν δύο ή περισσότερα πιόνια στην ίδια γραμμή ή στήλη.

14. Να βρεθεί με πόσους τρόπους μπορούν να τοποθετηθούν ο λευκός και ο μαύρος βασιλιάς στα τετράγωνα μιας 8×8 σκακιέρας ώστε

    (i) ο ένας να απειλεί τον άλλο,

    (ii) ο ένας να μην απειλεί τον άλλο.

    Ποια είναι η απάντηση στα ίδια ερωτήματα αν και οι δύο βασιλιάδες έχουν το ίδιο χρώμα;

15. Να βρεθεί ο αριθμός των διαδοχικών μηδενικών που εμφανίζονται στο τέλος των αριθμών:
α) 24! β) 30! γ) 40! δ) 50! ε) 129!.

16. Να βρεθεί ο αριθμός των τρόπων τοποθέτησης n διαφορετικών αντικειμένων σε k διαφορετικά κουτιά, έτσι ώστε κάθε κουτί να περιέχει το πολύ ένα αντικείμενο.

17. Με πόσους τρόπους μπορούν να χωρισθούν 20 φοιτητές σε 3 ομάδες

(i) των 10, 6 και 4 ατόμων αντίστοιχα;

(ii) των 10, 5 και 5 ατόμων αντίστοιχα;

(iii) των 10, 5 και 5 ατόμων αν τα ονόματα των ομάδων είναι ΚΟΚΚΙΝΟΙ, ΠΡΑΣΙΝΟΙ και ΚΙΤΡΙΝΟΙ αντίστοίχα;

18. Από 21 καθηγητές, εκ των οποίων 8 είναι μαθηματικοί, 6 φυσικοί και 7 χημικοί θέλουμε να σχηματίσουμε μια επιτροπή από 5 καθηγητές στους οποίους τουλάχιστον ένας πρέπει να είναι φυσικός, για να πάρουν μέρος σε ένα συνέδριο. Πόσες επιτροπές μπορούν να σχηματισθούν;

19. Ένα δημοτικό συμβούλιο διοικείται από δύο παρατάξεις A και B. Η παράταξη A εκπροσωπείται με 12 μέλη εκ των οποίων 3 είναι γυναίκες και η παράταξη B εκπροσωπείται με 13 μέλη εκ των οποίων 5 είναι γυναίκες. Να βρεθεί με πόσους τρόπους μπορεί να σχηματισθεί μια οκταμελής επιτροπή στην οποία να συμμετέχουν ίσος αριθμός ανδρών και γυναικών και ίσος αριθμός μελών και από τις δύο παρατάξεις.

20. Να βρεθεί ο αριθμός των τρόπων επιλογής δύο διαφορετικών αριθμών από το σύνολο [100] έτσι ώστε το άθροισμά τους να είναι

(i) άρτιος,

(ii) περιττός,

(iii) πολλαπλάσιο του 3.

21. Να βρεθεί με πόσους τρόπους μπορεί να επιλεγεί μια διατεταγμένη τριάδα φυσικών αριθμών έτσι ώστε ο πρώτος αριθμός να είναι διαιρέτης του 90, ο δεύτερος αριθμός να είναι μικρότερος ή ίσος του πρώτου και ο τρίτος να είναι ίσος με το ημιάθροισμα των δύο πρώτων αριθμών.

22. Σε ένα φοιτητικό όμιλο συμμετέχουν 8 Γεωλόγοι, 5 Θεολόγοι, 4 Μαθηματικοί, 6 Φυσικοί και 7 Χημικοί. Να βρεθεί με πόσους τρόπους μπορεί να σχηματισθεί μια πενταμελής επιτροπή

(i) όταν όλοι είναι εξίσου εκλέξιμοι,

(ii) όταν στην επιτροπή δεν εκπροσωπούνται οι Φυσικοί,

(iii) όταν στην επιτροπή πρέπει να συμμετέχουν ακριβώς 2 Χημικοί,

(iv) όταν πρέπει να συμμετέχει τουλάχιστον ένας Γεωλόγος,

(v) όταν στην επιτροπή μπορεί να συμμετέχει το πολύ ένας Χημικός,

(vi) όταν στην επιτροπή συμμετέχουν τουλάχιστον 2 Μαθηματικοί,

(vii) όταν η επιτροπή αποτελείται από ένα αντιπρόσωπο κάθε ειδικότητας,

(viii) όταν στην επιτροπή είτε συμμετέχουν δύο συγκεκριμένοι Γεωλόγοι (ο Κώστας και η Μαρία), είτε δεν συμμετέχουν καθόλου Γεωλόγοι,

(ix) όταν η επιτροπή έχει πρόεδρο και ο πρόεδρος πρέπει να είναι Γεωλόγος,

(x) όταν η επιτροπή έχει πρόεδρο και ο πρόεδρος μπορεί να είναι οποιασδήποτε ειδικότητας,

(xi) όταν η επιτροπή έχει πρόεδρο και γραμματέα οι οποίοι πρέπει να είναι Θεολόγοι.

23. Κατά πόσους τρόπους μπορεί να σχηματισθεί ένα k-μελές συμβούλιο από ένα συνόλο n ανδρογύνων

(i) χωρίς κανέναν περιορισμό,

(ii) αν πρέπει να περιλαμβάνονται ακριβώς μ γυναίκες,

(iii) αν δεν μπορεί να συμμετέχουν και οι δύο σύζυγοι,

(iv) αν πρέπει να συμμετέχουν ακριβώς λ ανδρόγυνα μεταξύ των μελών του.

24. Μια τάξη ενός σχολείου, που αποτελείται από 6 αγόρια και 6 κορίτσια, χωρίζεται σε 6 ομάδες εργασίας δύο ατόμων η κάθε μια. Με πόσους τρόπους μπορεί να γίνει αυτό

(i) χωρίς κανέναν περιορισμό,

(ii) ώστε κάθε ομάδα να αποτελείται από άτομα του ίδιου φύλου,

(iii) ώστε κάθε ομάδα να αποτελείται από άτομα διαφορετικού φύλου.

25. Ανάμεσα σε $4n+1$ αντικείμενα τα n είναι ίδια. Να βρεθεί ο αριθμός των τρόπων επιλογής n αντικειμένων από τα $4n+1$ αντικείμενα.

26. Να δοθεί αλγεβρική και συνδυαστική απόδειξη των ισοτήτων

$$\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l} = \binom{n}{k-l}\binom{n-k+l}{l}.$$

27. Να βρεθεί ο αριθμός των υποσυνόλων του [1000] με 50 στοιχεία τα οποία δεν περιέχουν κανένα πολλαπλάσιο των αριθμών 2, 3 και 5.

28. Να βρεθεί ο αριθμός των υποσυνόλων του $[20] = \{1, 2, \ldots, 20\}$ με 10 στοιχεία τα οποία

(i) περιέχουν το σύνολο $\{4, 8, 9, 10\}$ ως υποσύνολό τους,

(ii) δεν περιέχουν το σύνολο $\{4, 8, 9, 10\}$ ως υποσύνολο τους,

(iii) περιέχουν το πολύ έναν από τους αριθμούς 1, 2,

(iv) περιέχουν το πολύ δύο από τους αριθμούς 8, 9, 10.

29. Να βρεθεί ο αριθμός των υποσυνόλων του [19] με οκτώ στοιχεία που έχουν, ως υποσύνολο, τουλάχιστον ένα από τα σύνολα $\{1, 5\}$, $\{11, 17\}$ και $\{5, 11, 17, 19\}$.

30. Για τα μονοπάτια που αποτελούνται από βήματα $(1, 0)$ και $(0, 1)$ να υπολογισθεί

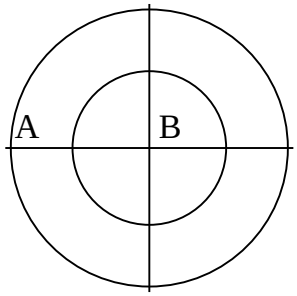
(i) ο αριθμός των μονοπατιών από το σημείο $(0, 0)$ στο σημείο $(50, 50)$,

(ii) ο αριθμός των μονοπατιών από το σημείο $(20, 20)$ στο σημείο $(50, 50)$,

(iii) ο αριθμός των μονοπατιών από το σημείο $(0, 0)$ στο σημείο $(50, 50)$ που διέρχονται από το σημείο $(20, 20)$,

(iv) ο αριθμός των μονοπατιών από το σημείο $(0,0)$ στο σημείο $(50,50)$ που δεν διέρχονται από το σημείο $(20,20)$.

31. Να βρεθεί ο αριθμός των διαδρομών από το σημείο A στο σημείο B χωρίς να χρησιμοποιηθεί δύο φορές ο ίδιος δρόμος.



32. Με πόσους τρόπους μπορούν να χορέψουν 8 ανδρόγυνα σε ένα κυκλικό χορό

(i) όταν δεν υπάρχουν άλλοι περιορισμοί,

(ii) ώστε οι σύζυγοι να χορεύουν δίπλα-δίπλα,

(iii) ώστε για 3 συγκεκριμένα ανδρόγυνα η γυναίκα να χορεύει δίπλα στον άνδρα.

33. Να δειχθεί ότι ο αριθμός των απεικονίσεων $f : [m] \to [n]$

(i) χωρίς περιορισμούς είναι ίσος με τον αριθμό των επαναληπτικών διατάξεων n ανά m,

(ii) που είναι 1–1 είναι ίσος με το πλήθος των διατάξεων των n ανά m,

(iii) που είναι γνησίως αύξουσες είναι ίσος με $\binom{n}{m}$,

(iv) που είναι αύξουσες είναι ίσος με $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]$.

34. Να βρεθεί μια αμφιμονοσήμαντη απεικόνιση μεταξύ του συνόλου των αυξουσών συναρτήσεων $f : [m] \to [n]$ και του συνόλου όλων των μη αρνητικών λύσεων της εξίσωσης $x_1+x_2+\cdots+x_n = m$.

(Υπόδειξη. Για $f : [m] \to [n]$ αύξουσα, ορίζουμε $x_i = |f^{-1}(\{i\})|$, για κάθε $i \in [n]$. Τότε $x_1 + x_2 + \cdots + x_n = m$.)

35. Να διατυπωθεί και να αποδειχθεί ανάλογο αποτέλεσμα με αυτό της λυμένης άσκησης 3.15 όταν $s = s_1 + s_2 + \cdots + s_n \geq m$ και $x_i \leq s_i$ για κάθε $i \in [n]$.

36. Πέντε άτομα μπαίνουν σε ασανσέρ στο ισόγειο ενός κτιρίου με 4 ορόφους. Με πόσους τρόπους μπορούν να κατανεμηθούν στους ορόφους αν μας ενδιαφέρει μόνο ο αριθμός των ατόμων που βγήκαν σε κάθε όροφο;

37. Με πόσους τρόπους μπορούμε να τοποθετήσουμε 10 αριθμημένες μπάλες σε 3 κουτιά με χωρητικότητες 3, 2 και 5 μπάλες αντίστοιχα;

38. (i) Με πόσους τρόπους μπορούμε να μοιράσουμε 10 μήλα σε 4 άτομα A, B, C, D;

(ii) Με πόσους τρόπους μπορούμε να μοιράσουμε 10 μήλα σε 4 άτομα A, B, C, D, έτσι ώστε κάθε άτομο να πάρει τουλάχιστον ένα μήλο;

(iii) Με πόσους τρόπους μπορούμε να μοιράσουμε 10 μήλα και 8 πορτοκάλια σε 4 άτομα A, B, C, D, έτσι ώστε κάθε άτομο να πάρει τουλάχιστον ένα μήλο;

39. Να δειχθεί ότι οι αριθμοί $\dfrac{(5n)!}{(n!)^3(2n)!}$ και $\dfrac{(5n)!}{(5!)^n}$ είναι ακέραιοι για κάθε $n \in \mathbb{N}^*$.

40. Να δειχθεί ότι για κάθε $m, n \in \mathbb{N}$ ισχύει ότι

$$\begin{aligned} n\binom{n}{m} &= (m+1)\binom{n}{m+1} + m\binom{n}{m} \\ &= m\binom{n+1}{m+1} + \binom{n}{m+1}. \end{aligned}$$

41. Να βρεθούν οι φυσικοί αριθμοί n οι οποίοι επαληθεύουν τις ανισότητες

(i) $\dfrac{n! + (n-2)!}{(n-2)!} \leq 3.$

(ii) $\dfrac{n \cdot (n+1)!}{2 \cdot n!} \leq 2n + 9.$

42. Να λυθούν στο σύνολο $\mathbb{N}$ οι εξισώσεις

(i) $\binom{n+1}{3} = 5(n-1).$

(ii) $\binom{n+1}{n-2} - 2\binom{n+1}{2} + 2\binom{n+1}{1} = 0.$

(iii) $\dfrac{\binom{n}{3}}{\binom{n+2}{3}} = \dfrac{1}{5}.$

(iv) $\binom{n}{n-3} = 2\binom{n}{n-2}.$

(v) $\dfrac{1}{\binom{4}{n}} = \dfrac{1}{\binom{5}{n}} + \dfrac{1}{\binom{6}{n}}.$

(vi) $\dfrac{1}{\binom{n}{4}} = \dfrac{1}{\binom{n}{5}} + \dfrac{1}{\binom{n}{6}}.$

43. Να δειχθεί ότι για κάθε $n, r \in \mathbb{N}$ ισχύει ότι

$$\binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \binom{r+3}{r} + \cdots + \binom{n-1}{r} + \binom{n}{r} = \binom{n+1}{r+1}.$$

i) Να δειχθεί ότι για κάθε $n \in \mathbb{N}^*$ ισχύει ότι $1 + 2 + 3 + \cdots + n = \binom{n+1}{2}$.

ii) Να δειχθεί ότι για κάθε $n \in \mathbb{N}^*$ ισχύει ότι $\dfrac{1}{2}(2 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + \cdots + n(n-1)) = \binom{n+1}{3}$.

44. Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι

(i) $\binom{n}{1} + 6\binom{n}{2} + 6\binom{n}{3} = n^3.$

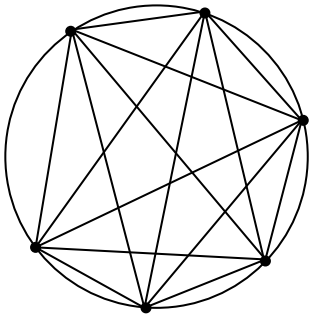
(ii) $1 + 7\binom{n}{1} + 12\binom{n}{2} + 6\binom{n}{3} = (n+1)^3.$

(iii) $1 + 14\binom{n}{1} + 36\binom{n}{2} + 24\binom{n}{3} = (n+1)^4 - n^4.$

(iv) $\binom{n}{1} + 14\binom{n}{2} + 36\binom{n}{3} + 24\binom{n}{4} = n^4.$

45. Έστω n σταθερός φυσικός αριθμός. Να δειχθεί ότι η μέγιστη τιμή του συνδυασμού $\binom{n}{k}$ λαμβάνεται όταν $k = n/2$ (αν ο n είναι άρτιος) και όταν $k = (n-1)/2$ (αν ο n είναι περιττός).

46. Δίνονται $n \geq 4$ σημεία στην περιφέρεια ενός κύκλου τα οποία ενώνονται ανά δύο με χορδές (ευθύγραμμα τμήματα). Επίσης, ισχύει ότι δεν υπάρχει εσωτερικό σημείο του κύκλου στο οποίο τεμνονται 3 χορδές.



i) Να βρεθεί ο αριθμός των χορδών που ορίζουν τα n σημεία.

ii) Να βρεθεί ο αριθμός των σημείων τομής των χορδών στο εσωτερικό του κύκλου.

∗iii) Να βρεθεί ο αριθμός των περιοχών του κύκλου που ορίζονται από τις χορδές.

47. i) Να δειχθεί ότι ο αριθμός των τρόπων επιλογής δύο υποσυνόλων A και B του $[n]$ με $A \subseteq B$ ισούται με 3^n.

ii) Να δειχθεί ότι ο αριθμός των τρόπων επιλογής δύο υποσυνόλων A και B του $[n]$ με $A \neq B$ ισούται με $2^n(2^n - 1)$.

iii) Να δειχθεί ότι ο αριθμός των τρόπων επιλογής δύο μη κενών ξένων υποσυνόλων A και B του $[n]$ ισούται με $3^n - 2^{n+1} + 1$.

48. Το αλφάβητο της πρωτόγονης γλώσσας Abba αποτελείται μόνο από δύο γράμματα. Είναι γνωστό ότι κάθε λέξη αυτής της γλώσσας δεν είναι αρχή μιας άλλης λέξης της γλώσσας.

(i) Να δειχθεί ότι αν στη γλώσσα Abba υπάρχει λέξη μήκους 2, τότε υπάρχουν το πολύ 12 λέξεις μήκους 4.

(ii) Να δειχθεί ότι αν στη γλώσσα Abba υπάρχουν 3 λέξεις μήκους 3, τότε υπάρχουν το πολύ 20 λέξεις μήκους 5.

(iii) Να δειχθεί ότι δεν είναι δυνατόν στη γλώσσα Abba να υπάρχουν 3 λέξεις μήκους 4, 10 λέξεις μήκους 5, 30 λέξεις μήκους 6 και 5 λέξεις μήκους 7.

∗49 i) Έστω A ένα σύνολο k-αδικών λέξεων μήκους n (δηλαδή λέξεων τα ψηφία των οποίων λαμβάνουν k διαφορετικές τιμές) με την ιδιότητα ότι κάθε ζευγάρι λέξων w, u που ανήκει στο A διαφέρει σε τουλάχιστον $2d + 1$ θέσεις. Να δειχθεί ότι

$$|A| \sum_{j=0}^{d} \binom{n}{j} (k-1)^j \leq k^n.$$

ii) Να δειχθεί, χρησιμοποιώντας το προηγούμενο υποερώτημα, ότι δεν υπάρχουν 10 δυαδικές λέξεις μήκους 6 με την ιδιότητα ότι οποιεσδήποτε δύο από αυτές να διαφέρουν σε τουλάχιστον 3 θέσεις.

50. Να δειχθεί ότι αν ένα σύνολο $\mathcal{X}$ υποσυνόλων του $[n]$ έχει την ιδιότητα ότι για κάθε $A, B \in \mathcal{X}$ ισχύει ότι $A \cap B \neq \emptyset$, τότε $|\mathcal{X}| \leq 2^{n-1}$.

51. Να βρεθεί ένα υποσύνολο X του $[100]$ με 9 στοιχεία, για το οποίο ισχύουν οι παρακάτω ιδιότητες:

i) $1 \in X$, $100 \in X$.

ii) Κάθε στοιχείο του X (εκτός του 1) γράφεται ως άθροισμα δύο (μπορεί και ίσων) στοιχείων του X.

52. i) Ένα σύνολο θετικών ακεραίων ονομάζεται **τέλειο** όταν η διαφορά κάθε ζεύγους στοιχείων του είναι διαφορετική από τη διαφορά οποιουδήποτε άλλου ζεύγους. Να κατασκευασθεί ένα τέλειο υποσύνολο του [20] με 5 στοιχεία.

ii) Ένα σύνολο θετικών ακεραιών ονομάζεται **μαγικό** όταν το άθροισμα κάθε ζεύγους στοιχείων του είναι διαφορετικό από το άθροισμα οποιουδήποτε άλλου ζευγους. Να αποδειχθεί ότι κάθε τέλειο σύνολο είναι μαγικό και αντιστρόφως.

53. Ένα υποσύνολο A του $[n]$ ονομάζεται **μεγάλο** αν για κάθε $x \in A$ ισχύει ότι $x \geq |A|$. Το κενό σύνολο θεωρείται μεγάλο. (Για παράδειγμα το σύνολο $\{2,3\}$ είναι μεγάλο, ενώ το σύνολο $\{2,3,5\}$ δεν είναι μεγάλο.) Να δειχθεί ότι ο αριθμός των μεγάλων υποσυνόλων του $[n]$ ισούται με τον αριθμό των υποσυνόλων του $[n]$ τα οποία δεν περιέχουν διαδοχικούς αριθμούς.

54. Μια διαμέριση π του $[n]$ ονομάζεται **συγχώνευση** μιας άλλης διαμέρισης σ του $[n]$ ανν η π προκύπτει από τη σ ενώνοντας ακριβώς δύο σύνολα της σ. Να δειχθεί ότι ο αριθμός των διαφορετικών τρόπων να καταλήξουμε στην διαμέριση του $[n]$ που αποτελείται από μόνο από το σύνολο $[n]$, ξεκινώντας από την διαμέριση του $[n]$ που αποτελείται από τα μονοσύνολα $\{1\}$, $\{2\}$, …, $\{n\}$ έτσι ώστε σε κάθε βήμα η διαμέριση του $[n]$ που προκύπτει να είναι συγχώνευση της αμέσως προηγούμενης διαμέρισης του $[n]$ ισούται με

$$\binom{n}{2}\binom{n-1}{2}\cdots\binom{2}{2} = \frac{n!(n-1)!}{2^n}$$

Για παράδειγμα, το σύνολο $[3] = \{1,2,3\}$ μπορεί να κατασκευασθεί με $\binom{4}{2}\binom{3}{2}\binom{2}{2} = 6 \cdot 3 \cdot 2 = 18$ διαφορετικούς τρόπους:

1ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,2\},\{3\},\{4\} \to \{1,2,3\},\{4\} \to \{1,2,3,4\}$.

2ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,2\},\{3\},\{4\} \to \{1,2,4\},\{3\} \to \{1,2,3,4\}$.

3ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,2\},\{3\},\{4\} \to \{1,2\},\{3,4\} \to \{1,2,3,4\}$.

4ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,3\},\{2\},\{4\} \to \{1,2,3\},\{4\} \to \{1,2,3,4\}$.

5ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,3\},\{2\},\{4\} \to \{1,3,4\},\{2\} \to \{1,2,3,4\}$.

6ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,3\},\{2\},\{4\} \to \{1,3\},\{2,4\} \to \{1,2,3,4\}$.

7ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,4\},\{2\},\{3\} \to \{1,2,4\},\{3\} \to \{1,2,3,4\}$.

8ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,4\},\{2\},\{3\} \to \{1,3,4\},\{2\} \to \{1,2,3,4\}$.

9ος: $\{1\},\{2\},\{3\},\{4\} \to \{1,4\},\{2\},\{3\} \to \{1,4\},\{2,3\} \to \{1,2,3,4\}$.

10ος: $\{1\},\{2\},\{3\},\{4\} \to \{2,3\},\{1\},\{4\} \to \{1,2,3\},\{4\} \to \{1,2,3,4\}$.

11ος: $\{1\},\{2\},\{3\},\{4\} \to \{2,3\},\{1\},\{4\} \to \{2,3,4\},\{1\} \to \{1,2,3,4\}$.

12ος: $\{1\},\{2\},\{3\},\{4\} \to \{2,3\},\{1\},\{4\} \to \{2,3\},\{1,4\} \to \{1,2,3,4\}$.

13ος: $\{1\},\{2\},\{3\},\{4\} \to \{2,4\},\{1\},\{3\} \to \{1,2,4\},\{3\} \to \{1,2,3,4\}$.

14ος: $\{1\},\{2\},\{3\},\{4\} \to \{2,4\},\{1\},\{3\} \to \{2,3,4\},\{1\} \to \{1,2,3,4\}$.

15ος: $\{1\},\{2\},\{3\},\{4\} \to \{2,4\},\{1\},\{3\} \to \{2,4\},\{1,3\} \to \{1,2,3,4\}$.

16ος: $\{1\},\{2\},\{3\},\{4\} \to \{3,4\},\{1\},\{2\} \to \{1,3,4\},\{2\} \to \{1,2,3,4\}$.

17ος: $\{1\},\{2\},\{3\},\{4\} \to \{3,4\},\{1\},\{2\} \to \{2,3,4\},\{1\} \to \{1,2,3,4\}$.

18ος: $\{1\},\{2\},\{3\},\{4\} \to \{3,4\},\{1\},\{2\} \to \{3,4\},\{1,2\} \to \{1,2,3,4\}$.

3.7 Παράρτημα: Οικογένειες Sperner

Έστω E ένα μη κενό σύνολο με n στοιχεία. Μια οικογένεια υποσυνόλων του E ονομάζεται **οικογένεια Sperner** αν και μόνο αν κανένα στοιχείο της δεν είναι υποσύνολο κάποιου άλλου στοιχείου της, δηλαδή τα στοιχεία της δεν είναι συγκρίσιμα ως προς τη σχέση του υποσυνόλου.

Παράδειγμα.

Έστω $E = \{1, 2, 3, 4, 5\}$. Η οικογένεια

$$\{1, 2, 4\}, \{1, 5\}, \{2, 3\}, \{1, 3, 4\}$$

είναι οικογένεια Sperner, ενώ η οικογένεια

$$\{1, 2, 4\}, \{1, 5\}, \{2, 3\}, \{1, 2, 5\}$$

δεν είναι οικογένεια Sperner, διότι $\{1, 5\} \subseteq \{1, 2, 5\}$.

Προφανώς, τα k-υποσύνολα του E αποτελούν μια οικογένεια Sperner.

Ο μέγιστος δυνατός πληθάριθμος για την οικογένεια των k-υποσυνόλων του E προκύπτει όταν $k = \lfloor \frac{n}{2} \rfloor$ (βλέπε άλυτη άσκηση 45).

Στην επόμενη πρόταση αποδεικνύεται ότι αυτός είναι ο μέγιστος δυνατός πληθάριθμος για κάθε οικογένεια Sperner ενός συνόλου E με n στοιχεία.

Πρόταση 3.15 (Μέγιστη οικογένεια Sperner). *Έστω E ένα μη κενό σύνολο με n στοιχεία. Η μέγιστη οικογένεια Sperner του E έχει πληθάριθμο* $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Απόδειξη. Έστω S μια οικογένεια Sperner του E.

Μια μετάθεση των στοιχείων του E θα ονομάζεται S-μετάθεση, αν υπάρχει σύνολο $A \in S$ έτσι ώστε τα πρώτα $|A|$ στοιχεία της μετάθεσης να είναι στοιχεία του συνόλου A. Στην περίπτωση αυτή λέμε ότι η S-μετάθεση αντιστοιχεί στο A.

Κάθε S-μετάθεση του E αντιστοιχεί σε ένα και μοναδικό σύνολο $A \in S$. Πράγματι, αν υπάρχουν δύο σύνολα $A, B \in S$ έτσι ώστε τα πρώτα $|A|$ και $|B|$ στοιχεία της μετάθεσης να είναι στοιχεία των συνόλων A και B τότε ένα από τα A, B θα ήταν υποσύνολο του άλλου, το οποίο είναι άτοπο.

Επίσης, κάθε σύνολο $A \in S$ αντιστοιχεί σε $|A|!(n-|A|)!$ S-μεταθέσεις του E. Πράγματι, υπάρχουν $|A|!$ διαφορετικές μεταθέσεις των στοιχείων του A και $(n-|A|)!$ μεταθέσεις των στοιχείων του $E \setminus \{A\}$. Άρα, από τον κανόνα του γινομένου υπάρχουν $|A|!(n-|A|)!$ S-μεταθέσεις που αντιστοιχούν στο A.

Επιπλέον, για κάθε οικογένεια Sperner S μπορεί να υπάρχουν το πολύ $n!$ S-μεταθέσεις του E (αφού όλες οι μεταθέσεις του E είναι $n!$).

Από τα προηγούμενα, αθροίζοντας τον αριθμό των S-μεταθέσεων του E που αντιστοιχούν σε κάθε σύνολο $A \in S$ προκύπτει η ανισότητα

$$\sum_{A \in S} |A|!(n - |A|)! \leq n!.$$

Διαιρώντας κατά μέλη με $n!$ προκύπτει η ανισότητα

$$\sum_{A \in S} \frac{1}{\binom{n}{|A|}} \leq 1.$$

Επειδή $\binom{n}{|A|} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ έπεται ότι

$$\sum_{A \in S} \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \leq \sum_{A \in S} \frac{1}{\binom{n}{|A|}} \leq 1$$

ή, ισοδύναμα

$$|S|\frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \leq \sum_{A \in S} \frac{1}{\binom{n}{|A|}} \leq 1.$$

Από την τελευταία ανισότητα προκύπτει ότι η μέγιστη τιμή του πληθαρίθμου $|S|$ είναι μικρότερη ή ίση από $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Τέλος, επειδή τα $\lfloor \frac{n}{2} \rfloor$-υποσύνολα του E αποτελούν μια οικογένεια Sperner του E με το μέγιστο δυνατό πληθάριθμο $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ η πρόταση ισχύει. □

Κεφάλαιο 4

Διαφορές, παραγοντικά πολυώνυμα, διώνυμο του Νεύτωνα

4.1 Διαφορές

Έστω h ένας σταθερός πραγματικός αριθμός. Για κάθε συνάρτηση g ορίζεται μια άλλη συνάρτηση Δg ως εξής:

$$\Delta g(x) \overset{1}{=} g(x+h) - g(x),$$

η οποία ονομάζεται **(πρώτη) διαφορά της** g (ή **διαφορά πρώτης τάξης** της g).

Η απεικόνιση

$$\Delta : g \to \Delta g$$

ονομάζεται **τελεστής διαφοράς**.

Παράδειγμα. Αν $g(x) = 3x^2 + 4x + 5$, τότε

$$\begin{aligned}\Delta g(x) &= g(x+h) - g(x)\\ &= 3(x+h)^2 + 4(x+h) + 5 - (3x^2 + 4x + 5)\\ &= 6xh + 3h^2 + 4h.\end{aligned}$$

Ιδιότητες διαφοράς

1. $\Delta(g_1 + g_2) = \Delta g_1 + \Delta g_2$, για κάθε δύο συναρτήσεις g_1, g_2,
2. $\Delta(cg) = c\Delta g$, για κάθε $c \in \mathbb{R}$,

δηλαδή ο τελεστής διαφοράς είναι *γραμμικός*.

Η διαφορά $\Delta(\Delta g)(x)$ ονομάζεται **δεύτερη διαφορά** (ή **διαφορά δεύτερης τάξης**) και σημειώνεται με

$$\Delta^2 g(x) = \Delta(\Delta g(x)).$$

Επαγωγικά, ορίζεται η n**-οστή διαφορά** (ή **διαφορά** n**-οστής τάξης**) ως η διαφορά της $(n-1)$-οστής διαφοράς, δηλαδή

$$\Delta^n g(x) = \Delta(\Delta^{n-1} g(x)).$$

Στα επόμενα θα θεωρείται $h = 1$.

[1] Θεωρούμε ότι για κάθε x στο πεδίο ορισμού της g ισχύει ότι και $x + h$ ανήκει επίσης σ' αυτό.

Παρατήρηση.

Οι διαφορές μιας συνάρτησης g εκφράζονται ως γραμμικός συνδυασμός διαδοχικών τιμών της g.

Παραδείγματα

1. $\Delta g(x) = g(x+1) - g(x)$.

2. $$\begin{aligned}\Delta^2 g(x) &= \Delta(\Delta g(x)) = \Delta(g(x+1) - g(x)) \\ &= \Delta g(x+1) - \Delta g(x) \\ &= g(x+2) - g(x+1) - (g(x+1) - g(x)) \\ &= g(x+2) - 2g(x+1) + g(x).\end{aligned}$$

3. $$\begin{aligned}\Delta^3 g(x) &= \Delta(\Delta^2 g(x)) = \Delta\left(g(x+2) - 2g(x+1) + g(x)\right) \\ &= \Delta g(x+2) - 2\Delta g(x+1) + \Delta g(x) \\ &= g(x+3) - g(x+2) - 2(g(x+2) - g(x+1)) + g(x+1) - g(x) \\ &= g(x+3) - 3g(x+2) + 3g(x+1) - g(x).\end{aligned}$$

4. $$\begin{aligned}\Delta^4 g(x) &= \Delta(\Delta^3 g(x)) = \Delta\left(g(x+3) - 3g(x+2) + 3g(x+1) - g(x)\right) \\ &= \Delta g(x+3) - 3\Delta g(x+2) + 3\Delta g(x+1) - \Delta g(x) \\ &= g(x+4) - g(x+3) - 3\left(g(x+3) - g(x+2)\right) + 3\left(g(x+2) - g(x+1)\right) - \left(g(x+1) - g(x)\right) \\ &= g(x+4) - 4g(x+3) + 6g(x+2) - 4g(x+1) + g(x).\end{aligned}$$

Γενικά ισχύει το παρακάτω αποτέλεσμα:

Πρόταση 4.1 (Γραμμικός συνδυασμός διαφορών). *Για κάθε $n \in \mathbb{N}^*$ ισχύει ότι*

$$\Delta^n g(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} g(x+n-k).$$

Απόδειξη. Για την απόδειξη της πρότασης βλέπε στις λυμένες ασκήσεις. □

Προσδιορισμός των διαφορών με τη βοήθεια πινάκων

Συνήθως οι διαφορές μιας συνάρτησης υπολογίζονται με τη βοήθεια πινάκων.

Παράδειγμα 4.1.1. *Να βρεθούν οι διαφορές πρώτης, δεύτερης και τρίτης τάξης, για $x = 0$, της συνάρτησης $g(x)$ όταν $g(0) = 4$, $g(1) = 6$, $g(2) = 9$ και $g(3) = 14$.*

x	$g(x)$	$\Delta g(x)$	$\Delta^2 g(x)$	$\Delta^3 g(x)$
3	14			
2	9	5		
1	6	3	2	
0	4	2	1	1

Άρα, $\Delta g(0) = 2$, $\Delta^2 g(0) = 1$ και $\Delta^3 g(0) = 1$.

4.2 Παραγοντικά πολυώνυμα

Παραγοντικό πολύωνυμο τάξεως k.

$$F_0(x) = 1,$$

$$F_k(x) = \underbrace{x(x-1)(x-2)\cdots(x-k+1)}_{k \text{ όροι}} = (x)_k, \qquad \text{για } k \in \mathbb{N}^*.$$

Παραδείγματα

1. $F_1(x) = x$
2. $F_2(x) = x(x-1) = x^2 - x$
3. $F_3(x) = x(x-1)(x-2) = x^3 - 3x^2 + 2x$
4. $F_4(x) = x(x-1)(x-2)(x-3) = x^4 - 6x^3 + 11x^2 - 6x.$

Οι συντελεστές των x^i που εμφανίζονται στους τύπους των παραγοντικών πολυωνύμων ονομάζονται αριθμοί Stirling πρώτου είδους.

Ιδιότητες παραγοντικών πολυωνύμων

1. $F_k(k) = k!$.
2. $F_k(n) = 0$, για κάθε $n \in \mathbb{N}$ με $n < k$.
3. $F_k(n) = P(n,k)$, για κάθε $n \in \mathbb{N}$ με $n > k$.
4. $F_k(x) = (x-k+1)F_{k-1}(x)$, για κάθε $k \geq 1$.
5. $\Delta F_k(x) = kF_{k-1}(x)$.
   Πραγματικά,
   $$\begin{aligned}\Delta F_k(x) &= F_k(x+1) - F_k(x)\\ &= (x+1)x\cdots(x-k+2) - x(x-1)\cdots(x-k+1)\\ &= x(x-1)\cdots(x-k+2)((x+1)-(x-k+1))\\ &= kx(x-1)\cdots(x-(k-1)+1)\\ &= kF_{k-1}(x).\end{aligned}$$
6. Γενικά, αποδεικνύεται ότι $\Delta^\nu F_k(x) = F_\nu(k)F_{k-\nu}(x)$, για κάθε $\nu, k \in \mathbb{N}^*$ με $\nu \leq k$.

Εκφράσεις πολυωνύμων με τη βοήθεια παραγοντικών πολυωνύμων

Κάθε πολυώνυμο $p(x)$ βαθμού k μπορεί να εκφραστεί ως γραμμικός συνδυασμός των παραγοντικών πολυωνύμων $F_0(x)$, $F_1(x)$, $F_2(x)$, …, $F_k(x)$.

Πράγματι, επειδή κάθε πολυώνυμο $p(x)$ βαθμού k είναι γραμμικός συνδυασμός των μονονύμων 1, x, x^2, …, x^k, αρκεί να εκφράσουμε τα μονώνυμα ως γραμμικό συνδυασμό των παραγοντικών πολυωνύμων.

Εκφράσεις μονωνύμων

Τα μονώνυμα μπορούν να εκφρασθούν με τη βοήθεια παραγοντικών πολυωνύμων.

Παραδείγματα

1. $x = F_1(x)$, διότι $F_1(x) = x$.

2. $x^2 = F_1(x) + F_2(x)$, διότι $F_2(x) = x^2 - x \Rightarrow x^2 = x + F_2(x) = F_1(x) + F_2(x)$

3. $x^3 = F_1(x) + 3F_2(x) + F_3(x)$,
   διότι $F_3(x) = x(x-1)(x-2) = x^3-3x^2+2x \Rightarrow x^3 = F_3(x)+3x^2-2x = F_3(x)+3(F_1(x)+F_2(x))-2F_1(x)$.

4. Όμοια αποδεικνύεται ότι $x^4 = F_1(x) + 7F_2(x) + 6F_3(x) + F_4(x)$.

Οι συντελεστές των $F_i(x)$ που εμφανίζονται στους τύπους έκφρασης των μονονύμων από τα παραγοντικά πολυώνυμα ονομάζονται **αριθμοί Stirling δευτέρου είδους**.

Με τη βοήθεια των τύπων των προηγούμενων παραδειγμάτων μπορούμε να εκφράσουμε οποιοδήποτε πολυώνυμο βαθμού μέχρι 4 ως γραμμικό συνδυασμό παραγοντικών πολυωνύμων.

Παράδειγμα 4.2.1. *Να εκφραστεί το πολύωνυμο $p(x) = 7x^3 - 2x^2 + 6x + 4$ ως γραμμικός συνδυασμός των παραγοντικών πολυωνύμων $F_0(x)$, $F_1(x)$, $F_2(x)$ και $F_3(x)$.*

Λύση. Από τα προηγούμενα παραδείγματα ισχύει ότι

$$\begin{aligned} p(x) &= 7(F_1(x) + 3F_2(x) + F_3(x)) - 2(F_1(x) + F_2(x)) + 6F_1(x) + 4F_0(x) \\ &= 7F_3(x) + 19F_2(x) + 11F_1(x) + 4F_0(x). \end{aligned}$$

□

Βασική ιδιότητα πολυωνύμων

Για δύο πολυώνυμα $p_1(x)$, $p_2(x)$ ισχύει:

$$\text{Αν } \Delta p_1(x) = \Delta p_2(x), \text{ τότε υπάρχει } c \in R \text{ ώστε } p_1(x) - p_2(x) = c \text{ για κάθε } x \in \mathbb{R}.$$

Με άλλα λόγια, αν δύο πολυώνυμα έχουν την ίδια διαφορά τότε έχουν τον ίδιο βαθμό και διαφέρουν κατά μία σταθερά. Η ιδιότητα αυτή είναι χρήσιμη σε πολλά προβλήματα.

Προσδιορισμός πολυωνύμων με γνωστή διαφορά

Παράδειγμα 4.2.2. *Να βρεθεί πολυώνυμο $p(x)$ για το οποίο ισχύουν*

$$p(x+1) - p(x) = x(x+1)(x+2) \text{ και } p(1) = 0.$$

Λύση. Εκφράζουμε το πολυώνυμο του δεύτερου μέλους συναρτήσει των παραγοντικών πολυωνύμων.

$$\begin{aligned} x(x+1)(x+2) &= x^3 + 3x^2 + 2x \\ &= (F_1(x) + 3F_2(x) + F_3(x)) + 3(F_1(x) + F_2(x)) + 2F_1(x) \\ &= F_3(x) + 6F_2(x) + 6F_1(x). \end{aligned}$$

Εφαρμόζουμε τον τύπο $F_k(x) = \dfrac{\Delta F_{k+1}(x)}{k+1}$.

$$\begin{aligned} x(x+1)(x+2) &= \frac{\Delta F_4(x)}{4} + 6\frac{\Delta F_3(x)}{3} + 6\frac{\Delta F_2(x)}{2} \\ &= \Delta\left(\frac{1}{4}F_4(x) + 2F_3(x) + 3F_2(x)\right). \end{aligned}$$

Άρα, από την υπόθεση προκύπτει ότι

$$\Delta p(x) = \Delta\left(\frac{1}{4}F_4(x) + 2F_3(x) + 3F_2(x)\right)$$

και επομένως υπάρχει $c \in \mathbb{R}$ ώστε

$$\begin{aligned} p(x) &= \frac{1}{4}F_4 + 2F_3(x) + 3F_2(x) + c \\ &= \frac{x(x-1)(x-2)(x-3)}{4} + 2x(x-1)(x-2) + 3x(x-1) + c. \end{aligned}$$

Για $x = 1$ προκύπτει $0 = p(1) = c$, οπότε,

$$p(x) = \frac{x(x-1)(x-2)(x-3)}{4} + 2x(x-1)(x-2) + 3x(x-1) = \frac{(x+2)(x+1)x(x-1)}{4}.$$ □

Παρατήρηση.

Το προηγούμενο παράδειγμα μπορεί να χρησιμοποιηθεί στον υπολογισμό αθροισμάτων πολυωνυμικών εκφράσεων.

Εφαρμογή 4.2.1. *Να βρεθεί η τιμή του αθροίσματος*

$$S_n = 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + (n-1)n(n+1) + n(n+1)(n+2).$$

Λύση. Βρίσκουμε πολυώνυμο $p(x)$ με

$$\Delta p(x) = x(x+1)(x+2),$$

σύμφωνα με το προηγούμενο παράδειγμα

$$p(x) = \frac{(x+2)(x+1)x(x-1)}{4}.$$

οπότε είναι

$$\begin{aligned} S_n &= \Delta p(1) + \Delta p(2) + \cdots + \Delta p(n-1) + \Delta p(n) \\ &= (p(2) - p(1)) + (p(3) - p(2)) + \cdots + (p(n) - p(n-1)) + (p(n+1) - p(n)) \\ &= p(n+1) - p(1) \\ &= \frac{(n+3)(n+2)(n+1)n}{4}. \end{aligned}$$ □

Παρατήρηση.

Η ιδέα της προηγούμενης εφαρμογής είναι ότι για τον υπολογισμό ενός αθροίσματος $\sum_{k=a}^{b} f(k)$ αρκεί να βρούμε μια συνάρτηση $g(x)$ με $\Delta g(x) = f(x)$. Τότε, $\sum_{k=a}^{b} f(k) = g(b+1) - g(a)$.

Στην περίπτωση όπου η $f(x)$ είναι πολυώνυμο του x, η εύρεση της $g(x)$ μπορεί να γίνει με τη βοήθεια των παραγοντικών πολυωνύμων.

Όμως, όταν η $f(x)$ δεν είναι πολυώνυμο του x, για την εύρεση της $g(x)$ δεν υπάρχει γενική μέθοδος.

4.3 Ο τύπος του Gregory

Πρόταση 4.2 (Τύπος του Gregory με παραγοντικά πολυώνυμα). *Για κάθε πολυώνυμο $p(x)$ βαθμού n, ισχύει ότι*

$$p(x) = \sum_{k=0}^{n} \frac{\Delta^k p(0)}{k!} F_k(x).$$

Εφαρμογή 4.3.1. *Να βρεθεί πολυώνυμο $p(x)$ βαθμού το πολύ 3 όταν $p(0) = 3$, $p(1) = 5$, $p(2) = 7$ και $p(3) = 15$.*

Λύση.

x	$p(x)$	$\Delta p(x)$	$\Delta^2 p(x)$	$\Delta^3 p(x)$
3	15			
2	7	8		
1	5	2	6	
0	3	2	0	6

Άρα,

$$\Delta p(0) = 2,\ \Delta^2 p(0) = 0,\ \Delta^3 p(0) = 6.$$

Οπότε από τον τύπο του Gregory είναι:

$$\begin{aligned} p(x) &= p(0) + \frac{\Delta^1 p(0)}{1!} F_1(x) + \frac{\Delta^2 p(0)}{2!} F_2(x) + \frac{\Delta^3 p(0)}{3!} F_3(x) \\ &= 3 + 2x + 0x(x-1) + \frac{6}{3!} x(x-1)(x-2) \\ &= x^3 - 3x^2 + 4x + 3. \end{aligned}$$

□

Παρατήρηση. Ο τύπος του Gregory χρησιμοποιείται επίσης σε προβλήματα πολυωνυμικής παρεμβολής: Δίδονται οι $n+1$ διαδοχικές τιμές $f(0)$, $f(1)$, $f(2)$, ..., $f(n)$ μιας συνάρτησης $f(x)$ με άγνωστο ή σύνθετο τύπο και ζητείται να βρεθεί πολυώνυμο $p(x)$, βαθμού το πολύ n, οι τιμές του οποίου ταυτίζονται με τις τιμές της $f(x)$ στα συγκεκριμένα σημεία.

Εφαρμογή 4.3.2. *Να βρεθεί ο επόμενος όρος της παρακάτω ακολουθίας*

$$1, 1, 1, 19, 109, ?$$

Λύση. Τέτοιες ερωτήσεις χρησιμοποιούνται συχνά σε τέστ ευφυίας. Φυσικά υπάρχουν άπειρες ακολουθίες με αρχή την παραπάνω υπακολουθία. Κάθε απάντηση είναι δεκτή αρκεί να δοθεί ένας "κανόνας" ή "τύπος" που να παράγει τους παραπάνω αριθμούς.

Από τον τύπο του Gregory μπορούμε, χωρίς ιδιαίτερη σκέψη, να βρίσκουμε τύπους για τέτοιες ερωτήσεις με τη **μορφή πολυωνύμων**.

Το πρόβλημα ανάγεται στην εύρεση πολυωνύμου $p(x)$ βαθμού το πολύ 4 όπου $p(0) = 1$, $p(1) = 1$, $p(2) = 1$, $p(3) = 19$ και $p(4) = 109$.

Αρχικά υπολογίζουμε τις διαφορές του $p(x)$ στο 0 με τη βοήθεια του παρακάτω πίνακα:

x	$p(x)$	$\Delta p(x)$	$\Delta^2 p(x)$	$\Delta^3 p(x)$	$\Delta^4 p(x)$
4	109				
3	19	90			
2	1	18	72		
1	1	0	18	54	
0	1	0	0	18	36

Από τον πίνακα έχουμε ότι $p(0) = 1$, $\Delta p(0) = 0$, $\Delta^2 p(0) = 0$, $\Delta^3 p(0) = 18$ και $\Delta^4 p(0) = 36$.

Επομένως,

$$\begin{aligned} p(x) &= p(0) + \frac{\Delta p(0)}{1!}F_1(x) + \frac{\Delta^2 p(0)}{2!}F_2(x) + \frac{\Delta^3 p(0)}{3!}F_3(x) + \frac{\Delta^4 p(0)}{4!}F_4(x) \\ &= 1 + \frac{18}{6}x(x-1)(x-2) + \frac{36}{24}x(x-1)(x-2)(x-3) \\ &= 1 + 3x(x-1)(x-2) + \frac{3}{2}x(x-1)(x-2)(x-3) \end{aligned}$$

Άρα, η επόμενη τιμή της ακολουθίας (θα μπορούσε να) είναι

$$p(5) = 1 + 3 \cdot 5 \cdot 4 \cdot 3 + \frac{3}{2} \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 361.$$

Παρατήρηση. Στη περίπτωση που δεχτούμε ότι ο τύπος της ακολουθίας είναι πολυώνυμο βαθμού 4, μπορούμε να υπολογίσουμε τον επόμενο όρο της ακολουθίας χωρίς να βρούμε τον γενικό τύπο του πολυωνύμου χρησιμοποιώντας την εξής ιδέα: Η 5η διαφορά ενός πολυωνύμου $p(x)$ βαθμού 4 είναι το μηδενικό πολυώνυμο, δηλαδή[2] $\Delta^5 p(x) = 0$.

Έστω $p(5) = a$. Τότε πρέπει $\Delta^5 p(0) = 0$. Από τον επόμενο πίνακα έχουμε ότι

x	$p(x)$	$\Delta p(x)$	$\Delta^2 p(x)$	$\Delta^3 p(x)$	$\Delta^4 p(x)$	$\Delta^5 p(x)$
5	a					
4	109	$a - 109$				
3	19	90	$a - 199$			
2	1	18	72	$a - 271$		
1	1	0	18	54	$a - 325$	
0	1	0	0	18	36	$a - 361$

Άρα, $a - 361 = 0$, δηλαδή $a = 361$. □

[2] Βλέπε άλυτη άσκηση 4).

4.4 Ο τύπος του Vandermonde

Πρόταση 4.3 (Τύπος του Vandermonde). *Για κάθε $x, y \in \mathbb{R}$ και $n \in \mathbb{N}^*$ ισχύει ότι*

$$F_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} F_k(x) F_{n-k}(y). \tag{4.1}$$

Απόδειξη. Για την απόδειξη της πρότασης βλέπε στις λυμένες ασκήσεις. □

4.5 Ο τύπος του διωνύμου του Νεύτωνα

Γνωρίζουμε ότι

$$(a+\beta)^2 = \sum_{k=0}^{2} \binom{2}{k} a^{2-k}\beta^k.$$

Πράγματι,

$$\begin{aligned}\sum_{k=0}^{2} \binom{2}{k} a^{2-k}\beta^k &= \binom{2}{0} a^{2-0}\beta^0 + \binom{2}{1}\alpha^{2-1}\beta^1 + \binom{2}{2}\alpha^{2-2}\beta^2 \\ &= 1a^2\beta^0 + 2a^1\beta^1 + 1a^0\beta^2 \\ &= a^2 + 2a\beta + \beta^2 \\ &= (a+b)^2.\end{aligned}$$

Επίσης,

$$(a+\beta)^3 = \sum_{k=0}^{3} \binom{3}{k} a^{3-k}\beta^k.$$

Πράγματι,

$$\begin{aligned}\sum_{k=0}^{3} \binom{3}{k} a^{3-k}\beta^k &= \binom{3}{0} a^{3-0}\beta^0 + \binom{3}{1}\alpha^{3-1}\beta^1 + \binom{3}{2}\alpha^{3-2}\beta^2 + \binom{3}{3}\alpha^{3-3}\beta^3 \\ &= 1a^3\beta^0 + 3a^2\beta^1 + 3a^1\beta^2 + 1a^0\beta^3 \\ &= a^3 + 3a^2\beta + 3a\beta^2 + \beta^3 \\ &= (a+b)^3.\end{aligned}$$

Γενικά ισχύει το επόμενο αποτέλεσμα:

Πρόταση 4.4 (Τύπος του διωνύμου του Νεύτωνα). *Για κάθε $\alpha, \beta \in \mathbb{R}$ και $n \in \mathbb{N}^*$ ισχύει ότι*

$$(\alpha+\beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k}.$$

Απόδειξη. (Με επαγωγή ως προς n). Για $n = 1$ ισχύει διότι

$$\sum_{k=0}^{1} \binom{n}{k} \alpha^k \beta^{1-k} = \binom{1}{0}\alpha^0\beta^1 + \binom{1}{1}\alpha^1\beta^0 = \beta + \alpha.$$

Υποθέτουμε ότι ισχύει για $n = m$, δηλαδή

$$(\alpha+\beta)^m = \sum_{k=0}^{m} \binom{m}{k} \alpha^k \beta^{m-k}$$

και θα δείξουμε ότι ισχύει για $n = m+1$, δηλαδή

$$(\alpha+\beta)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} \alpha^k \beta^{m+1-k}.$$

Πραγματικά, είναι

$$\begin{aligned}
(\alpha+\beta)^{m+1} &= (\alpha+\beta)(\alpha+\beta)^m = (\alpha+\beta)\sum_{k=0}^{m}\binom{m}{k}\alpha^k\beta^{m-k} = \sum_{k=0}^{m}\binom{m}{k}a^{k+1}\beta^{m-k} + \sum_{k=0}^{m}\binom{m}{k}a^k\beta^{m+1-k} \\
&= \sum_{\lambda=1}^{m+1}\binom{m}{\lambda-1}\alpha^{\lambda}\beta^{m+1-\lambda} + \sum_{k=0}^{m}\binom{m}{k}\alpha^k\beta^{m+1-k} \\
&= a^{m+1} + \sum_{k=1}^{m}\binom{m}{k-1}\alpha^k\beta^{m+1-k} + \beta^{m+1} + \sum_{k=1}^{m}\binom{m}{k}\alpha^k\beta^{m+1-k} \\
&= a^{m+1} + \beta^{m+1} + \sum_{k=1}^{m}\left(\binom{m}{k} + \binom{m}{k-1}\right)\alpha^k\beta^{m+1-k} \\
&= a^{m+1} + \beta^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k}\alpha^k\beta^{m+1-k} = \sum_{k=0}^{m+1}\binom{m+1}{k}a^k\beta^{m+1-k}.
\end{aligned}$$

□

Οι αριθμοί $\binom{n}{k}$ με $n, k \in \mathbb{N}^*$ και $k \le n$ ονομάζονται **διωνυμικοί συντελεστές**.

Ο τύπος του Νεύτωνα έχει πολλές εφαρμογές. Μια σημαντική εφαρμογή του είναι στον υπολογισμό αθροισμάτων τα οποία περιέχουν διωνυμικούς συντελεστές.

Εφαρμογή 4.5.1. *Να υπολογισθούν τα αθροίσματα:*

$$S_1 = \sum_{k=0}^{n}\binom{n}{k}, \qquad S_2 = \sum_{k=0}^{n}(-1)^k\binom{n}{k}, \qquad S_3 = \sum_{k=0}^{\left[\frac{n}{2}\right]}\binom{n}{2k},$$

$$S_4 = \sum_{k=0}^{\left[\frac{n-1}{2}\right]}\binom{n}{2k+1}, \qquad S_5 = \sum_{k=1}^{n}k\binom{n}{k}, \qquad S_6 = \sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k},$$

$$S_7 = \sum_{k=0}^{n}\frac{(-1)^{k+1}}{k+1}\binom{n}{k}, \qquad S_8 = \sum_{k=0}^{\left[\frac{n}{2}\right]}\frac{1}{2k+1}\binom{n}{2k}.$$

Λύση. Εφαρμόζοντας τον τύπο του διωνύμου του Νεύτωνα για $\alpha = \beta = 1$ και $\alpha = -1$, $\beta = 1$ προκύπτουν τα παρακάτω:

$$(1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^k1^{n-k} \Leftrightarrow S_1 = \sum_{k=0}^{n}\binom{n}{k} = 2^n,$$

$$(-1+1)^n = \sum_{k=0}^{n}\binom{n}{k}(-1)^k1^{n-k} \Leftrightarrow S_2 = \sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0.$$

Τα S_3, S_4 θα υπολογισθούν όταν $n = 2m$ άρτιος (ανάλογα υπολογίζονται όταν n περιττός). Τότε $\left[\frac{n}{2}\right] = m$ και $\left[\frac{n-1}{2}\right] = m-1$.

$$S_3 + S_4 = \sum_{k=0}^{m}\binom{n}{2k} + \sum_{k=0}^{m-1}\binom{n}{2k+1} = \sum_{k=0}^{n}\binom{n}{k} = S_1 = 2^n$$

$$S_3 - S_4 = \sum_{k=0}^{m}\binom{n}{2k} - \sum_{k=0}^{m-1}\binom{n}{2k+1} = \sum_{k=0}^{m}(-1)^{2k}\binom{n}{2k} + \sum_{k=0}^{m-1}(-1)^{2k+1}\binom{n}{2k+1} = \sum_{k=0}^{n}-1^k\binom{n}{k} = S_2 = 0.$$

Άρα,

$$S_3 = S_4 = 2^{n-1}.$$

Για το S_5 θα χρησιμοποιήσουμε την ταυτότητα

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{4.2}$$

Είναι

$$S_5 = \sum_{k=1}^{n} k\binom{n}{k} = \sum_{k=1}^{n} n\binom{n-1}{k-1} \overset{\lambda=k-1}{=} n\sum_{\lambda=0}^{n-1}\binom{n-1}{\lambda} \overset{(S_1)}{=} n2^{n-1}.$$

Άρα,

$$S_5 = n2^{n-1}.$$

Για το S_6 θα χρησιμοποιήσουμε την (4.2) με $n+1$ αντί n και $k+1$ αντί k, δηλαδή

$$(k+1)\binom{n+1}{k+1} = (n+1)\binom{n}{k} \Leftrightarrow$$

$$\frac{1}{k+1}\binom{n}{k} = \frac{1}{n+1}\binom{n+1}{k+1}. \tag{4.3}$$

Είναι

$$S_6 = \sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k} = \sum_{k=0}^{n}\frac{1}{n+1}\binom{n+1}{k+1} \overset{\lambda=k+1}{=} \frac{1}{n+1}\sum_{\lambda=1}^{n+1}\binom{n+1}{\lambda} \overset{S_1}{=} \frac{1}{n+1}(2^{n+1}-1).$$

Άρα,

$$S_6 = \frac{2^{n+1}-1}{n+1}.$$

Για τον υπολογισμό του S_7 χρησιμοποιούμε την (4.3) οπότε είναι:

$$\begin{aligned} S_7 &= \sum_{k=0}^{n}\frac{(-1)^{k+1}}{k+1}\binom{n}{k} = \sum_{k=0}^{n}(-1)^{k+1}\frac{1}{n+1}\binom{n+1}{k+1} \\ &= \frac{1}{n+1}\sum_{\lambda=1}^{n+1}(-1)^{\lambda}\binom{n+1}{\lambda} = \frac{1}{n+1}\left(\sum_{\lambda=0}^{n_1}(-1)^{\lambda}\binom{n+1}{\lambda} - 1\right) \\ &= \frac{1}{n+1}(0-1). \end{aligned}$$

Άρα,

$$S_7 = -\frac{1}{n+1}.$$

Για το S_8 χρησιμοποιούμε την (4.3) με $2k$ αντί για k, οπότε είναι:

$$S_8 = \sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{1}{2k+1}\binom{n}{k} = \sum_{k=0}^{\left[\frac{n}{2}\right]} \frac{1}{n+1}\binom{n+1}{2k+1}$$
$$= \frac{1}{n+1}\sum_{k=0}^{\left[\frac{m-1}{2}\right]} \binom{m}{2k+1} = \frac{1}{n+1}2^{m-1} = \frac{1}{n+1}2^n.$$

Άρα,

$$S_8 = \frac{2^n}{n+1}.$$ □

Πρόταση 4.5 (Τύπος του Cauchy). *Για κάθε $r, s, n \in \mathbb{N}^*$ ισχύει ότι*

$$\binom{r+s}{n} = \sum_{k=0}^{n}\binom{r}{k}\binom{s}{n-k}.$$

Απόδειξη. Για κάθε $x \in \mathbb{R}$ είναι:

$$(x+1)^{r+s} = (x+1)^r(x+1)^s \Leftrightarrow$$
$$\sum_{n=0}^{r+s}\binom{r+s}{n}x^n 1^{r+s-n} = \left(\sum_{k=0}^{r}\binom{r}{k}x^k 1^{r-k}\right)\left(\sum_{\lambda=0}^{s}\binom{s}{\lambda}x^\lambda 1^{s-\lambda}\right) \Leftrightarrow$$
$$\sum_{n=0}^{r+s}\binom{r+s}{n}x^n = \left(\sum_{k=0}^{r}\binom{r}{k}x^k\right)\left(\sum_{\lambda=0}^{s}\binom{s}{\lambda}x^\lambda\right) \Leftrightarrow$$
$$\sum_{n=0}^{r+s}\binom{r+s}{n}x^n = \sum_{k=0}^{r}\sum_{\lambda=0}^{s}\binom{r}{k}\binom{s}{\lambda}x^{k+\lambda}. \tag{4.4}$$

Αν τεθεί $n = k + \lambda$ τότε είναι:

$$\sum_{k=0}^{r}\sum_{\lambda=0}^{s}\binom{r}{k}\binom{s}{\lambda}x^{k+\lambda} = \sum_{n=0}^{r+s}\sum_{k=0}^{n}\binom{r}{k}\binom{s}{n-k}x^n, \tag{4.5}$$

οπότε από τις σχέσεις (4.4), (4.5) είναι:

$$\sum_{n=0}^{r+s}\binom{r+s}{n}x^n = \sum_{n=0}^{r+s}\left(\sum_{k=0}^{n}\binom{r}{k}\binom{s}{n-k}\right)x^n, \text{ για κάθε } x \in \mathbb{R}.$$

Άρα

$$\binom{r+s}{n} = \sum_{k=0}^{n}\binom{r}{k}\binom{s}{n-k}.$$ □

Εφαρμογή: Από τον τύπο του Cauchy για $r = s = n$ προκύπτει ότι

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}.$$

Επέκταση των διωνυμικών συντελεστών $\binom{x}{k}$ όταν $x \in \mathbb{R}$ και $k \in \mathbb{N}$.

$$\binom{x}{k} = \frac{F_k(x)}{k!} = \frac{x(x-1)\cdots(x-k+1)}{k!}.$$

Αν $x = n \in \mathbb{N}$ οι διωνυμικοί συντελεστές εκφράζουν τους αριθμούς των n ανά k συνδυασμών.
Αν $x = -n$, όπου $n \in \mathbb{N}^*$, είναι:

$$\begin{aligned}\binom{-n}{k} &= \frac{(-n)(-n-1)\cdots(-n-k+1)}{k!} = (-1)^k \frac{n(n+1)\cdots(n+k-1)}{k!} \\ &= (-1)^k \binom{n+k-1}{k} = (-1)^k \left[\!\!\binom{n}{k}\!\!\right].\end{aligned}$$

Έτσι το $\left|\binom{-n}{k}\right|$ εκφράζει τον αριθμό των n ανά k επαναληπτικών συνδυασμών.

Χρησιμοποιώντας την επέκταση των διωνυμικών συντελεστών, ο τύπος του Gregory διατυπώνεται ως εξής:

Πρόταση 4.6 (Τύπος του Gregory με διωνυμικούς συντελεστές). *Για κάθε πολυώνυμο $p(x)$ βαθμού n, ισχύει ότι*

$$p(x) = \sum_{k=0}^{n} \binom{x}{k} \Delta^k p(0).$$

Παρατήρηση. Από τον παραπάνω τύπο προκύπτει ότι κάθε πολυώνυμο γράφεται ως γραμμικός συνδυασμός των διωνυμικών συντελεστών.

Επιπλέον, χρησιμοποιώντας την επέκταση των διωνυμικών συντελεστών, ο τύπος του Vandermonde γενικεύει τον τύπο του Cauchy και διατυπώνεται ως εξής:

Πρόταση 4.7 (Τύπος του Vandermonde με διωνυμικούς συντελεστές). *Για κάθε $x, y \in \mathbb{R}$ και $n \in \mathbb{N}^*$ ισχύει ότι*

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}.$$

Εφαρμογή 4.5.2. *Να υπολογισθούν τα αθροίσματα*

i) $S_1 = \sum_{k=0}^{n} \binom{2n}{k}\binom{m-n}{n-k}$

ii) $S_2 = \sum_{k=0}^{n} \binom{n}{k}\binom{3n}{2n+k}$

Λύση. Από τον τύπο του Vandermonde ισχύει ότι

i) $S_1 = \sum_{k=0}^{n} \binom{2n}{k}\binom{m-n}{n-k} = \binom{2n+m-n}{n} = \binom{n+m}{n}.$

ii) $S_2 = \sum_{k=0}^{n} \binom{n}{k}\binom{3n}{2n+k} = \sum_{k=0}^{n} \binom{n}{k}\binom{3n}{n-k} = \binom{3n+n}{n} = \binom{4n}{n}$. □

Επέκταση του τύπου του διωνύμου του Νεύτωνα

Πρόταση 4.8 (Επέκταση του τύπου του διωνύμου του Νεύτωνα).

$$(\alpha+\beta)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} \alpha^k \beta^{-n-k}$$

όπου $n \in \mathbb{N}^*$, $\frac{\alpha}{\beta} \in (-1,1)$ *και* $\beta \neq 0$.

Εφαρμογή 4.5.3. *Να δειχθεί ότι*

$$\binom{r+s+n-1}{n} = \sum_{k=0}^{n} \binom{r+k-1}{k}\binom{s+n-k-1}{n-k}$$

όπου $r, s, n \in \mathbb{N}^*$.

Απόδειξη. Με τη βοήθεια της επέκτασης του διωνύμου του Νεύτωνα για $\alpha = -x$ και $\beta = 1$, η σχέση

$$(1-x)^{-(r+s)} = (1-x)^{-r} \cdot (1-x)^{-s}$$

δίνει ισοδύναμα:

$$\begin{aligned}
\sum_{n=0}^{\infty} \binom{-(r+s)}{n} (-x)^n &= \left(\sum_{k=0}^{\infty} \binom{-r}{k}(-x)^k\right)\left(\sum_{\lambda=0}^{\infty} \binom{-s}{\lambda}(-x)^\lambda\right) \\
&= \sum_{n=0}^{\infty} (-1)^n \binom{-(r+s)}{n} x^n = \sum_{k=0}^{\infty}\sum_{\lambda=0}^{\infty} \binom{-r}{k}\binom{-s}{\lambda}(-1)^{k+\lambda} x^{k+\lambda} \\
&= \sum_{n=0}^{\infty} (-1)^n \binom{-(r+s)}{n} x^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} \binom{-r}{k}\binom{-s}{n-k}\right)(-1)^n x^n.
\end{aligned}$$

Άρα

$$(-1)^n \binom{-(r+s)}{n} = \sum_{k=0}^{n} \left((-1)^k \binom{-r}{k}\right)\left((-1)^{n-k}\binom{-s}{n-k}\right)$$

$$\binom{r+s+n-1}{n} = \sum_{k=0}^{n} \binom{r+k-1}{k}\binom{s+n-k-1}{n-k}.$$ □

4.6 Λυμένες ασκήσεις

Άσκηση 4.1. *Να δειχθεί ότι για κάθε $n \in \mathbb{N}^*$ ισχύει ότι*

$$\Delta^n g(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} g(x+n-k).$$

Απόδειξη. Θα αποδειχθεί με τη μέθοδο της επαγωγής. Για $n = 1$ ισχύει, διότι

$$\sum_{k=0}^{1} (-1)^k \binom{1}{k} g(x+1-k) = (-1)^0 \binom{1}{0} g(x+1-0) + (-1)^1 \binom{1}{1} g(x+1-1) = g(x+1) + g(x) = \Delta g(x).$$

Έστω ότι ισχύει για $n = m$, δηλαδή

$$\Delta^m g(x) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} g(x+m-k).$$

Θα αποδειχθεί ότι ισχύει και για $n = m+1$, δηλαδή

$$\Delta^{m+1} g(x) = \sum_{k=0}^{m+1} (-1)^k \binom{m+1}{k} g(x+m+1-k).$$

Πράγματι, από τον ορισμό της διαφοράς και την υπόθεση της επαγωγής ισχύει ότι

$$\Delta^{m+1} g(x) = \Delta(\Delta^m g(x)) = \Delta\Big(\sum_{k=0}^{m} (-1)^k \binom{m}{k} g(x+m-k)\Big).$$

Λόγω της γραμμικότητας του τελεστή Δ έπεται ότι

$$\begin{aligned}
&\Delta^{m+1} g(x) \\
&= \sum_{k=0}^{m} (-1)^k \binom{m}{k} \Delta g(x+m-k) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (g(x+m-k+1) - g(x+m-k)) \\
&= \sum_{k=0}^{m} (-1)^k \binom{m}{k} g(x+m-k+1) + \sum_{k=0}^{m} (-1)^{k+1} \binom{m}{k} g(x+m-k) \\
&= \sum_{k=0}^{m} (-1)^k \binom{m}{k} g(x+m-k+1) + \sum_{k=1}^{m+1} (-1)^k \binom{m}{k-1} g(x+m-k+1) \\
&= (-1)^0 \binom{m}{0} g(x+m-0+1) + \sum_{k=1}^{m} (-1)^k \left(\binom{m}{k} + \binom{m}{k-1} \right) g(x+m-k+1) + (-1)^{m+1} \binom{m}{m} g(x+m-(m+1)+1) \\
&= (-1)^0 \binom{m+1}{0} g(x+m-0+1) + \sum_{k=1}^{m} (-1)^k \binom{m+1}{k} g(x+m+1) + (-1)^{m+1} \binom{m+1}{m+1} g(x+m-(m+1)+1) \\
&= \sum_{k=0}^{m+1} (-1)^k \binom{m+1}{k} g(x+m+1-k),
\end{aligned}$$

αφού $\binom{m}{0} = \binom{m+1}{0} = 1 = \binom{m}{m} = \binom{m+1}{m+1}$ και $\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k}$. □

Άσκηση 4.2. *Να υπολογισθεί η τιμή του αθροίσματος*

$$S_n = 1^3 + 2^3 + \cdots + n^3, \text{ όπου } n \in \mathbb{N}^*.$$

Λύση. Αρχικά βρίσκουμε πολυώνυμο $p(x)$ τέτοιο ώστε

$$p(x+1) - p(x) = x^3, \text{ για κάθε } x \in \mathbb{R}. \tag{4.6}$$

Γνωρίζουμε ότι $x^3 = F_3(x) + 3F_2(x) + F_1(x)$.
Για να ισχύει η σχέση (4.6) πρέπει

$$\begin{aligned}\Delta p(x) &= F_3(x) + 3F_2(x) + F_1(x)\\ &= \frac{\Delta F_4(x)}{4} + 3\frac{\Delta F_3(x)}{3} + \frac{\Delta F_2(x)}{2}\\ &= \Delta(\frac{1}{4}F_4(x) + F_3(x) + \frac{F_2(x)}{2})\end{aligned}$$

Άρα, θα υπάρχει σταθερά $c \in \mathbb{R}$ τέτοια ώστε

$$\begin{aligned}p(x) &= \frac{1}{4}F_4(x) + F_3(x) + \frac{1}{2}F_2(x) + c\\ &= \frac{1}{4}x(x-1)(x-2)(x-3) + x(x-1)(x-2) + \frac{1}{2}x(x-1) + c\\ &= \frac{1}{4}(x(x-1))^2 + c.\end{aligned} \tag{4.7}$$

Από τις σχέσεις (4.6) και (4.7) προκύπτει ότι

$$\begin{aligned}S_n &= (p(2) - p(1)) + (p(3) - p(2)) + \cdots + (p(n+1) - p(n))\\ &= p(n+1) - p(1)\\ &= \frac{(n+1)^2n^2}{4} + c - (p(1) + c)\\ &= \frac{(n+1)^2n^2}{4},\end{aligned}$$

διότι $p(1) = 0$. □

Παρατήρηση. Με ανάλογο τρόπο βρίσκεται η τιμή του αθροίσματος

$$S_n = 1^k + 2^k + \cdots + n^k, \text{ όπου } n, k \in \mathbb{N}^*.$$

Άσκηση 4.3. *Να δειχθεί ότι για κάθε $x, y \in \mathbb{R}$ και $n \in \mathbb{N}^*$ ισχύει ότι*

$$F_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} F_k(x)F_{n-k}(y). \tag{4.8}$$

Απόδειξη. Η απόδειξη θα γίνει όταν η μια μεταβλητή εκ των x, y είναι θετικός αριθμός.
Έτσι υποθέτουμε ότι $x \in \mathbb{N}^*$ και θα δείξουμε με επαγωγή ως προς x τον τύπο (4.8).

Για $x = 1$ ο τύπος (4.8) γράφεται

$$\begin{aligned} F_n(y+1) &= \sum_{k=0}^{n} \binom{n}{k} F_k(1) F_{n-k}(y) \\ &= \binom{n}{0} 1 F_n(y) + \binom{n}{1} 1 F_{n-1}(y) \\ &= F_n(y) + n F_{n-1}(y). \end{aligned} \tag{4.9}$$

το οποίο ισχύει, αφού από την ιδιότητα 4 των παραγοντικών πολυωνύμων:

$$F_n(y+1) - F_n(y) = \Delta F_n(y) = n F_{n-1}(y).$$

Υποθέτουμε τώρα ότι ο τύπος (4.8) ισχύει για $x = \nu$, δηλαδή

$$F_n(\nu + y) = \sum_{k=0}^{n} \binom{n}{k} F_k(\nu) F_{n-k}(y) \tag{4.10}$$

και θα δειχθεί για $x = \nu + 1$, δηλαδή

$$F_n(\nu + 1 + y) = \sum_{k=0}^{n} \binom{n}{k} F_k(\nu + 1) F_{n-k}(y). \tag{4.11}$$

Πραγματικά, εφαρμόζοντας την (4.9) για $\nu + y$ αντί y προκύπτει ότι

$$F_n(\nu + 1 + y) = F_n(\nu + y) + n F_(n-1)(\nu + y).$$

Λόγω της (4.10) έχουμε

$$F_n(\nu + 1 + y) = \sum_{k=0}^{n} \binom{n}{k} F_k(\nu) F_{n-k}(y) + n \sum_{k=0}^{n-1} \binom{n-1}{k} F_k(\nu) F_{n-1-k}(y).$$

Χρησιμοποιώντας την ταυτότητα

$$n \binom{n-1}{k} = (k+1) \binom{n}{k+1}$$

προκύπτει ότι

$$F_n(\nu + 1 + y) = \sum_{k=0}^{n} \binom{n}{k} F_k(\nu) F_{n-k}(y) + \sum_{k=0}^{n-1} (k+1) \binom{n}{k+1} F_k(\nu) F_{n-1-k}(y).$$

Αν τεθεί $\lambda = k + 1$ τότε

$$\begin{aligned} F_n(\nu + 1 + y) &= \sum_{k=0}^{n} \binom{n}{k} F_k(\nu) F_{n-k}(y) + \sum_{\lambda=1}^{n} \lambda \binom{n}{\lambda} F_{\lambda-1}(\nu) F_{n-\lambda}(y) \\ &= \sum_{k=0}^{n} \binom{n}{k} F_k(\nu) F_{n-k}(y) + \sum_{k=0}^{n} k \binom{n}{k} F_{k-1}(\nu) F_{n-k}(y) \\ &= \sum_{k=0}^{n} \binom{n}{k} F_{n-k}(y)(F_k(\nu) + k F_{k-1}(\nu)). \end{aligned}$$

Λόγω της (4.9) προκύπτει ότι

$$F_n(\nu + 1 + y) = \sum_{k=0}^{n} \binom{n}{k} F_k(\nu + 1) F_{n-k}(y). \qquad \square$$

Άσκηση 4.4. *Να βρεθεί, με τη βοήθεια του τύπου του Gregory πολυώνυμο $p(x)$ τρίτου βαθμού ώστε*

$$p(0) = 6, \quad p(1) = -1, \quad p(2) = -6, \quad p(3) = 3.$$

Λύση. Από τον τύπο του Gregory προκύπτει ότι

$$p(x) = p(0) + \frac{\Delta p(0)}{1!}x + \frac{\Delta^2 p(0)}{2!}x(x-1) + \frac{\Delta^3 p(0)}{3!}x(x-1)(x-2). \tag{4.12}$$

Προκειμένου να βρεθούν οι διαφορές $\Delta^k p(0)$, $k = 1, 2, 3$ χρησιμοποιείται ο επόμενος πίνακας:

x	$p(x)$	$\Delta p(x)$	$\Delta^2 p(x)$	$\Delta^3 p(x)$
3	3			
2	−6	9		
1	−1	−5	14	
0	6	−7	2	12

Άρα, $\Delta p(0) = -7$, $\Delta^2 p(0) = 2$ και $\Delta^3 p(0) = 12$. Τότε από τη σχέση (4.12) προκύπτει ότι

$$\begin{aligned} p(x) &= 6 + \frac{(-7)}{1!}x + \frac{2}{2!}x(x-1) + \frac{12}{3!}x(x-1)(x-2) \\ &= 6 - 7x + x^2 - x + 2x^3 - 6x^2 + 4x \\ &= 2x^3 - 5x^2 - 4x + 6. \end{aligned}$$

□

Άσκηση 4.5. *Να βρεθεί ο συντελεστής του όρου $a^4\beta^8$ στο ανάπτυγμα του αθροίσματος $(a+\beta)^{12}$.*

Λύση. Από τον τύπο του διωνύμου του Νεύτωνα έχουμε ότι

$$(a+\beta)^{12} = \sum_{k=0}^{12} \binom{12}{k} a^{12-k}\beta^k.$$

Ο συντελεστής του όρου $a^{12-k}\beta^k$ είναι ο $\binom{12}{k}$.
Ο όρος $a^4\beta^8$ εμφανίζεται στο άθροισμα για $k = 8$.
Άρα ο αντίστοιχος συντελεστής είναι ο $\binom{12}{8} = \frac{12!}{8!4!} = \frac{9\cdot10\cdot11\cdot12}{1\cdot2\cdot3\cdot4} = 3\cdot5\cdot11\cdot3 = 495$. □

Άσκηση 4.6. *Να βρεθεί ο όρος που δεν περιέχει a στο ανάπτυγμα του αθροίσματος $(a^2 + \frac{1}{a})^9$.*

Λύση. Από τον τύπο του διωνύμου του Νεύτωνα έχουμε ότι

$$(a^2 + \frac{1}{\alpha})^9 = \sum_{k=0}^{9} \binom{9}{k} (a^2)^{9-k} (\frac{1}{\alpha})^k,$$

οπότε

$$\sum_{k=0}^{9} \binom{9}{k} (a^2)^{9-k} (\frac{1}{\alpha})^k = \sum_{k=0}^{9} \binom{9}{k} \alpha^{18-2k-k} = \sum_{k=0}^{9} \binom{9}{k} \alpha^{18-3k}.$$

Επομένως, ο όρος που δεν περιέχει a εμφανίζεται στο άθροισμα όταν $18 - 3k = 0$, δηλαδή $k = 6$. Άρα ο όρος που δεν περιέχει a ισούται με

$$\binom{9}{6} = \frac{9!}{6!3!} = \frac{9 \cdot 8 \cdot 7}{3 \cdot 2 \cdot 1} = 3 \cdot 4 \cdot 7 = 84. \qquad \square$$

Άσκηση 4.7. *Να υπολογισθεί το άθροισμα*

$$S_n = \sum_{k=0}^{n} \binom{n}{k} 2^k.$$

Λύση. Από τον τύπο του διωνύμου του Νεύτωνα για $a = 1$, $\beta = 2$ προκύπτει ότι

$$S_n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 2^k = (1 + 2)^n = 3^n. \qquad \square$$

Άσκηση 4.8. *Να υπολογισθεί το άθροισμα*

$$S_n = \sum_{k=0}^{n} k^2 \binom{n}{k}.$$

Λύση. (1 τρόπος). Με τη βοήθεια των τύπων

$$k\binom{n}{k} = n\binom{n-1}{k-1}, \qquad \sum_{k=0}^{n} \binom{n}{k} = 2^n, \qquad \sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$$

προκύπτει ότι

$$\begin{aligned} S &= \sum_{k=0}^{n} k \cdot k\binom{n}{k} = \sum_{k=1}^{n} k \cdot n\binom{n-1}{k-1} = n \sum_{k=0}^{n-1} (k+1)\binom{n-1}{k} = n \sum_{k=0}^{n-1} k\binom{n-1}{k} + n \sum_{k=0}^{n-1} \binom{n-1}{k} \\ &= n(n-1)2^{n-2} + n2^{n-1} = n2^{n-2}(n-1+2) = n(n+1)2^{n-2}. \end{aligned}$$

(2 τρόπος): Παραγωγίζοντας δύο φορές, από τον δυωνυμικό τύπο

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

προκύπτει ότι

$$n(1+x)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k x^{k-1}$$

και

$$n(n-1)(1+x)^{n-2} = \sum_{k=2}^{n} \binom{n}{k} k(k-1) x^{k-2}.$$

Θέτοντας $x = 1$ στις παραπάνω δύο σχέσεις, προκύπτει ότι

$$n2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k}$$

και

$$n(n-1)2^{n-2} = \sum_{k=2}^{n} k(k-1)\binom{n}{k}.$$

Προσθέτωντας κατά μέλη, προκύπτει ότι

$$\sum_{k=2}^{n} (k + k(k-1))\binom{n}{k} + \binom{n}{1} = n2^{n-1} + n(n-1)2^{n-2},$$

οπότε

$$S_n = \sum_{k=1}^{n} k^2 \binom{n}{k} = n(n+1)2^{n-2}.$$ □

Άσκηση 4.9. *Να υπολογισθούν τα αθροίσματα*

i) $\sum_{k=0}^{n} (7k+10)\binom{n}{k}$, *ii)* $\sum_{k=0}^{n} (3k^2 - 2k + 1)\binom{n}{k}$, *iii)* $\sum_{k=1}^{n} \frac{3k+7}{k+1}\binom{n}{k}$.

Λύση.

i) $$\sum_{k=0}^{n} (7k+10)\binom{n}{k} = 7\sum_{k=0}^{n} k\binom{n}{k} + 10\sum_{k=0}^{n}\binom{n}{k} = 7n \cdot 2^{n-1} + 10 \cdot 2^n = (7n+20)\cdot 2^{n-1}.$$

ii)

$$\begin{aligned}\sum_{k=0}^{n} (3k^2 - 2k + 1)\binom{n}{k} &= 3\sum_{k=0}^{n} k^2\binom{n}{k} + 2\sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n}\binom{n}{k} \\ &= 3n(n+1)2^{n-2} + 2n2^{n-1} + 2^n \\ &= (3n^2 + 3n + 4n + 4)\cdot 2^{n-2} \\ &= (3n^2 + 7n + 4)\cdot 2^{n-2}.\end{aligned}$$

iii)

$$\begin{aligned}\sum_{k=1}^{n}\frac{3k+7}{k+1}\binom{n}{k} &= \sum_{k=1}^{n}\frac{3(k+1)+4}{k+1}\binom{n}{k}\\ &= 3\sum_{k=1}^{n}\binom{n}{k}+4\sum_{k=1}^{n}\frac{1}{k+1}\binom{n}{k}\\ &= 3\left(\sum_{k=0}^{n}\binom{n}{k}-\binom{n}{0}\right)+4\left(\sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k}-\frac{1}{0+1}\binom{n}{0}\right)\\ &= 3\sum_{k=0}^{n}\binom{n}{k}-3+4\sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k}-4\\ &= 3\cdot 2^n+4\frac{2^{n+1}-1}{n+1}-7.\end{aligned}$$

□

Άσκηση 4.10. *Να υπολογισθεί το άθροισμα*

$$S=\sum_{k=0}^{n}\frac{1}{k+2}\binom{n}{k}.$$

Λύση. Ολοκληρώνοντας τη σχέση

$$x(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^{k+1}$$

προκύπτει ότι

$$\sum_{k=0}^{n}\binom{n}{k}\int_0^1 x^{k+1}\,dx=\int_0^1 x(1+x)^n\,dx$$

δηλαδή

$$\sum_{k=0}^{n}\binom{n}{k}\left[\frac{x^{k+2}}{k+2}\right]_0^1=\frac{1}{n+1}\int_0^1 x(1+x)^{n+1})'\,dx,$$

οπότε

$$\begin{aligned}S &= \frac{1}{n+1}\left[x(1+x)^{n+1}\right]_0^1-\frac{1}{n+1}\int_0^1 x'(1+x)^{n+1}\,dx\\ &= \frac{1}{n}2^{n+1}-\frac{1}{n+1}\left[\frac{(1+x)^{n+2}}{n+2}\right]_0^1\\ &= \frac{1}{n+1}2^{n+1}-\frac{1}{n+1}\frac{1}{n+2}(2^{n+1}-1)=\frac{n2^{n+1}-1}{(n+1)(n+2)}.\end{aligned}$$

□

Άσκηση 4.11. *Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι*

$$\sum_{k=0}^{n} \binom{2n+1}{k} = 4^n.$$

Λύση. Έστω $S_n = \sum_{k=0}^{n} \binom{2n+1}{k}$. Από τον τύπο του διωνύμου του Νεύτωνα ισχύει ότι

$$\begin{aligned}
\sum_{k=0}^{2n+1} \binom{2n+1}{k} = 2^{2n+1} &\Leftrightarrow \\
\sum_{k=0}^{n} \binom{2n+1}{k} + \sum_{k=n+1}^{2n+1} \binom{2n+1}{k} = 2^{2n+1} &\Leftrightarrow \\
S_n + \sum_{k=0}^{n} \binom{2n+1}{k+n+1} = 2^{2n+1} &\Leftrightarrow \\
S_n + \sum_{k=0}^{n} \binom{2n+1}{n-k} = 2^{2n+1} &\Leftrightarrow \\
S_n + \sum_{k=0}^{n} \binom{2n+1}{k} = 2^{2n+1} &\Leftrightarrow \\
2S_n = 2^{2n+1} \Leftrightarrow S_n = 2^{2n} = 4^n &
\end{aligned}$$

□

Άσκηση 4.12. *Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι*

$$\sum_{k=0}^{n} \binom{2n}{k}\binom{n}{n-k} = \binom{3n}{n}.$$

Λύση. Από τον τύπο του Cauchy ισχύει ότι

$$\sum_{k=0}^{n} \binom{2n}{k}\binom{n}{n-k} = \binom{2n+n}{n} = \binom{3n}{n}.$$

□

Άσκηση 4.13. *Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι*

$$\binom{-\frac{1}{2}}{n} = (-4)^{-n}\binom{2n}{n}.$$

Λύση.

$$\begin{aligned}
\binom{-\frac{1}{2}}{n} &= \frac{\left(-\frac{1}{2}\right)\left(-\frac{1}{2}-1\right)\cdots\left(-\frac{1}{2}-n+1\right)}{n!} \\
&= (-1)^n \frac{\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdots\frac{2n-1}{2}}{n!} \\
&= (-1)^n \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2^n n!} \\
&= (-1)^n \frac{1\cdot 3\cdot 5\cdots(2n-1)\cdot 2^n n!}{2^n n!\cdot 2^n n!} \\
&= (-1)^n \frac{(2n)!}{4^n n! n!} = (-4)^{-n}\binom{2n}{n}.
\end{aligned}$$

□

4.7 Ασκήσεις προς επίλυση

1) Να δειχθεί ότι

   i) $\Delta(f(x)g(x)) = f(x)\Delta g(x) + g(x+1)\Delta f(x)$.

   ii) $\Delta\left(\dfrac{f(x)}{g(x)}\right) = \dfrac{g(x)\Delta f(x) - f(x)\Delta g(x)}{g(x)g(x+1)}$.

2) Να δειχθεί ότι

$$\Delta^2 \ln x = \ln\left(1 - \frac{1}{(1+x)^2}\right), \text{ για κάθε } x \in (0, +\infty).$$

3) Να δειχθεί ότι

$$\Delta^n e^x = e^x(e-1)^n \text{ για κάθε } n \in \mathbb{N}^*.$$

4) Έστω $p(x)$ πολυώνυμο βαθμού n. Να δειχθεί ότι

   i) $\Delta^k x^n = 0$, για κάθε $k > n$.

   ii) $\Delta^k p(x) = 0$, για κάθε $k > n$.

   iii) $\Delta^k p(x)$ είναι ένα πολυώνυμο του x βαθμού $n-k$ για κάθε $k \leq n$.

5) Να βρεθεί πολυώνυμο $p(x)$ τέτοιο ώστε

   i) $p(x+1) - p(x) = x$ για κάθε $x \in \mathbb{R}$ και $p(1) = 0$.

   ii) $p(x+1) - p(x) = (3x-7)x$, για κάθε $x \in \mathbb{R}$ και $p(1) = 3$.

   iii) $p(x+1) - p(x) = x^3$ για κάθε $x \in \mathbb{R}$ και $p(1) = 0$.

   iv) $p(x+1) - p(x) = x^4 + 1$ για κάθε $x \in \mathbb{R}$ και $p(1) = 0$.

   v) $p(x+1) - p(x) = (x+1)(x+3)(x+5)$ για κάθε $x \in \mathbb{N}^*$ και $p(0) = 10$.

   vi) $p(x+1) - p(x) = (x+5)(x+4)(x+3)$ για κάθε $x \in \mathbb{R}$ και $p(1) = 0$.

6) Να υπολογισθούν οι τιμές του αθροισμάτων

   i) $S_n = 1\cdot 3\cdot 5 + 3\cdot 5\cdot 7 + \cdots + (2n-1)(2n+1)(2n+3)$, όπου $n \in \mathbb{N}^*$.

   ii) $S_n = 1^2\cdot 2 + 2^2\cdot 3 + \cdots + n^2(n+1)$, όπου $n \in \mathbb{N}^*$.

   iii) $S_n = 1^2 + 3^2 + 5^2 + \cdots + (2n+1)^2$, όπου $n \in \mathbb{N}$.

7) Να βρεθεί, με τη βοήθεια του τύπου του Gregory,

   i) πολυώνυμο $p(x)$ τρίτου βαθμού, τέτοιο ώστε

$$p(0) = 0,\ \Delta p(0) = 5,\ \Delta^2 p(0) = 8,\ \Delta^3 p(0) = 6.$$

   ii) πολυώνυμο $p(x)$ τρίτου βαθμού, τέτοιο ώστε

$$p(0) = 8, \quad p(1) = -2, \quad p(2) = -6, \text{ και } p(3) = 14.$$

   iii) πολυώνυμο $p(x)$ ώστε

$$p(0) = 5,\ p(1) = 13,\ p(2) = 25,\ p(3) = 83,\ p(4) = 277,\ p(5) = 745,$$
$$p(6) = 1673,\ p(7) = 3295,\ p(8) = 5893,\ p(9) = 9797,\ p(10) = 15385.$$

   Τί βαθμού είναι το πολυώνυμο $p(x)$;

8) Να δειχθεί ότι
$$\Delta^{\nu} F_k(x) = F_{\nu}(k) F_{k-\nu}(x), \text{ για κάθε } \nu, k \in \mathbb{N}^* \text{ με } \nu \leq k.$$

9) Να δειχθεί ότι
$$F_n(y) = (-1)^n F_n(n - y - 1)$$
για κάθε $y \in \mathbb{R}$ και $n \in \mathbb{N}^*$.

10) Να δειχθεί ότι
$$F_n(x + y) = F_k(x + y) F_{n-k}(x + y - k)$$
για κάθε $x, y \in \mathbb{R}$ και $n, k \in \mathbb{N}^*$ με $k \leq n$.

11) Να δειχθεί ότι
$$\frac{F_n(y)}{F_n(x + y)} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{F_k(x)}{F_k(x + y)}$$
για κάθε $n \in \mathbb{N}^*$ και $x, y \in \mathbb{R}$ με $x + y \neq 0, 1, 2, \ldots, n - 1$.

12) Να δειχθεί με τη βοήθεια του τύπου του Vandermonde η σχέση
$$\frac{F_n(x + y + n)}{F_n(y + n)} = \sum_{k=0}^{n} \binom{n}{k} \frac{F_k(x)}{F_k(y + k)}$$
για κάθε $n \in \mathbb{N}^*$ και $x, y \in \mathbb{R}$ με $y \neq -1, -2, \ldots, -n$.

13) Να δειχθούν με τη βοήθεια της προηγούμενης άσκησης οι σχέσεις:

(i) $\displaystyle\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \frac{x}{x - k} = \frac{1}{\binom{x-1}{n}}$, για $x \neq 1, 2, \ldots, n$.

(ii) $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{y}{y + k} = \frac{1}{\binom{y+k}{n}}$, για $y \neq -1, -2, \ldots, -n$.

14) i) Να βρεθεί ο συντελεστής του όρου $a^6\beta^8$ στο ανάπτυγμα του αθροίσματος $(a + \beta)^{14}$.
ii) Να βρεθεί ο συντελεστής του όρου $a\beta^{333}$ στο ανάπτυγμα του αθροίσματος $(a + \beta)^{334}$.
iii) Να βρεθεί ο συντελεστής του σταθερού όρου στο ανάπτυγμα της παράστασης $(x + \frac{1}{x^2})^{30}$.
iv) Να βρεθεί ο συντελεστής του όρου a^{15} στο ανάπτυγμα του αθροίσματος $(a + \beta)^{100}$.

15) Να βρεθεί ο συντελεστής του x^k στο ανάπτυγμα των επόμενων εκφράσεων:

i) $(1 + 2x - 3x^2)^8$, όπου $k = 9$.
ii) $(1 - x + 2x^2)^{10}$, όπου $k = 7$.
iii) $(2 + x - 2x^3)^{20}$, όπου $k = 10$.
iv) $(2 + x^4 + x^7)^{15}$, όπου $k = 17$.

16) Να βρεθεί ο αριθμός των ρητών όρων στο ανάπτυγμα των επόμενων εκφράσεων:

i) $\left(\sqrt{2} + \sqrt[3]{3}\right)^{20}$.
ii) $\left(\sqrt{3} + \sqrt[4]{5}\right)^{50}$.
iii) $\left(\sqrt[3]{6} + \sqrt[4]{2}\right)^{100}$.
iv) $\left(\sqrt[3]{12} + \sqrt[6]{3}\right)^{30}$.

17) Να αποδειχθούν οι τύποι $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$ και $\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}$ δια παραγωγίσεως και ολοκληρώσεως αντίστοιχα του $(1+x)^n$, και εφαρμογής του διωνύμου του Νεύτωνα.

18) Να υπολογισθούν τα αθροίσματα:

i) $\sum_{k=0}^{n}(3k+5)\binom{n}{k}$.

ii) $\sum_{k=0}^{n}(2k^2-k+3)\binom{n}{k}$.

iii) $\sum_{k=1}^{n}\frac{2k+5}{k+1}\binom{n}{k}$.

iv) $\sum_{k=0}^{n}\frac{1}{(k+1)(k+2)}\binom{n}{k}$.

19) Να δειχθεί ότι

$$\sum_{k=1}^{n} k\binom{r}{k}\binom{s}{n-k} = r\binom{r+s-1}{n-1}, \text{ όπου } r,s \in \mathbb{N}^*.$$

και

$$\sum_{k=1}^{n} k\binom{n}{k}^2 = (2n-1)\binom{2n-2}{n-1}.$$

(Υπόδειξη: Να χρησιμοποιηθεί ο τύπος $k\binom{r}{k} = r\binom{r-1}{k-1}$.)

20) Να δειχθεί, με τη βοήθεια της επέκτασης του διώνυμου του Νεύτωνα, ότι

$$\binom{r+s+1}{n} = \sum_{k=0}^{n}\binom{r+k}{k}\binom{s-k}{n-k}$$

για κάθε $r,s,n \in \mathbb{N}^*$ με $s \geq n$.

21) Να δειχθεί ότι

i) $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$.

ii) $\sum_{k=m}^{n}\binom{n}{k}\binom{k}{m} = \binom{n}{m}2^{n-m}$.

iii) $\sum_{k=0}^{m}\binom{n+k}{m}\binom{m}{k} = \sum_{k=0}^{m}\binom{n}{k}\binom{m}{k}2^k$.

22) Να δειχθεί ότι $\sum_{k=0}^{m}(-1)^k\binom{n}{k} = (-1)^m\binom{n-1}{m}$, για κάθε $m \in \mathbb{N}$ και $n \in \mathbb{N}^*$.

23) Να δειχθεί ότι για κάθε $n,k \in \mathbb{N}^*$ ισχύει ότι

$$\left(\binom{n+1}{k+1} - \binom{n}{k}\right)\binom{n-1}{k-1} = k\left(\binom{n}{k}^2 - \binom{n+1}{k+1}\binom{n-1}{k-1}\right).$$

24) Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι

$$\sum_{k=0}^{\left[\frac{n}{2}\right]}(-3)^k\binom{n}{2k} = (-1)^n 2^n \cos\frac{2\pi n}{3}.$$

(Υπόδειξη: Να χρησιμοποιηθεί η ισότητα $\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^n = \left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right)^n = \cos\frac{2\pi n}{3}+i\sin\frac{2\pi n}{3}$ και να εξισωθούν το πραγματικό και το φανταστικό μέρος του αναπτύγματος του αριστερού μέλους και το πραγματικό και φανταστικό μέρος του δεξιού μέλους.)

∗25) Να δειχθεί ότι για κάθε $n \in \mathbb{N}^*$ ισχύει ότι

$$\sum_{k=1}^{n} \frac{\binom{n-1}{k-1}}{\binom{2n-1}{k}} = \frac{2}{n+1}.$$

26) Να δειχθεί ότι

i) $\binom{n}{k} = \frac{n}{n-k}\binom{n-1}{k}$, για κάθε $n \in \mathbb{N}^*$ και $k \in \mathbb{N}$ με $n \neq k$.

ii) $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$, για κάθε $n \in \mathbb{N}$ και $k \in \mathbb{N}^*$.

27) Να βρεθούν οι τιμές των παρακάτω γενικευμένων διωνυμικών συντελεστών:

$$\binom{-1}{2}, \binom{3/2}{3}, \binom{-2}{3} \text{ και } \binom{3.2}{0}.$$

28) Να εκφραστούν οι γενικευμένοι διωνυμικοί συντελεστές $\binom{\frac{1}{2}}{n}$ και $\binom{-n}{n}$ με τη βοήθεια παραγοντικών που περιλαμβάνουν μόνο θετικούς ακεραίους

Κεφάλαιο 5

Στοιχεία θεωρίας αριθμών

5.1 Διαιρετότητα

5.1.1 Ο αλγόριθμος της διαίρεσης

Η επόμενη πρόταση είναι η βάση όλων των επόμενων αποτελεσμάτων.

Πρόταση 5.1 (Αλγόριθμος της διαίρεσης). *Έστω a, b φυσικοί αριθμοί με $a \geq b > 0$. Τότε υπάρχουν μοναδικοί φυσικοί αριθμοί π και υ ώστε*

$$a = \pi b + \upsilon, \text{ όπου } 0 \leq \upsilon < b. \tag{5.1}$$

Απόδειξη. Πρώτα θα δείξουμε ότι υπάρχουν φυσικοί αριθμοί π, υ που ικανοποιούν τη σχέση (5.1).

Έστω $S = \{a - kb : a - kb \geq 0 \text{ και } k \in \mathbb{N}\}$ δηλαδή S είναι το σύνολο των μη αρνητικών ακεραίων αριθμών της μορφής $a - kb$, όπου $k \in \mathbb{N}$.

Για $k = 1$ ισχύει ότι $a - 1 \cdot b \geq 0$, άρα το S είναι μη κενό. Επομένως, από την αρχή της καλής διάταξης[1] το S έχει ελάχιστο στοιχείο. Έστω υ το ελάχιστο στοιχείο του S και π η τιμή του k ώστε $\upsilon = a - \pi b \Leftrightarrow a = \pi b + \upsilon$. Τότε, αφενός

$$a - \pi b = \upsilon \in S, \text{ οπότε } \upsilon \geq 0$$

και αφετέρου το π είναι η μέγιστη τιμή του k ώστε $a - kb \in S$ δηλαδή

$$a - (\pi + 1)b = \upsilon - b \notin S, \text{ οπότε } \upsilon - b < 0.$$

Επομένως, η σχέση (5.1) ισχύει.

Στη συνέχεια θα δείξουμε ότι οι αριθμοί π, υ είναι μοναδικοί. Έστω ότι για τους φυσικούς αριθμούς π' και υ' ισχύει ότι

$$a = \pi' b + \upsilon' \text{ όπου } 0 \leq \upsilon' < b.$$

Διακρίνουμε δύο περιπτώσεις: Αν $\pi' < \pi$ έχουμε ότι

$$\pi' \leq \pi - 1 \Leftrightarrow -\pi' \geq -(\pi - 1) \Leftrightarrow -\pi' b \geq -(\pi - 1)b \Leftrightarrow a - \pi' b \geq a - (\pi - 1)b \Leftrightarrow \upsilon' \geq \upsilon + b$$

Άρα, $\upsilon' \geq b$, άτοπο.

Ομοίως, αν $\pi' > \pi$ έχουμε ότι

$$a - \pi b \geq a - (\pi' - 1)b \Leftrightarrow \upsilon \geq \upsilon' + b$$

Άρα, $\upsilon \geq b$, άτοπο. Επομένως, $\pi = \pi'$ και $\upsilon = \upsilon'$, δηλαδή οι αριθμοί π, υ είναι μοναδικοί. □

[1] Αρχή της καλής διάταξης: Κάθε μη κενό σύνολο φυσικών αριθμών έχει ελάχιστο στοιχείο.

Η Πρόταση 5.1 γενικεύεται άμεσα ως εξής:

Πρόταση 5.2. *Αν a είναι ακέραιος και b είναι μη μηδενικός ακέραιος, τότε υπάρχουν μοναδικοί ακέραιοι π και υ ώστε*

$$a = \pi b + \upsilon, \text{ όπου } 0 \leq \upsilon < |b|. \tag{5.2}$$

Απόδειξη. Άσκηση. □

Παρατηρήσεις.

1. Οι προτάσεις αυτές αντιστοιχούν στην γνωστή διαίρεση του αριθμού a από τον αριθμό b. Ο αριθμός π ονομάζεται **πηλίκο** και ο αριθμός υ ονομάζεται **υπόλοιπο** της διαίρεσης του a από τον b.

2. **Προσοχή!** Το υπόλοιπο της διαίρεσης υ είναι πάντα μη αρνητικός αριθμός φραγμένος από το 0 και το $|b| - 1$.

3. Ο b **διαιρεί** τον a αν το υπόλοιπο υ είναι 0, δηλαδή $a = \pi b$. Στην περίπτωση αυτή γράφουμε $\mathbf{b \mid a}$ και λέμε ότι ο b είναι **διαιρέτης** του a, ενώ ο a είναι **πολλαπλάσιο** του b. (Ο συμβολισμός $a \mid b$ δεν πρέπει να συγχέεται με τον συμβολισμό a/b που εκφράζει το κλάσμα με αριθμητή τον a και παρονομαστή τον b.) Στη περίπτωση όπου $b \neq a$, ο b ονομάζεται **γνήσιος διαιρέτης** του a. Στην περίπτωση που το υπόλοιπο υ είναι μη μηδενικό, δηλαδή δεν υπάρχει φυσικός αριθμός k που επαληθεύει την εξίσωση $a = kb$ λέμε ότι ο b **δεν διαιρεί** τον a και γράφουμε $\mathbf{b \nmid a}$.

   Για παράδειγμα, έστω $b = 13$.

   Αν $a = 26$, έχουμε

   $$26 = 2 \cdot 13 + 0,$$

   οπότε $\pi = 2$ και $\upsilon = 0$. Επίσης, $13 \mid 26$.

   Αν $a = 17$, έχουμε

   $$17 = 1 \cdot 13 + 4,$$

   οπότε $\pi = 1$ και $\upsilon = 4$. Επίσης, $13 \nmid 17$.

   Αν $a = 8$, έχουμε

   $$8 = 0 \cdot 13 + 8,$$

   οπότε $\pi = 0$ και $\upsilon = 8$. Επίσης, $13 \nmid 8$.

   Αν $a = -39$, έχουμε

   $$-39 = (-3) \cdot 13 + 0,$$

   οπότε $\pi = -3$ και $\upsilon = 0$. Επίσης, $13 \mid (-39)$.

   Τέλος, αν $a = -20$, έχουμε

   $$-20 = (-2) \cdot 13 + 6,$$

   οπότε $\pi = -2$ και $\upsilon = 6$. Επίσης, $13 \nmid -20$.

   Στην περίπτωση που $\upsilon = 0$ η διαίρεση ονομάζεται **τέλεια**, ενώ αν $\upsilon \neq 0$ τότε η διαίρεση ονομάζεται **ατελής**.

4. Η Πρόταση 5.1 και η γενίκευσή της ονομάζεται **αλγόριθμος διαίρεσης**, αν και η εκφώνησή της δεν δίνει κάποια μέθοδο υπολογισμού των π, υ. Όμως, ακολουθώντας την ιδέα της απόδειξης, μπορούμε να προσδιορίσουμε τα π, υ θεωρώντας επαναληπτικά τα στοιχεία της ακολουθίας $a - kb$, για $k = 1, 2, \ldots$, (αντίστοιχα $k = -1, -2, \ldots$) ώσπου η ακολουθία να πάρει τιμές μεταξύ του 0 και του $|b| - 1$ για $a \geq 0$ (αντίστοιχα $a \leq 0$).

   Για παράδειγμα, αν $a = 37$ και $b = 11$, τότε έχουμε

$$37 - 1 \cdot 11 = 26, \;\; 37 - 2 \cdot 11 = 15, \;\; 37 - 3 \cdot 11 = 4.$$

   Άρα, $\pi = 3$ και $\upsilon = 4$.

Χρησιμοποιώντας την Πρόταση 5.1 και την γενίκευσή της, εύκολα αποδεικνύονται οι επόμενες ιδιότητες, όπου a, b, c ακέραιοι, και $a \neq 0$.

1. $a \mid 0$ και $a \mid a$ (δηλαδή, οι μη μηδενικοί ακέραιοι αριθμοί διαιρούν το 0 και τον εαυτό τους).

2. $1 \mid b$ για κάθε b, (δηλαδή, το 1 διαιρεί κάθε ακέραιο αριθμό).

3. Αν $a \mid b$ και $a \mid c$, τότε $a \mid (b + c)$.

4. Αν $a \mid b$ και $a \nmid c$, τότε $a \nmid (b + c)$.

5. Αν $a \mid b$, τότε $a \mid bc$.

6. Αν $a \mid b$ και $b \mid c$, τότε $a \mid c$, (για $b \neq 0$).

7. Αν $a \mid b$ και $a \mid c$, τότε $a \mid (bx + cy)$ για οποιουσδήποτε ακέραιους x, y.

8. Αν $b > 0$ και $a \mid b$, τότε $a \leq b$.

9. Αν $a \mid b$, τότε $|a| \leq |b|$.

10. Αν $a \mid b$ και $b \mid a$, τότε $|a| = |b|$, (για $b \neq 0$).

11. Αν $a \mid b$ τότε $-a \mid b$, $a \mid -b$ και $a \mid |b|$.

Παρατηρήσεις.

1. Δεν ισχύει το αντίστροφο της ιδιότητας 3, δηλαδή αν $a \mid (x + y)$ τότε **δεν** ισχύει παντα ότι $a \mid x$ και $a \mid y$. Για παράδειγμα $3 \mid (7 + 2)$ αλλά $3 \nmid 7$ και $3 \nmid 2$.

2. Δεν ισχύει το αντίστροφο της ιδιότητας 6, δηλαδή αν $a \mid bc$ τότε **δεν** ισχύει πάντα ότι $a \mid b$ και $a \mid c$. Για παράδειγμα $6 \mid 36 = 4 \cdot 9$ αλλά $6 \nmid 4$ και $6 \nmid 9$.

   Επιπλέον, αν $ab \nmid x$, τότε **δεν** ισχύει πάντα ότι $a \nmid x$ και $b \nmid x$. Για παράδειγμα: $3 \cdot 3 = 9 \nmid 21$ αλλά $3 \mid 21$.

5.1.2 Μέγιστος κοινός διαιρέτης

Έστω a, b φυσικοί αριθμοί. Ο **μέγιστος κοινός διαιρέτης** (μκδ) των a και b είναι ο μεγαλύτερος φυσικός αριθμός ο οποίος διαιρεί και τους δύο αριθμούς και συμβολίζεται με μκδ(a, b), ή $\gcd(a, b)$. (Επίσης, αρκετά συνηθισμένος είναι και ο συμβολισμός (a, b) ο οποίος δεν πρέπει να συγχέεται με τον συμβολισμό των διατεταγμένων ζευγών.)

Για παράδειγμα, ο μέγιστος κοινός διαιρέτης των $12, 18$ είναι το 6, διότι οι διαιρέτες του 12 είναι οι 1, 2, 3, 4, 6, 12, ενώ οι διαιρέτες του 18 είναι οι 1, 2, 3, 6, 9, 18, οι κοινοί διαιρέτες τους είναι το 1, 2, 3, 6, και ο μέγιστος από αυτούς είναι το 6, συμβολικά $\gcd(12, 18) = 6$. Επίσης, ο μέγιστος κοινός διαιρέτης των $12, 7$ είναι το 1, συμβολικά $\gcd(12, 7) = 1$. Τέλος, ο μέγιστος κοινός διαιρέτης των $12, 4$ είναι το 4, συμβολικά $\gcd(12, 4) = 4$.

Παρατηρήσεις.

1. Ο μέγιστος κοινος διαιρέτης των a και b είναι ο μέγιστος θετικός ακέραιος d που ικανοποιεί τις παρακάτω δύο ιδιότητες:

   i) $d \mid a$ και $d \mid b$, και

   ii) Αν $c \mid a$ και $c \mid b$, τότε $c \mid d$.

2. Αν $d \mid a$, τότε $\gcd(a, d) = d$.

3. Όταν $\gcd(a, b) = 1$, λέμε ότι οι a και b είναι **πρώτοι προς αλλήλους** ή (**σχετικά**) **πρώτοι μεταξύ τους**.

4. Αν $\gcd(a, b) = d$ τότε $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, δηλαδή αν διαιρέσουμε δύο αριθμούς με τον μέγιστο κοινό διαιρέτη τους οι αριθμοί που προκύπτουν είναι πρώτοι μεταξύ τους.

5. Για τον μκδ δύο ή περισσοτέρων ακέραιων αριθμών $a_1, \ldots, a_{n-1}, a_n$ ισχύει ότι

$$\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n).$$

6. Αν $a = \pi b + \upsilon$ τότε $\gcd(a, b) \mid \upsilon$ και $\gcd(b, \upsilon) \mid a$. Η ιδιότητα αυτή είναι η βάση του αλγόριθμου του Ευκλείδη, που παρουσιάζεται στην επόμενη ενότητα.

Η επόμενη πρόταση είναι ένα αποτέλεσμα το οποίο χρησιμοποιείται σε πολλές άλλες προτάσεις όπου εμφανίζεται ο μέγιστος κοινός διαιρέτης δύο αριθμών.

Πρόταση 5.3. *Έστω a, b ακέραιοι αριθμοί, όχι και οι δύο μηδέν. Τότε υπάρχουν (όχι κατ' ανάγκη μοναδικοί) ακέραιοι s και t τέτοιοι ώστε*

$$\gcd(a, b) = sa + tb.$$

Επιπλέον, ο μκδ των a, b είναι ο ελάχιστος θετικός ακέραιος που εκφράζεται ως γραμμικός συνδυασμός των a, b.

Απόδειξη. Έστω

$$S = \{ax + by : ax + by > 0 \text{ και } x, y \in \mathbb{Z}\},$$

δηλαδή, S είναι το σύνολο των θετικών γραμμικών συνδυασμών των a και b.

Επειδή $S \neq \emptyset$ και $S \subseteq \mathbb{N}$ έπεται ότι το S έχει ελάχιστο στοιχείο, το οποίο ας συμβολίσουμε με d. Θα αποδείξουμε ότι $d = \gcd(a, b)$.

Επειδή $d \in S$, έπεται ότι υπάρχουν $x_0, y_0 \in \mathbb{Z}$ ώστε $ax_0 + by_0 = d$. Επειδή $\gcd(a, b) \mid a$ και $\gcd(a, b) \mid b$, προκύπτει ότι $\gcd(a, b) \mid (ax_0 + by_0)$, άρα $\gcd(a, b) \mid d$, οπότε $\gcd(a, b) \leq d$.

Στη συνέχεια θα αποδείξουμε ότι ο d είναι κοινός διαιρέτης των a, b δηλαδή $d \mid a$ και $d \mid b$. Πράγματι, έστω $a = \pi d + \upsilon$, με $0 \leq \upsilon < d$. Έχουμε ότι

$$\begin{aligned} ax_0 + by_0 = d \Leftrightarrow \\ a\pi x_0 + b\pi y_0 = \pi d \Leftrightarrow \\ a\pi x_0 + b\pi y_0 = a - \upsilon \Leftrightarrow \\ a(1 - \pi x_0) + b(-\pi y_0) = \upsilon. \end{aligned}$$

Αν $\upsilon \neq 0$, τότε $\upsilon > 0$ και άρα $\upsilon \in S$, το οποίο είναι άτοπο, αφού $\min S = d$. Άρα $\upsilon = 0$, δηλαδή $d \mid a$. Ομοίως, αποδεικνύεται ότι $d \mid b$. Άρα $d \leq \gcd(a, b)$.

Συνδυάζοντας τις δύο ανισότητες που συνδέουν τον d και τον $\gcd(a, b)$ προκύπτει το ζητούμενο, δηλαδή ότι $d = \gcd(a, b)$. □

Παρατήρηση. Μόλις αποδείξαμε όχι μόνο ότι ο $\gcd(a, b)$ γράφεται ως γραμμικός συνδυασμός των a, b, αλλά επιπλέον ότι είναι και ο μικρότερος θετικός φυσικός αριθμός που μπορεί να γραφεί με αυτόν τον τρόπο.

Για παράδειγμα, αν $a = 18$ και $b = 12$, τότε $\gcd(18, 12) = 6$. Ισχύει ότι

$$6 = 1 \cdot 18 + (-1) \cdot 12$$

άρα $s = 1$ και $t = -1$.

Αν $a = 12$ και $b = 7$, τότε $\gcd(12, 7) = 1$. Ισχύει ότι

$$1 = 3 \cdot 12 + (-5) \cdot 7$$

άρα $s = 3$ και $t = -5$.

Παρατήρηση. Οι ακέραιοι s και t για τους οποίους $\gcd(a, b) = as + bt$ δεν είναι μοναδικοί. Πράγματι, αν $\gcd(a, b) = as + bt$, τότε για κάθε $k \in \mathbb{Z}$ έχουμε ότι

$$\gcd(a, b) = (s + kb)a + (t - ka)b.$$

Για παράδειγμα, επειδή

$$1 = 3 \cdot 12 + (-5) \cdot 7,$$

θα είναι

$$1 = (3 + 7k) \cdot 12 + (-5 - 12k) \cdot 7, \text{ για κάθε } k \in \mathbb{Z}.$$

Έτσι, για $k = 1$ προκύπτει ότι

$$1 = 10 \cdot 12 + (-17) \cdot 7.$$

5.1.3 Λυμένες ασκήσεις

Η βασική γνώση για την επίλυση προβλημάτων σχετικά με τον μκδ δύο αριθμών είναι η Πρόταση 5.3 και η απόδειξή της.

Στα επόμενα ισχύει ότι $a, b, c \in \mathbb{N}$.

Άσκηση 5.1. *Να δειχθεί ότι αν* $d = \gcd(a, b)$, *τότε* $d \mid (xa + yb)$ *για κάθε* $x, y \in \mathbb{Z}$.

Λύση. Έστω $d = \gcd(a, b)$. Τότε υπάρχουν $k_1, k_2 \in \mathbb{N}$ ώστε $a = k_1 d$ και $b = k_2 d$, οπότε $xa + yb = (xk_1 \pm yk_2)d$ και, άρα $d \mid (xa + yb)$. □

Άσκηση 5.2. *Να δειχθεί ότι για κάθε* $n \in \mathbb{N}$ *ισχύει ότι* $\gcd(6n + 5, 7n + 6) = 1$.

Λύση. Αν $d = \gcd(6n+5, 7n+6)$, έπεται ότι $d \mid (7(6n+5)+(-6)(7n+6))$, δηλαδή $d \mid 1$, οπότε $d = 1$. □

Άσκηση 5.3. *Να δειχθεί ότι αν* $\gcd(a, b) = 1$, *τότε* $\gcd(3a + 5b, 8a + 13b) = 1$.

Λύση. Αν $d = \gcd(3a+5b, 8a+13b)$, έπεται ότι $d \mid (8(3a+5b)+(-3)(8a+13b)) = b$ και $d \mid ((-13)(3a+5b)+5(8a+13b) = a$, οπότε $d \mid \gcd(a, b) = 1$, επομένως $d = 1$, άρα $\gcd(3a + 5b, 8a + 13b) = 1$. □

Άσκηση 5.4. *Να δειχθεί ότι κάθε φυσικός αριθμός* $n > 6$ *μπορεί να γραφεί ως άθροισμα δύο φυσικών αριθμών, μεγαλύτερων της μονάδας, οι οποίοι είναι πρώτοι μεταξύ τους.*

Λύση. Διακρίνουμε δύο περιπτώσεις:

Αν n είναι περιττός, τότε $n = 2k + 1$, όπου $k \geq 3$, οπότε

$$n = k + (k + 1)$$

με $\gcd(k, k + 1) = 1$ και $k, k + 1 > 1$.

Αν n είναι άρτιος, τότε $n = 2k$, όπου $k \geq 4$.

Διακρίνουμε επιπλέον δύο υποπεριπτώσεις για το k.

i) Αν k είναι άρτιος, τότε $k = 2m$, όπου $m \geq 2$, δηλαδή $n = 4m$, οπότε

$$n = (2m - 1) + (2m + 1).$$

Αν $d = \gcd(2m + 1, 2m - 1)$ τότε $d \mid ((2m + 1) - (2m - 1))$, οπότε $d \mid 2$. Όμως $d \neq 2$, αφού οι $2m + 1$, $2m - 1$ είναι περιττοί, οπότε $d = 1$. Άρα $\gcd(2m + 1, 2m - 1) = 1$ και $2m + 1, 2m - 1 > 1$.

ii) Αν k είναι περιττός, τότε $k = 2m + 1$, όπου $m \geq 2$, δηλαδή $n = 4m + 2$, οπότε

$$n = 2m + 3 + 2m - 3.$$

Αν $d = \gcd(2m + 3, 2m - 1)$ τότε $d \mid ((2m + 3) - (2m - 1))$, οπότε $d \mid 4$, Όμως, όπως και πριν, οι $2m+3$, $2m-1$ είναι περιττοί, οπότε $d = 1$. Άρα $\gcd(2m+3, 2m-1) = 1$ και $2m+3, 2m-1 > 1$. □

Άσκηση 5.5. *Να δειχθεί ότι* $\gcd(a, b) = \gcd(a, a - b)$.

Λύση. Έστω $S_1 = \{xa+yb : x, y \in \mathbb{Z} \text{ και } xa+yb > 0\}$ και $S_2 = \{sa+t(a-b) : s, t \in \mathbb{Z} \text{ και } sa+y(a-b) > 0\}$.
Από την Πρόταση 5.3 ισχύει ότι $\min S_1 = \gcd(a, b)$ και $\min S_2 = \gcd(a, a-b)$.
Έστω $d_1 = \gcd(a, b)$ και $d_2 = \gcd(a, a-b)$. Τότε υπάρχουν $x, y, s, t \in \mathbb{Z}$ ώστε

$$xa + yb = d_1$$

και

$$sa + t(a-b) = d_2.$$

Από την πρώτη ισότητα προκύπτει ότι

$$(x+y)a + (-y)(a-b) = d_1,$$

οπότε, επειδή $d_1 > 0$, έπεται ότι $d_1 \in S_2$, οπότε $d_1 \geq d_2 = \min S_2$.
Από την δεύτερη ισότητα προκύπτει ότι

$$(s+t)a + (-t)b = d_2,$$

οπότε, επειδή $d_2 > 0$, έπεται ότι $d_2 \in S_1$, οπότε $d_2 \geq d_1 = \min S_1$.
Συνεπώς $d_1 = d_2$. □

Άσκηση 5.6. *Να δειχθεί ότι αν* $\gcd(a, b) = \gcd(a, c) = 1$, *τότε* $\gcd(a, bc) = 1$.

Λύση. Επειδή $\gcd(a, b) = \gcd(a, c) = 1$, έπεται ότι υπάρχουν $x, y, s, t \in \mathbb{Z}$ ώστε

$$xa + yb = ta + sc = 1.$$

Ισχύει ότι

$$\begin{aligned} xa + y1b &= 1 \\ xa + y(ta + sc)b &= 1 \\ xa + ybta + sbc &= 1 \\ (x + ybt)a + sbc &= 1. \end{aligned}$$

Άρα, από την Πρόταση 5.3 έπεται ότι $\gcd(a, bc) = 1$. (Διότι, αφού ο $\gcd(a, bc)$ διαιρεί το πρώτο μέλος της ισότητας, πρέπει να διαιρεί και το δεύτερο.) □

Άσκηση 5.7. *Να δειχθεί ότι αν* $\gcd(a, b) = 1$ *τότε* $\gcd(a^2, b^2) = 1$.

Λύση. Από την προηγούμενη άσκηση, με $b = c$, προκύπτει ότι $\gcd(a, b \cdot b) = \gcd(a, b^2) = 1$. Εφαρμόζοντας το αποτέλεσμα της προηγούμενης άσκησης για την ισότητα $\gcd(b^2, a) = 1$, προκύπτει ότι $\gcd(b^2, a \cdot a) = \gcd(b^2, a^2) = 1$. □

Άσκηση 5.8. *Να δειχθεί ότι αν* $a \mid n$, $b \mid n$ *και* $\gcd(a, b) = 1$, *τότε* $ab \mid n$.

Λύση. Επειδή $a \mid n$ και $b \mid n$, υπάρχουν $k_1, k_2 \in \mathbb{Z}$ ώστε $n = k_1 a$ και $n = k_2 b$.

Επειδή $\gcd(a, b) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ ώστε $xa + yb = 1$.

Πολλαπλασιάζοντας την τελευταία σχέση με n έχουμε ότι

$$\begin{aligned} xan + ybn &= n \\ xak_2 b + ybk_1 a &= n \\ xk_2 ab + yk_1 ab &= n. \end{aligned}$$

Επειδή το ab διαιρεί το πρώτο μέλος, έπεται ότι $ab \mid n$. □

Άσκηση 5.9. *Η ακολουθία των αριθμών Fibonacci ορίζεται από τις σχέσεις $F_0 = F_1 = 1$ και $F_{n+2} = F_{n+1} + F_n$, όπου $n \in \mathbb{N}$. Να δειχθεί ότι $\gcd(F_{n+1}, F_n) = 1$, για κάθε $n \in \mathbb{N}$.*

Λύση. Με επαγωγή ως προς n.

Για $n = 0$ έχουμε $\gcd(F_1, F_0) = \gcd(1, 1) = 1$, δηλαδή ο ισχυρισμός ισχύει.

Έστω ότι ο ισχυρισμός ισχύει για $n = k$, δηλαδή $\gcd(F_{k+1}, F_k) = 1$. Θα δειχθεί ότι ο ισχυρισμός ισχύει για $n = k + 1$.

Πράγματι, έστω $d = \gcd(F_{k+2}, F_{k+1})$. Τότε αφού $d \mid F_{k+2}$ και $d \mid F_{k+1}$, έπεται ότι $d \mid (F_{k+2} - F_{k+1})$, και άρα $d \mid F_k$. Επομένως, $d \mid F_{k+1}$ και $d \mid F_k$. Όμως $\gcd(F_k, F_{k+1}) = 1$, οπότε $d = 1$. Δηλαδή, ο ισχυρισμός ισχύει.

Άρα, για κάθε $n \in \mathbb{N}$ ισχύει ότι $\gcd(F_{n+1}, F_n) = 1$. □

5.1.4 Ασκήσεις προς επίλυση

1) Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι $\gcd(n + 1, n) = 1$.

2) Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι $\gcd(9n + 8, 8n + 7) = 1$.

3) Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει ότι $\gcd(2k + 1, 9k + 4) = 1$.

4) Αν $\gcd(a, b) = 1$, να δειχθεί ότι $\gcd(2a + 3b, 5a + 8b) = 1$.

5) Αν $\gcd(a, b) = 1$, να δειχθεί ότι $\gcd(a, b^3) = 1$.

6) Να δειχθεί ότι αν $\gcd(a, b) = 1$, τότε $\gcd(a^3, b^3) = 1$.

7) Να δειχθεί ότι αν $a \mid bc$ και $\gcd(a, b) = 1$, τότε $a \mid c$.

8) Να δειχθεί ότι αν $\gcd(a, b) = 1$, τότε $\gcd(a^n, b^k) = 1$, για κάθε $n, k \in \mathbb{N}^*$.

5.1.5 Ο αλγόριθμος του Ευκλείδη

Ο απλοϊκός τρόπος υπολογισμού του μκδ δύο αριθμών a και b είναι η εύρεση όλων των διαιρετών των a και b και στη συνέχεια η επιλογή του μεγαλύτερου από αυτούς. Η διαδικασία αυτή απαιτεί πολλούς υπολογισμούς. Μια αποτελεσματικότερη μέθοδος είναι ο **αλγόριθμος του Ευκλείδη**.[2]

Ο αλγόριθμος του Ευκλείδη παρουσιάζεται, στις προτάσεις 1 και 2 του 7ου βιβλίου των Στοιχείων.

[2] Ο **Ευκλείδης** (325–265 π.Χ.) έζησε στην Αλεξάνδρεια την εποχή του Πτολεμαίου του Α΄. Το έργο του **Στοιχεία** γράφτηκε περίπου το 300 π.Χ. και αποτελείται από 13 βιβλία, 3 από τα οποία πραγματεύονται τη θεωρία αριθμών, και είναι το πιο πολυδιαβασμένο μαθηματικό έργο με πάνω από 1000 διαφορετικές εκδόσεις. Έχει μείνει ιστορική η

Πρόταση 5.4. *Έστω $a, b \in \mathbb{N}^*$ με $a = \pi b + \upsilon$, όπου $0 \leq \upsilon < b$. Τότε ισχύει ότι*

$$\gcd(a, b) = \gcd(b, \upsilon).$$

Επιπλέον, αν $\upsilon = 0$, τότε $\gcd(a, b) = b$.

Απόδειξη. Επειδή $\gcd(b, \upsilon) \mid a$ και $\gcd(a, b) \mid \upsilon$, προκύπτει ότι

$$\gcd(\gcd(b, \upsilon), a) = \gcd(b, \upsilon) \text{ και } \gcd(\gcd(a, b), \upsilon) = \gcd(a, b).$$

Επομένως, από τις ισότητες

$$\gcd(a, b, \upsilon) = \gcd(\gcd(a, b), \upsilon)) = \gcd(a, b)$$

και

$$\gcd(a, b, \upsilon) = \gcd(a, \gcd(b, \upsilon)) = \gcd(b, \upsilon),$$

προκύπτει ότι

$$\gcd(a, b) = \gcd(b, \upsilon).$$

Επιπλέον, αν $\upsilon = 0$, έπεται ότι $b \mid a$, οπότε $\gcd(a, b) = b$. □

Θα χρησιμοποιήσουμε το επόμενο λήμμα.

Λήμμα 5.5. *Έστω $a, b \in \mathbb{N}^*$ με $a = \pi b + \upsilon$, όπου $0 \leq \upsilon < b$. Τότε $\pi = \lfloor \frac{a}{b} \rfloor$ και $\upsilon = a - \lfloor \frac{a}{b} \rfloor b$.*

Απόδειξη. Πράγματι $a = \pi b + \upsilon \Leftrightarrow \frac{a}{b} = \pi + \frac{\upsilon}{b}$. Επομένως $\lfloor \frac{a}{b} \rfloor = \lfloor \pi + \frac{\upsilon}{b} \rfloor = \pi + \lfloor \frac{\upsilon}{b} \rfloor = \pi + 0 = \pi$. Επιπλέον, ισχύει ότι $\upsilon = a - \pi b = a - \lfloor \frac{a}{b} \rfloor b$. □

Πόρισμα 5.6 (Αλγόριθμος του Ευκλείδη). *Για κάθε $a, b \in \mathbb{N}^*$ με $a > b$ η ακολουθία (υ_i) με $\upsilon_{-1} = a$, $\upsilon_0 = b$ και*

$$\upsilon_i = \upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \cdot \upsilon_{i-1}, \text{ όπου } \upsilon_{i-1} \neq 0 \text{ και } i \geq 1,$$

είναι πεπερασμένη με ελάχιστη τιμή το 0. Επιπλέον, αν $\upsilon_k = 0$ τότε $\gcd(a, b) = \upsilon_{k-1}$.

Απόδειξη. Η ακολουθία (υ_i) είναι γνησίως φθίνουσα ακολουθία φυσικών αριθμών.

Πράγματι, επειδή $\upsilon_{-1} = a$ και $\upsilon_0 = b$, από το προηγούμενο λήμμα προκύπτει ότι το υ_i είναι το υπόλοιπο της διαίρεσης του υ_{i-2} με το υ_{i-1}, οπότε $\upsilon_i \in \mathbb{N}$ και $\upsilon_i < \upsilon_{i-1}$. Επομένως, από την αρχή της καλής διάταξης, η (υ_i) λαμβάνει πεπερασμένες τιμές. Έστω m η ελάχιστη τιμή της και $\upsilon_k = m$. Αν $m > 0$ έπεται ότι ορίζεται ο υ_{k+1} και ισχύει ότι $\upsilon_{k+1} < \upsilon_k = m$, άτοπο. Άρα, $m = 0$.

Έστω $u_k = 0$. Για κάθε $i \in [k]$ ισχύει ότι $\upsilon_i = \upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \cdot \upsilon_{i-1}$, ή ισοδύναμα $\upsilon_{i-2} = \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \cdot \upsilon_{i-1} + \upsilon_i$, οπότε από την Πρόταση 5.4 προκύπτει ότι

$$\gcd(\upsilon_{i-2}, \upsilon_{i-1}) = \gcd(\upsilon_{i-1}, \upsilon_i) \text{ για κάθε } i \in [k].$$

Επομένως, λόγω μεταβατικότητας, προκύπτει ότι $\gcd(a, b) = \gcd(\upsilon_{i-1}, \upsilon_i)$ για κάθε $i \in [k]$. Με $i = k$ έχουμε ότι $\gcd(a, b) = \gcd(\upsilon_{k-1}, \upsilon_k) = \gcd(\upsilon_{k-1}, 0) = \upsilon_{k-1}$. □

απάντηση που έδωσε όταν ο βασιλιάς Πτολεμαίος του ζήτησε έναν πιο εύκολο τρόπο για να μάθει γεωμετρία από το να μελετήσει το έργο Στοιχεία. Ο Ευκλείδης του απάντησε: "Δεν υπάρχει βασιλική οδός για τη Γεωμετρία". Επίσης, χαρακτηριστική είναι και η στάση του απέναντι σε ένα πλούσιο μαθητή του ο οποίος μετά την διδασκαλία ενός θεωρήματος τον ρώτησε τι θα κέρδιζε από αυτό. Ο Ευκλείδης παρήγγειλε σε ένα δούλο του "να του δώσει χρήματα αφού θέλει οπωσδήποτε να κερδίσει κάτι".

Παρατήρηση. Σημαντική συνέπεια του προηγούμενου πορίσματος είναι ότι ο μκδ των a, b προσδιορίζεται **χωρίς την εύρεση των διαιρετών τους** αλλά με επαναλαμβανόμενη εφαρμογή του αλγορίθμου της διαίρεσης στους όρους της πεπερασμένης ακολουθίας υ_i.

Για παράδειγμα, ο υπολογισμός του μκδ των 168 και 25 προκύπτει ως εξής:

Αρχικά, θέτουμε $\upsilon_{-1} = 168$ και $\upsilon_0 = 25$.

Στην συνέχεια, για κάθε $i \geq 1$ και όσο $\upsilon_{i-1} \neq 0$, υπολογίζουμε τον όρο υ_i χρησιμοποιώντας τη σχέση

$$\upsilon_i = \upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \upsilon_{i-1},$$

οπότε έχουμε ότι

$$\begin{aligned}
\upsilon_1 &= \upsilon_{-1} - \lfloor \frac{\upsilon_{-1}}{\upsilon_0} \rfloor \upsilon_0 = 168 - \lfloor \frac{168}{25} \rfloor 25 = 168 - 6 \cdot 25 = 18 \\
\upsilon_2 &= \upsilon_0 - \lfloor \frac{\upsilon_0}{\upsilon_1} \rfloor \upsilon_1 = 25 - \lfloor \frac{25}{18} \rfloor 18 = 25 - 1 \cdot 18 = 7 \\
\upsilon_3 &= \upsilon_1 - \lfloor \frac{\upsilon_1}{\upsilon_2} \rfloor \upsilon_2 = 18 - \lfloor \frac{18}{7} \rfloor 7 = 18 - 2 \cdot 7 = 4 \\
\upsilon_4 &= \upsilon_2 - \lfloor \frac{\upsilon_2}{\upsilon_3} \rfloor \upsilon_3 = 7 - \lfloor \frac{7}{4} \rfloor 4 = 7 - 1 \cdot 4 = 3 \\
\upsilon_5 &= \upsilon_3 - \lfloor \frac{\upsilon_3}{\upsilon_4} \rfloor \upsilon_4 = 4 - \lfloor \frac{4}{3} \rfloor 3 = 4 - 1 \cdot 3 = 1 \\
\upsilon_6 &= \upsilon_4 - \lfloor \frac{\upsilon_4}{\upsilon_5} \rfloor \upsilon_5 = 3 - \lfloor \frac{3}{1} \rfloor 1 = 3 - 3 \cdot 1 = 0.
\end{aligned}$$

Άρα, $\gcd(168, 25) = \upsilon_5 = 1$.

Η παραπάνω διαδικασία μπορεί να περιγραφεί και με τη βοήθεια των παρακάτω ισοτήτων που περιγράφουν τις διαιρέσεις κάθε βήματος:

$$\begin{aligned}
168 &= 6 \cdot 25 + 18, \\
25 &= 1 \cdot 18 + 7, \\
18 &= 2 \cdot 7 + 4, \\
7 &= 1 \cdot 4 + 3, \\
4 &= 1 \cdot 3 + 1, \\
3 &= 3 \cdot 1 + 0.
\end{aligned}$$

Με αυτή την περιγραφή, ο υπολογισμός του μκδ των 2520 και 154 προκύπτει ως εξής:

$$\begin{aligned}
2520 &= 16 \cdot 154 + 56, \\
154 &= 2 \cdot 56 + 42, \\
56 &= 1 \cdot 42 + 14, \\
42 &= 3 \cdot 14 + 0.
\end{aligned}$$

Άρα, $\gcd(2520, 154) = 14$.

Τέλος, ο υπολογισμός του $\gcd(a, b)$ για τους φυσικούς αριθμούς a, b, με τον αλγόριθμο του Ευκλείδη μπορεί να γίνει χρησιμοποιώντας τις αναδρομικές σχέσεις

$\gcd(a, 0) = a$,

$\gcd(a, b) = gcd(b, \upsilon)$, όπου υ το υπόλοιπο της διαίρεσης του a με το b.

Προφανώς αν $b > a$, δηλαδή αν το πρώτο όρισμα είναι μικρότερο από το δεύτερο, τότε $a = 0 \cdot b + a$, οπότε $\gcd(a, b) = \gcd(b, a)$, δηλαδή ο αλγόριθμος εκτελείται σωστά για το ζεύγος b, a με κόστος μια επιπλέον αναδρομική κλήση.

Ποιά είναι η πολυπλοκότητα του αλγορίθμου του Ευκλείδη;

Το κόστος εκτέλεσης του αλγορίθμου του Ευκλείδη είναι ανάλογο του αριθμού των διαιρέσεων που απαιτούνται για την εύρεση των υπολοίπων κάθε ενδιαμέσου ζεύγους. Ένα φράγμα για το κόστος του αλγορίθμου του Ευκλείδη δίδεται στην Πρόταση 5.8. Για την απόδειξή της, θα χρειαστούμε το επόμενο λήμμα.

Λήμμα 5.7. *Έστω $a, b \in \mathbb{N}^*$ με $a > b$ και $a = \pi b + \upsilon$, όπου $0 \leq \upsilon < b$. Τότε $\upsilon < a/2$.*

Απόδειξη. Διακρίνουμε δύο περιπτώσεις:

Αν $b \leq a/2$, τότε $\upsilon < b \leq a/2$.

Αν $a > b > a/2$, τότε $a = 1 \cdot b + (a - b)$, οπότε $\upsilon = a - b < a - a/2 = a/2$. □

Πρόταση 5.8 (Πολυπλοκότητα του αλγορίθμου του Ευκλείδη). *Έστω $a, b \in \mathbb{N}^*$ με $a > b$. Ο αριθμός των διαιρέσεων $c(a, b)$ που απαιτούνται για τον υπολογισμό του μέγιστου κοινού διαιρέτη των a, b είναι μικρότερος από $2 \log_2 a$.*

Απόδειξη. Επειδή $a > b$, έπεται ότι $a \geq 2$. Θα χρησιμοποιήσουμε επαγωγή ως προς a.

Για $a = 2$ έπεται ότι $b = 1$. Στην περίπτωση αυτή έχουμε ότι $2 = 2 \cdot 1 + 0$ άρα $c(2, 1) = 1$ και $2 \log_2 2 = 2$, οπότε ο ισχυρισμός ισχύει.

Έστω ότι ο ισχυρισμός ισχύει για κάθε $a < n$, δηλαδή αν $b < a < n$ τότε $c(a, b) < 2 \log_2 a$.

Θα αποδειχθεί ότι ο ισχυρισμός ισχύει και για $a = n$.

Πράγματι, στην περίπτωση όπου $b \mid a$ έχουμε $c(a, b) = 1$, οπότε ο ισχυρισμός ισχύει.

Αν $b \nmid a$, τότε μετά τα δύο πρώτα βήματα του αλγορίθμου του Ευκλείδη

$$a = \pi_1 b + \upsilon_1, \text{ όπου } 0 \leq \upsilon_1 < b,$$

$$b = \pi_2 \upsilon_1 + \upsilon_2, \text{ όπου } 0 \leq \upsilon_2 < \upsilon_1,$$

(που απαιτούν δύο διαιρέσεις), το πρόβλημα υπολογισμού του $\gcd(a, b)$ ανάγεται στο πρόβλημα υπολογισμού του $\gcd(\upsilon_1, \upsilon_2)$.

Άρα,

$$c(a, b) = c(\upsilon_1, \upsilon_2) + 2.$$

Από το προηγούμενο λήμμα προκύπτει ότι $\upsilon_2 < \upsilon_1 < a/2 < a = n$, και επομένως από την υπόθεση της επαγωγής ισχύει ότι

$$c(\upsilon_1, \upsilon_2) < 2 \log_2 \upsilon_1 < 2 \log_2 a/2.$$

Άρα,

$$c(a, b) < 2 \log_2 a/2 + 2 = 2 \log_2 a - 2 \log_2 2 + 2 = \log_2 a.$$

Δηλαδή, ο ισχυρισμός ισχύει. □

Πόρισμα 5.9. *Για κάθε $a, b \in \mathbb{N}^*$ με $a > b$, η πεπερασμένη ακολουθία (υ_i) με $\upsilon_{-1} = a$, $\upsilon_0 = b$ και*

$$\upsilon_i = \upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \cdot \upsilon_{i-1}, \text{ όπου } \upsilon_{i-1} \neq 0 \text{ και } i \geq 1,$$

έχει μέγιστο δείκτη μικρότερο από $2\log_2 a$.

Παρατήρηση. Η προηγούμενη πρόταση αποδείχθηκε από το Γάλλο μαθηματικό Gabriel Lamé. Μάλιστα, ο Lamé βρήκε ένα καλύτερο φράγμα για τον αριθμό των διαιρέσεων, συγκεκριμένα απέδειξε ότι $c(a, b) < 5\log_{10} a \simeq 1.50515 \log_2 a$. **Η πρόταση αυτή θεωρείται το πρώτο αποτέλεσμα σχετικά με τον υπολογισμό της πολυπλοκότητας ενός αλγορίθμου**.

5.1.6 Ο επεκτεταμένος αλγόριθμος του Ευκλείδη

Μια σημαντική εφαρμογή του αλγόριθμου του Ευκλείδη, εκτός της εύρεσης του μκδ των αριθμών a, b, είναι ότι μπορεί να χρησιμοποιηθεί και για την εύρεση δύο ακεραίων s και t για τους οποίους $\gcd(a, b) = as + bt$.

Για παράδειγμα, από τις σχέσεις

$$\begin{aligned} 2520 &= 16 \cdot 154 + 56, \\ 154 &= 2 \cdot 56 + 42, \\ 56 &= 1 \cdot 42 + 14, \end{aligned}$$

προκύπτει ότι $\gcd(2520, 154) = 14$ και επιπλέον

$$\begin{aligned} 14 &= 1 \cdot 56 + (-1) \cdot 42 \\ &= 1 \cdot 56 + (-1) \cdot (1 \cdot 154 + (-2) \cdot 56) = 3 \cdot 56 + (-1) \cdot 154 \\ &= 3 \cdot (1 \cdot 2520 + (-16) \cdot 154) + (-1) \cdot 154 \\ &= 3 \cdot 2520 + (-49) \cdot 154, \end{aligned}$$

δηλαδή $\gcd(2520, 154) = 3 \cdot 2520 + (-49) \cdot 154$.

Αντίστοιχα, από τις σχέσεις

$$\begin{aligned} 168 &= 6 \cdot 25 + 18, \\ 25 &= 1 \cdot 18 + 7, \\ 18 &= 2 \cdot 7 + 4, \\ 7 &= 1 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0, \end{aligned}$$

προκύπτει ότι $\gcd(168, 25) = 1$ και επιπλέον

$$\begin{aligned} 1 &= 1 \cdot 4 + (-1) \cdot 3 \\ &= 1 \cdot 4 + (-1) \cdot (1 \cdot 7 + (-1) \cdot 4) = (-1) \cdot 7 + 2 \cdot 4 \\ &= (-1) \cdot 7 + 2 \cdot (1 \cdot 18 + (-2) \cdot 7) = 2 \cdot 18 + (-5) \cdot 7 \\ &= 2 \cdot 18 + (-5)(1 \cdot 25 + (-1) \cdot 18) = (-5) \cdot 25 + 7 \cdot 18 \\ &= (-5) \cdot 25 + 7 \cdot (1 \cdot 168 + (-6) \cdot 25) \\ &= 7 \cdot 168 + (-47) \cdot 25, \end{aligned}$$

δηλαδή $\gcd(168, 25) = 7 \cdot 168 + (-47) \cdot 25$.

Παρατήρηση. Από τα προηγούμενα παραδείγματα είναι φανερό ότι χρησιμοποιώντας τις παραπάνω ισότητες εκφράζουμε τον μκδ των a, b ως γραμμικό συνδυασμό όχι μόνο των a και b αλλά και όλων των πηλίκων και υπολοίπων που εμφανίζονται στα βήματα εκτέλεσης του αλγορίθμου του Ευκλείδη.

Έτσι, στο προηγούμενο παράδειγμα υπολογίσαμε ότι

$$1 = 1 \cdot 4 + (-1) \cdot 3 = (-1) \cdot 7 + 2 \cdot 4 = 2 \cdot 18 + (-5) \cdot 7 = (-5) \cdot 25 + 7 \cdot 18 = 7 \cdot 168 + (-47) \cdot 25,$$

δηλαδή βρήκαμε αριθμούς s, t ώστε $sx+sy = \gcd(a, b)$ για κάθε $(x, y) \in \{(4, 3), (7, 4), (18, 7), (25, 18), (168, 25)\}$

Στην επόμενη πρόταση δίδεται μια αναδρομική σχέση για τους συντελεστές s, t κάθε ζεύγους. Είναι ενδιαφέρον ότι για τον υπολογισμό αυτών των συντελεστών επαρκούν τα πηλίκα των διαιρέσεων που πραγματοποιούνται κατά την εκτέλεση του αλγορίθμου του Ευκλείδη.

Πρόταση 5.10 (Επεκτεταμένος αλγόριθμος του Ευκλείδη). *Έστω $a, b \in \mathbb{N}^*$ με $a > b$ και (υ_i) η ακολουθία με $\upsilon_{-1} = a$, $\upsilon_0 = b$, $\upsilon_k = 0$ και*

$$\upsilon_i = \upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \upsilon_{i-1}, \text{ για κάθε } i \in [k].$$

Αν για $i \in [k]$ και $s, t \in \mathbb{Z}$ ισχύει ότι

$$s\upsilon_{i-1} + t\upsilon_i = \gcd(a, b),$$

τότε

$$t\upsilon_{i-2} + (s - t\lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor)\upsilon_{i-1} = \gcd(a, b).$$

Απόδειξη. Έστω $i \in [k]$ με $s, t \in \mathbb{Z}$ με

$$s\upsilon_{i-1} + t\upsilon_i = \gcd(a, b).$$

Τότε

$$\upsilon_i = \upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \upsilon_{i-1},$$

οπότε

$$s\upsilon_{i-1} + t(\upsilon_{i-2} - \lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor \upsilon_{i-1}) = \gcd(a, b)$$

ή, ισοδύναμα

$$t\upsilon_{i-2} + (s - t\lfloor \frac{\upsilon_{i-2}}{\upsilon_{i-1}} \rfloor)\upsilon_{i-1} = \gcd(a, b). \qquad \square$$

Παρατήρηση. Δεδομένου ότι $\gcd(a, b) = \upsilon_{k-1} = \upsilon_{k-3} - \lfloor \frac{\upsilon_{k-3}}{\upsilon_{k-2}} \rfloor \upsilon_{k-2}$, δηλαδή, για $s' = 1$ και $t' = \lfloor \frac{\upsilon_{k-3}}{\upsilon_{k-2}} \rfloor$ ισχύει $s'\upsilon_{k-3} + t'\upsilon_{k-2} = \gcd(a, b)$, οι συντελεστές s, t για τους οποίους $sa+tb = \gcd(a, b)$ υπολογίζονται με επαναλαμβανόμενη εφαρμογή της προηγούμενης πρότασης.

Με τη βοήθεια των προτάσεων 5.6 και 5.10 η διαδικασία εύρεσης του μκδ των a και b, και στη συνέχεια ο υπολογισμός των s, t μπορεί να πινακοποιηθεί.

Για παράδειγμα, ο μκδ(168, 25) υπολογίζεται στον επόμενο πίνακα

Διαιρετέος	Διαιρέτης	Υπόλοιπο	Πηλίκο
168	25	18	6
25	18	7	1
18	7	4	2
7	4	3	1
4	3	1	1
3	1	0	3

Κάθε βήμα του αλγορίθμου, που αντιστοιχεί σε μια διαίρεση της μορφής $a = \pi a + \upsilon$, περιγράφεται από μια γραμμή του πίνακα: Στις δύο πρώτες στήλες εμφανίζονται τα a, b, στη τρίτη το υπόλοιπο υ και στη τέταρτη το πηλίκο π της διαίρεσης. Η διαδικασία σταματά όταν στη στήλη του υπολοίπου εμφανισθεί το 0. Ο μκδ διαιρέτης των δύο πρώτων στοιχείων κάθε γραμμής ισούται με το τελευταίο στοιχείο της δεύτερης στήλης.

Για τον υπολογισμό των συντελεστών s, t για τους οποίους $sa + tb = \gcd(a, b)$, επεκτείνουμε τον πίνακα με τρεις επιπλέον στήλες, τις οποίες συμπληρώνουμε από τη τελευταία γραμμή προς την πρώτη.

Διαιρετέος	Διαιρέτης	Υπόλοιπο	Πηλίκο	s	t	Γρ. Συνδυασμός
168	25	18	$\boxed{6}$	7	$-5 - 7 \cdot \boxed{6} = -47$	$7 \cdot 168 + (-47) \cdot 25$
25	18	7	$\boxed{1}$	-5	$2 - (-5) \cdot \boxed{1} = 7$	$(-5) \cdot 25 + 7 \cdot 18$
18	7	4	$\boxed{2}$	2	$-1 - 2 \cdot \boxed{2} = -5$	$2 \cdot 18 + (-5) \cdot 7$
7	4	3	$\boxed{1}$	-1	$1 - (-1) \cdot \boxed{1} = 2$	$(-1) \cdot 7 + 2 \cdot 4$
4	3	1	$\boxed{1}$	1	$0 - 1 \cdot \boxed{1} = -1$	$4 \cdot 1 + 3 \cdot (-1)$
3	1	0	3	0	1	

Στη πρώτη γραμμή της τελευταίας στήλης παρουσιάζεται ο ζητούμενος γραμμικός συνδυασμός, στις υπόλοιπες γραμμές φαίνονται όλοι οι επιπλέον γραμμικοί συνδυασμοί που υπολογίζονται κατά την εκτέλεση του επεκτεταμένου αλγορίθμου του Ευκλείδη.

5.1.7 Λυμένες ασκήσεις

Άσκηση 5.10. *Να υπολογισθεί ο μκδ των* 12075 *και* 4655 *και στη συνέχεια να εκφραστεί ως γραμμικός συνδυασμός αυτών.*

Λύση. Έχουμε ότι

$$\begin{aligned} 12075 &= 2 \cdot 4655 + 2765 \\ 4655 &= 1 \cdot 2765 + 1890 \\ 2765 &= 1 \cdot 1890 + 875 \\ 1890 &= 2 \cdot 875 + 140 \\ 875 &= 6 \cdot 140 + 35 \\ 140 &= 4 \cdot 35 + 0. \end{aligned}$$

Άρα, $\gcd(12075, 4655) = 35$.

Από τις προηγούμενες ισότητες προκύπτει ότι

$$\begin{aligned}35 &= 875 + (-6)\cdot 140\\ &= 875 + (-6)\cdot(1890 + (-2)\cdot 875) = (-6)\cdot 1890 + 13\cdot 875\\ &= (-6)\cdot 1890 + 13\cdot(2765 + (-1)\cdot 1890) = 13\cdot 2765 + (-19)\cdot 1890\\ &= 13\cdot 2765 + (-19)\cdot(4655 + (-1)\cdot 2765) = (-19)\cdot 4655 + 32\cdot 2765\\ &= (-19)\cdot 4655 + 32\cdot(12075 + (-2)\cdot 4655) = 32\cdot 12075 + (-83)\cdot 4655.\end{aligned}$$

Άρα, $\gcd(12075, 4655) = 32\cdot 12075 + (-83)\cdot 4655$. □

Άσκηση 5.11. *Να απλοποιηθεί το κλάσμα* $\frac{814}{532}$.

Λύση. Από τον αλγόριθμο του Ευκλείδη έχουμε ότι

$$\begin{aligned}814 &= 1\cdot 532 + 282\\ 532 &= 1\cdot 282 + 250\\ 282 &= 1\cdot 250 + 32\\ 250 &= 7\cdot 32 + 26\\ 32 &= 1\cdot 26 + 6\\ 26 &= 4\cdot 6 + 2\\ 6 &= 3\cdot 2 + 0.\end{aligned}$$

Άρα, $\gcd(814, 532) = 2$, και επομένως η μέγιστη απλοποίηση στο κλάσμα προκύπτει με διαίρεση του αριθμητή και του παρονομαστή με το 2 και δεν γίνεται άλλη απλοποίηση. Επομένως, $\frac{814}{532} = \frac{407}{261}$. □

5.1.8 Ασκήσεις προς επίλυση

1) Να ευρεθεί ο μέγιστος κοινός διαιρέτης των επόμενων ζευγών αριθμών:

   442 και 647, 362 και 290, 436 και 376, 529 και 841, 1271 και 1591,

   και να εκφραστεί ο μκδ κάθε ζεύγους ως γραμμικός συνδυασμός αυτών.

2) Να γραφεί πρόγραμμα που υπολογίζει τον μκδ των φυσικών αριθμών a, b, και στη συνέχεια υπολογίζει τους συντελεστές s, t ώστε $sa + tb = \gcd(a, b)$.

5.1.9 Γραμμικές διοφαντικές εξισώσεις

Έστω a, b, c τρεις ακέραιοι αριθμοί με $a \neq 0 \neq b$. Τα ζεύγη x, y για τα οποία ισχύει ότι

$$ax + by = c$$

μπορεί να θεωρηθεί ότι αντιστοιχούν σε σημεία του επιπέδου με συντεταγμένες (x, y) και ισχύει ότι όλα ανήκουν πάνω στην ευθεία με εξίσωση $ax + by = c$.

Ένα ενδιαφέρον ερώτημα είναι αν υπάρχουν ακέραια x, y οι οποίοι επαληθεύουν την εξίσωση αυτή, ή ισοδύναμα, αν η ευθεία $ax + by = c$ διέρχεται από σημεία με ακέραιες συντεταγμένες. Οι εξισώσεις στις οποίες αναζητούμε λύσεις ακέραιες (ή, και σε ορισμένες περιπτώσεις ρητές)

ονομάζονται γενικά **διοφαντικές εξισώσεις**, ενώ η εξίσωση αυτή ονομάζεται **γραμμική διοφαντική εξίσωση**.

Γνωρίζουμε ότι αν a, b είναι δύο φυσικοί αριθμοί, τότε υπάρχουν ακέραιοι αριθμοί x, y έτσι ώστε

$$ax + by = \gcd(a, b)$$

και μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο του Ευκλείδη προκειμένου να προσδιορίσουμε ένα ζεύγος τέτοιων αριθμών (x, y).

Για παράδειγμα, αν $a = 527$ και $b = 341$, τότε $\gcd(341, 527) = 31$ και

$$31 = 2 \cdot 527 - 3 \cdot 341,$$

δηλαδή $(x, y) = (2, -3)$.

Προφανώς, θα ισχύει επίσης ότι

$$31k = 2k \cdot 527 - 3k \cdot 341, \text{ για κάθε } k \in \mathbb{Z}$$

και, γενικότερα, αν (x_0, y_0) είναι λύση της εξίσωσης

$$ax + by = \gcd(a, b),$$

τότε (x_0, y_0) θα είναι επίσης λύση της εξίσωσης

$$akx + bky = k \gcd(a, b).$$

Επιπλέον, αν (x_0, y_0) είναι μια λύση της εξίσωσης

$$ax + by = \gcd(a, b),$$

τότε και $(x_0 + \lambda b, y_0 - \lambda a)$ είναι επίσης λύσεις της ίδιας εξίσωσης για κάθε $\lambda \in \mathbb{Z}$, αφού

$$a(x_0 + \lambda b) + b(y_0 - \lambda a) = ax_0 + by_0 = \gcd(a, b).$$

Αυτές οι παρατηρήσεις συστηματοποιούνται στην επόμενη πρόταση.

Πρόταση 5.11. *Η γραμμική διοφαντική εξίσωση*

$$ax + by = c$$

έχει λύση, αν και μόνο αν $\gcd(a, b) \mid c$.

Επιπλέον, αν (x_0, y_0) *είναι μια λύση της, τότε κάθε λύση της είναι της μορφής*

$$(x_0 + \lambda \frac{b}{\gcd(a, b)}, y_0 - \lambda \frac{a}{\gcd(a, b)})$$

όπου $\lambda \in \mathbb{Z}$.

Απόδειξη. Αν η εξίσωση έχει λύση, δηλαδή αν υπάρχουν $x, y \in \mathbb{Z}$ με $ax + by = c$, τότε $\gcd(a, b) \mid (ax + by)$, οπότε $\gcd(a, b) \mid c$.

Αντίστροφα, έστω $\gcd(a, b) \mid c$ με $c = k \gcd(a, b)$, όπου $k \in \mathbb{Z}$.

Με τη βοήθεια του αλγορίθμου του Ευκλείδη μπορούν να βρεθούν ακέραιοι s, t ώστε $as + bt = \gcd(a, b)$.

Πολλαπλασιάζοντας με k προκύπτει ότι $aks + bkt = k\gcd(a,b) = c$.
Επομένως, οι ακέραιοι (ks, kt) αποτελούν μια λύση της εξίσωσης $ax + by = c$.
Άρα, η εξίσωση $ax + by = c$ έχει λύση αν και μόνο αν $\gcd(a,b) \mid c$.

Έστω (x_0, y_0) μια λύση της εξίσωσης

$$ax + by = c.$$

Τότε η (x_0, y_0) είναι επίσης λύση της εξίσωσης

$$\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y = \frac{c}{\gcd(a,b)}$$

και αντιστρόφως.

Πράγματι, έστω $ax_0 + by_0 = c$. Διαιρώντας κατά μέλη με $\gcd(a,b)$, έπεται ότι $\frac{a}{\gcd(a,b)}x_0 + \frac{b}{\gcd(a,b)}y_0 = \frac{c}{\gcd(a,b)}$.

Αντίστροφα, έστω $\frac{a}{\gcd(a,b)}x_0 + \frac{b}{\gcd(a,b)}y_0 = \frac{c}{\gcd(a,b)}$. Πολλαπλασιάζοντας με $\gcd(a,b)$, έπεται ότι $ax_0 + by_0 = c$.

Άρα, οι λύσεις της εξίσωσης $ax + by = c$ ταυτίζονται με τις λύσεις της εξίσωσης

$$\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y = \frac{c}{\gcd(a,b)}.$$

Αν (x_0, y_0), (x_1, y_1) είναι δύο λύσεις αυτής της εξίσωσης, τότε έπεται ότι

$$\frac{a}{\gcd(a,b)}(x_0 - x_1) + \frac{b}{\gcd(a,b)}(y_0 - y_1) = c - c = 0.$$

Ισοδύναμα,

$$\frac{a}{\gcd(a,b)}(x_1 - x_0) = \frac{b}{\gcd(a,b)}(y_0 - y_1).$$

Άρα,

$$\frac{a}{\gcd(a,b)} \mid \frac{b}{\gcd(a,b)}(y_0 - y_1) \text{ και } \frac{b}{\gcd(a,b)} \mid \frac{b}{\gcd(a,b)}(x_1 - x_0).$$

Επειδή $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$, έπεται ότι

$$\frac{a}{\gcd(a,b)} \mid (y_0 - y_1) \text{ και } \frac{b}{\gcd(a,b)} \mid (x_1 - x_0).$$

Επομένως,

$$y_0 - y_1 = k\frac{a}{\gcd(a,b)} \text{ και } x_1 - x_0 = \lambda\frac{b}{\gcd a,b}, \text{ όπου } k, \lambda \in \mathbb{Z}$$

Τέλος, επειδή ισχύει ότι

$$\frac{a}{\gcd(a,b)}(x_1 - x_0) = \frac{b}{\gcd a,b}(y_0 - y_1),$$

έπεται ότι

$$\frac{a}{\gcd(a,b)}\lambda\frac{b}{\gcd a,b} = \frac{b}{\gcd a,b}k\frac{a}{\gcd(a,b)}.$$

Επομένως,

$$k = \lambda.$$

Άρα,

$$x_1 = x_0 + \lambda\frac{b}{\gcd(a,b)} \text{ και } y_1 = y_0 - \lambda\frac{a}{\gcd(a,b)}, \text{ όπου } \lambda \in \mathbb{Z}.$$

Δηλαδή, όλες οι λύσεις εκφράζονται συναρτήσει μιας λύσης (x_0, y_0) χρησιμοποιώντας τις προηγούμενες δύο σχέσεις. □

Παρατήρηση. Από την προηγούμενη πρόταση προκύπτει ότι αν $\gcd(a,b) \nmid c$, τότε η διοφαντική εξίσωση

$$ax + by = c$$

δεν έχει ακέραιες λύσεις.

Επιπλέον, οι λύσεις της εξίσωσης αυτής ταυτίζονται με τις λύσεις της απλούστερης εξίσωσης

$$\frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y = \frac{c}{\gcd(a,b)}.$$

Τέλος, επειδή

$$\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1,$$

από τον αλγόριθμο του Ευκλείδη προκύπτει ότι υπάρχουν (s,t) ώστε

$$\frac{a}{\gcd(a,b)}s + \frac{b}{\gcd(a,b)}t = 1.$$

Πολλαπλασιάζοντας με $\frac{c}{\gcd(a,b)}$ κατα μέλη προκύπτει ότι

$$\frac{a}{\gcd(a,b)}\left(\frac{c}{\gcd(a,b)}s\right) + \frac{b}{\gcd(a,b)}\left(\frac{c}{\gcd(a,b)}t\right) = \frac{c}{\gcd(a,b)}$$

και επομένως, μια λύση της εξίσωσης είναι το ζεύγος

$$(x_0, y_0) = \left(\frac{c}{\gcd(a,b)}s, \frac{c}{\gcd(a,b)}t\right).$$

Επιπρόσθετα, όλες οι λύσεις της προκύπτουν από τις σχέσεις

$$(x,y) = (x_0 + \lambda\frac{b}{\gcd(a,b)}, y_0 - \lambda\frac{a}{\gcd(a,b)}), \text{ όπου } \lambda \in \mathbb{Z}.$$

Παραδείγματα

Η διοφαντική εξίσωση

$$12x + 27y = 2$$

δεν έχει λύση, διότι $\gcd(12, 27) = 3$ και $3 \nmid 2$.

Η διοφαντική εξίσωση

$$69x + 39y = 15$$

έχει λύση, διότι $\gcd(69, 39) = 3$.

Αρκεί να βρούμε τις λύσεις της απλούστερης εξίσωσης

$$23x + 13y = 5$$

όπου $\gcd(23, 13) = 1$. Από τον αλγόριθμο του Ευκλείδη προκύπτει ότι

$$23 = 1 \cdot 13 + 10$$
$$13 = 1 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + 1.$$

Επομένως

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 = 10 - 3(13 - 1 \cdot 10) \\ &= -3 \cdot 13 + 4 \cdot 10 = -3 \cdot 13 + 4(23 - 1 \cdot 13) \\ &= 4 \cdot 23 - 7 \cdot 13, \end{aligned}$$

δηλαδή

$$23 \cdot 4 + 13 \cdot (-7) = 1$$

οπότε

$$23 \cdot (4 \cdot 5) + 13((-7) \cdot 5) = 1 \cdot 5$$

ή ισοδύναμα

$$23 \cdot 20 + 13 \cdot (-35) = 5.$$

Άρα, το ζεύγος $(x, y) = (20, -35)$ είναι μια λύση της εξίσωσης $23x + 13y = 5$, και επομένως είναι λύση και της εξίσωσης $69x + 39y = 15$. Άρα, τελικά, οι ζητούμενες λύσεις είναι τα ζεύγη της μορφής

$$(x, y) = (20 + 13\lambda, -35 - 23\lambda), \text{ όπου } \lambda \in \mathbb{Z}.$$

Ιστορικό σημείωμα. Η ονομασία "διοφαντικές εξισώσεις" δόθηκε προς τιμή του **Διόφαντου του Αλεξανδρινού**, ο οποίος στο έργο του **Αριθμητικά** μελέτησε προβλήματα εξισώσεων με ακέραιες ή ρητές λύσεις.

Τα Αριθμητικά του Διόφαντου, γράφτηκαν τον 3ο μ.Χ. αιώνα, και θεωρούνταν χαμένο έργο αφού είχε εξαφανισθεί για περισσότερα από 1000 χρόνια.

Το 1464, ο γερμανός μαθηματικός Regiomontanus (Johannes Moller von Konigsberg[3]) (1436–1476) ανακάλυψε 6 από τα 13 βιβλία των Αριθμητικών. Η πρώτη μετάφραση των βιβλίων στα λατινικά έγινε από τον Rafael Bombelli το 1570.

Το 1621 εκδόθηκαν εκ νέου από τον γάλλο Claude-Gaspar Bachet de Miziriac, και αποτέλεσαν έργο αναφοράς για πολλούς μαθηματικούς, όπως ο Pierre de Fermat (1601–1665) και ο Rene Descartes (1596–1650).

Το έργο Αριθμητικά παρά τα χίλια χρόνια λήθης ξεπερνούσε κατά πολύ τα καλύτερα έργα Άλγεβρας του 16ου αιώνα. Ο Διόφαντος, σε αντίθεση με τους ευρωπαίους αλγεβριστές της εποχής, εκτελούσε πράξεις με αρνητικούς και ρητούς αριθμούς, χρησιμοποιούσε συμβολισμό με γράμματα στις εξισώσεις, ήταν σε θέση να βρίσκει ακέραιες και ρητές λύσεις γραμμικών, δευτεροβάθμιων εξισώσεων και συστημάτων εξισώσεων με ακέραιους συντελεστές δύο ή περισσότερων μεταβλητών.

[3] Πρόκειται για το Konigsberg της Βαυαρίας και όχι για το πιο γνωστό Konigsberg της Ανατολικής Πρωσίας.

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.

AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V. C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

Σχήμα 5.1: Η έκδοση των Αριθμητικών του Διόφαντου, σε μετάφραση στα Λατινικά από τον Claude Gaspard Bachet

Τα Αριθμητικά του Διόφαντου άσκησαν μεγάλη επίδραση στους μαθηματικούς του 16ου αιώνα και έπειτα. Χαρακτηριστική είναι η περίπτωση του Fermat, ο οποίος ασκούσε το επάγγελμα του νομικού αλλά μετά την ανάγνωση των Αριθμητικών εντυπωσιάστηκε τόσο πολύ, ώστε αποφάσισε να ασχοληθεί με τα μαθηματικά.

Μάλιστα, ο Fermat έγραψε το διάσημο "τελευταίο Θεωρημα του Fermat", στα περιθώρια του βιβλίου Αριθμητικά του Διόφαντου.

Το 1974 ο Αιγύπτιος μαθηματικός Roshdi Rashed ανακάλυψε στο Ιράν, σε Αραβική μετάφραση, 4 επιπλέον από τα 13 βιβλία των Αριθμητικών. Έτσι, σήμερα, έχει σωθεί το περιεχόμενο των 10 από τα 13 βιβλία των Αριθμητικών.

5.1.10 Λυμένες ασκήσεις

Άσκηση 5.12. *Να δειχθεί ότι η εξίσωση* $84x - 44y = 6$ *δεν έχει ακέραιες λύσεις.*

Λύση. Παρατηρούμε ότι κάθε λύση της εξίσωσης $84x + 14y = 6$ αντιστοιχεί στη λύση $(x, -y)$ της εξίσωσης $84x - 44y = 6$ και αντιστρόφως.

Θα δείξουμε ότι $\gcd(84, 44) \nmid 6$.

Σύμφωνα με τον αλγόριθμο του Ευκλείδη έχουμε ότι

$$\begin{aligned} 84 &= 1 \cdot 44 + 40 \\ 44 &= 1 \cdot 40 + 4 \\ 40 &= 10 \cdot 4 + 0, \end{aligned}$$

οπότε προκύπτει ότι $\gcd(84, 44) = 4$. Επειδή $4 \nmid 6$, έπεται ότι η εξίσωση είναι αδύνατη. □

Άσκηση 5.13. *Να βρεθούν όλες οι ακέραιες λύσεις της εξίσωσης* $133x + 49y = 35$.

Λύση. Ακολουθώντας τον αλγόριθμο του Ευκλείδη έχουμε ότι

$$\begin{aligned} 133 &= 2 \cdot 49 + 35 \\ 49 &= 1 \cdot 35 + 14 \\ 35 &= 2 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0, \end{aligned}$$

οπότε $\gcd(133, 49) = 7$. Επειδή $7 \mid 35$, έπεται ότι η εξίσωση έχει λύση.

Από τον επεκτεταμένο αλγόριθμο του Ευκλείδη έχουμε ότι

$$\begin{aligned} 7 &= 1 \cdot 35 + (-2) \cdot 14 = 1 \cdot 35 + (-2) \cdot (1 \cdot 49 + (-1) \cdot 35) \\ &= (-2) \cdot 49 + 3 \cdot 35 = (-2) \cdot 49 + 3 \cdot (1 \cdot 133 + (-2) \cdot 49) \\ &= 3 \cdot 133 + (-8) \cdot 49. \end{aligned}$$

Άρα, το ζεύγος $(x, y) = (3, -8)$ είναι λύση της εξίσωσης $133x + 49y = 7$. Πολλαπλασιάζοντας με 5 προκύπτει ότι το ζεύγος $(x, y) = (15, -40)$ είναι λύση της εξίσωσης $133x + 49y = 35$.

Τέλος, οι λύσεις της εξίσωσης $133x + 49y = 35$ είναι όλα τα ζεύγη (x, y) της μορφής

$$(x, y) = (15 + \frac{49}{7}\lambda, -40 - \frac{133}{7}\lambda) = (15 + 7\lambda, -40 - 19\lambda), \text{ όπου } \lambda \in \mathbb{Z}.$$ □

Άσκηση 5.14. *Να βρεθεί το πλησιέστερο στην αρχή των αξόνων σημείο με ακέραιες συντεταγμένες, από το οποίο διέρχεται η ευθεία* $133x + 49y = 35$.

Λύση. Από την προηγούμενη άσκηση έχουμε ότι κάθε σημείο (x, y) με ακέραιες συντεταγμένες το οποίο ανήκει στην ευθεία $133x + 49y = 35$ έχει συντεταγμένες της μορφής

$$(x, y) = (15 + 7\lambda, -40 - 19\lambda), \text{ όπου } \lambda \in \mathbb{Z}.$$

Η απόσταση των σημείων αυτών από την αρχή των αξόνων ισούται με

$$\sqrt{(15 + 7\lambda)^2 + (-40 - 19\lambda)^2} = \sqrt{410t^2 + 1730t + 1825}.$$

Η απόσταση γίνεται ελάχιστη όταν η υπόρριζη ποσότητα γίνεται ελάχιστη.

Θεωρούμε το πολυώνυμο $f(x) = 410x^2 + 1730x + 1825$. (Η διακρίνουσα του είναι αρνητική άρα $f(x) > 0$ για κάθε $x \in \mathbb{R}$.)

Επίσης, $f'(x) = 820x + 1730$. Η εξίσωση $f'(x) = 0$ έχει λύση $x = -\frac{1730}{820} \simeq -2.1$.

Οι πλησιέστεροι ακέραιοι είναι τα -1, -2 και -3. Για $t = -1$ το σημείο $(8, 21)$ ικανοποιεί την εξίσωση της ευθείας και απέχει απόσταση $\sqrt{505}$ από την αρχή των αξόνων, για $t = -2$ το σημείο $(1, -2)$ ανήκει στην ευθεία και απέχει απόσταση $\sqrt{5}$ και για $t = -3$ το σημείο $(-6, 17)$ ανήκει στην ευθεία και απέχει απόσταση $\sqrt{325}$.

Άρα, το σημείο $(x, y) = (1, -2)$ είναι το πλησιέστερο σημείο στην αρχή των αξόνων που ανήκει στην ευθεία $133x + 49y = 35$ και έχει ακέραιες συντεταγμένες. □

Στην επόμενη άσκηση δίδεται ένα παράδειγμα για το πως μπορούμε να χρησιμοποιήσουμε τις παραπάνω ιδέες για να λύσουμε γραμμικές διοφαντικές εξισώσεις με 3 ή περισσότερους αγνώστους.

Άσκηση 5.15. *Να βρεθούν όλες οι ακέραιες λύσεις της διοφαντικής εξίσωσης*

$$500x + 68y + 30z = 18.$$

Λύση. Παρατηρούμε ότι για κάθε $x, y \in \mathbb{Z}$ ισχύει ότι

$$500x + 68y = \gcd(500, 68) \cdot r_1 \text{ για κάποιο ακέραιο } r_1.$$

Επομένως, η εξίσωση $500x + 68y + 30z = 18$ είναι ισοδύναμη με το σύστημα εξισώσεων

$$\begin{cases} 500x + 68y = \gcd(500, 68) \cdot r_1 \\ \gcd(500, 68) \cdot r_1 + 30z = 18 \end{cases}$$

Με τον αλγόριθμο του Ευκλείδη υπολογίζουμε τον μκδ των 500 και 68:

$$\begin{aligned} 500 &= 7 \cdot 68 + 24 \\ 68 &= 2 \cdot 24 + 20 \\ 24 &= 1 \cdot 20 + 4 \\ 20 &= 5 \cdot 4 + 0 \end{aligned}$$

Άρα, $\gcd(500, 68) = 4$.

Άρα, η εξίσωση $500x + 68y + 30z = 18$ είναι ισοδύναμη με το σύστημα εξισώσεων

$$\begin{cases} 500x + 68y = 4r_1 \\ 4r_1 + 30z = 18 \end{cases}$$

Χρησιμοποιώντας τον επεκτεταμένο αλγόριθμο του Ευκλείδη βρίσκουμε τις λύσεις της πρώτης εξίσωσης του συστήματος:

$$\begin{aligned} 4 &= 1 \cdot 24 + (-1)20 = 1 \cdot 24 + (-1)(1 \cdot 68 + (-2) \cdot 24) \\ &= (-1) \cdot 68 + 3 \cdot 24 = (-1) \cdot 68 + 3 \cdot (1 \cdot 500 + (-7) \cdot 68) \\ &= 3 \cdot 500 + (-22) \cdot 68. \end{aligned}$$

Άρα, το ζεύγος $(x, y) = (3, -22)$ είναι λύση της εξίσωσης $500x + 68y = 4$. Πολλαπλασιάζοντας με r_1 προκύπτει ότι το ζεύγος $(x, y) = (3r_1, -22r_1)$ είναι λύση της εξίσωσης $500x + 68y = 4r_1$. Επομένως, οι λύσεις της εξίσωσης $500x + 68y = 4r_1$ είναι όλα τα ζεύγη (x, y) της μορφής

$$(x, y) = (3r_1 - \frac{68}{4}\lambda_1, -22r_1 + \frac{500}{4}\lambda_1) = (3r_1 - 17\lambda_1, -22r_1 + 125\lambda_1), \text{ όπου } \lambda_1 \in \mathbb{Z}.$$

Πάλι χρησιμοποιώντας τον επεκτεταμένο αλγόριθμο του Ευκλείδη βρίσκουμε τις λύσεις της δεύτερης εξίσωσης του συστήματος:

$$\begin{aligned} 30 &= 7 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 2. \end{aligned}$$

Άρα, $\gcd(30, 4) = 2$ και $2 \mid 18$. Επίσης, άμεσα έχουμε ότι

$$2 = 1 \cdot 30 + (-7) \cdot 4.$$

Άρα, το ζεύγος $(r_1, z) = (-7, 1)$ είναι λύση της εξίσωσης $4r_1 + 30z = 2$. Πολλαπλασιάζοντας με 9 προκύπτει ότι το ζεύγος $(r_1, z) = (-63, 9)$ είναι λύση της εξίσωσης $4r_1 + 30z = 18$. Επομένως, οι λύσεις της εξίσωσης $4r_1 + 30z = 18$ είναι όλα τα ζεύγη (r_1, z) της μορφής

$$(r_1, z) = (-63 + \frac{30}{2}\lambda_2, 9 - \frac{4}{2}\lambda_2) = (-63 + 15\lambda_2, 9 - 2\lambda_2), \text{ όπου } \lambda_2 \in \mathbb{Z}.$$

Για να βρούμε τις λύσεις της αρχικής εξίσωσης $500x + 68y + 30z = 18$ αρκεί να απαλείψουμε την βοηθητική μεταβλητή r_1:

$$x = 3r_1 - 17\lambda_1 = 3(-63 + 15\lambda_2) - 17\lambda_1 = -189 + 45\lambda_2 - 17\lambda_1$$

$$y = -22r_1 + 125\lambda_1 = -22(-63 + 15\lambda_2) + 125\lambda_1 = 1386 - 330\lambda_2 + 125\lambda_1$$

$$z = 9 - 2\lambda_2$$

Τελικά, οι λύσεις τις εξίσωσης $500x + 68y + 30z = 18$ είναι οι τριάδες της μορφής

$$(x, y, z) = (-189 + 45\lambda_2 - 17\lambda_1, 1386 - 330\lambda_2 + 125\lambda_1, 9 - 2\lambda_2) \text{ όπου } \lambda_1, \lambda_2 \in \mathbb{Z}. \qquad \square$$

5.1.11 Ασκήσεις προς επίλυση

1) Να εξετασθεί για ποιές από τις παρακάτω διοφαντικές εξισώσεις υπάρχει λύση, και για οποίες υπάρχει να βρεθεί.

i) $2x + 3y = 4$.
ii) $17x + 19y = 23$.
iii) $15x + 51y = 41$.
iv) $23x + 29y = 25$.
v) $12x + 18y = 20$.
vi) $21x + 19y = 5$.
vii) $10x - 8y = 42$.
viii) $121x - 88y = 572$.

2) Να λυθεί η διοφαντική εξίσωση $500x + 230y + 206z = 50$.

Υπόδειξη: Θεωρείστε το σύστημα

$$\begin{cases} 500x + 230y = 10r_1 \\ 10r_1 + 206z = 50. \end{cases}$$

3) Να λυθεί η διοφαντική εξίσωση $70x + 20y + 45z + 15w = 10$.

Υπόδειξη: Θεωρείστε το σύστημα

$$\begin{cases} 70x + 20y = 10r_1 \\ 10r_1 + 45z = 5r_2 \\ 5r_2 + 15w = 10. \end{cases}$$

4) Έστω $a, b \in \mathbb{N}^*$ με $\gcd(a, b) = 1$. Να δειχθεί ότι κάθε φυσικός αριθμός $k \geq (a-1)(b-1)$ γράφεται στην μορφή $ax + by$ όπου $x, y \in \mathbb{N}$.

5) Να λυθεί η επόμενη διοφαντική εξίσωση: $\frac{1}{x} + \frac{1}{y} = \frac{1}{a}$, όπου $a \in \mathbb{Z}$.

5.1.12 Ελάχιστο κοινό πολλαπλάσιο

Έστω a, b μη μηδενικοί φυσικοί αριθμοί. Το **ελάχιστο κοινό πολλαπλάσιο** (εκπ) των a και b είναι ο μικρότερος φυσικός αριθμός ο οποίος διαιρείται και από τους δύο αριθμούς και συμβολίζεται με $\text{εκπ}(a, b)$, ή $\text{lcm}(a, b)$.

Ισοδύναμα, ο m είναι το εκπ των ακεραίων a και b αν και μόνο αν $m > 0$, $a|m, b|m$ και $m|n$ όπου n είναι κοινό πολλαπλάσιο των a και b.

Για παράδειγμα, το ελάχιστο κοινό πολλαπλάσιο των $12, 18$ είναι το 36, συμβολικά $\text{εκπ}(12, 18) = 36$, το ελάχιστο κοινό πολλαπλάσιο των $12, 7$ είναι το 84, συμβολικά $\text{εκπ}(12, 7) = 84$, και το ελάχιστο κοινό πολλαπλάσιο των $12, 4$ είναι το 12, συμβολικά $\text{εκπ}(12, 4) = 12$.

Παρατηρήσεις.

1. Αν $\text{εκπ}(a_1, \ldots, a_n) = m \neq 0$, τότε $\gcd(\frac{m}{a_1}, \ldots, \frac{m}{a_n}) = 1$.

   Για παράδειγμα, $\text{εκπ}(12, 30, 40) = 120$, οπότε

   $$\gcd\left(\frac{120}{12}, \frac{120}{30}, \frac{120}{40}\right) = \gcd(10, 4, 3) = 1.$$

2. Το ελάχιστο κοινό πολλαπλάσιο των ακέραιων αριθμών $a_1, \ldots, a_n$ **δεν** μεταβάλλεται αν ορισμένοι από αυτούς αντικατασταθούν με το εκπ τους. Έτσι έχουμε

   $$\text{εκπ}(13, 39, 154) = \text{εκπ}(\text{εκπ}(13, 39), 154) = \text{εκπ}(13, \text{εκπ}(39, 154)).$$

3. Αν οι ακέραιοι αριθμοί $a_1, \ldots, a_n$ είναι πρώτοι προς αλλήλους, τότε

   $$\text{εκπ}(a_1, \ldots, a_n) = |a_1 \cdots a_n|.$$

Η επόμενη πρόταση δίνει ένα τύπο για τον υπολογισμό του εκπ δύο αριθμών με τη βοήθεια του υπολογισμού του μκδ τους.

Πρόταση 5.12 (Ελάχιστο κοινό πολλαπλάσιο). *Αν $ab \neq 0$, τότε*

$$\varepsilon\kappa\pi(a, b) = \frac{ab}{\gcd(a, b)}.$$

Απόδειξη. Έστω

$$a = a' \cdot \gcd(a, b)$$
$$b = b' \cdot \gcd(a, b).$$

Τότε

$$\gcd(a', b') = 1.$$

Επίσης, έστω

$$\text{εκπ}(a, b) = a''a$$
$$\text{εκπ}(a, b) = b''b.$$

Τότε

$$\gcd(a'', b'') = 1.$$

Επομένως, διαιρώντας κατά μέλη, από τις πρώτες δύο σχέσεις προκύπτει ότι

$$\frac{a}{b} = \frac{a'}{b'}$$

και από τις δύο τελευταίες προκύπτει ότι

$$\frac{a}{b} = \frac{b''}{a''}.$$

Άρα

$$\frac{a'}{b'} = \frac{b''}{a''},$$

δηλαδή

$$a'a'' = b'b''.$$

Επειδή $a' \mid b'b''$ και $\gcd(a', b') = 1$, ισχύει ότι $a' \mid b''$.
Επειδή $b'' \mid a'a''$ και $\gcd(a'', b'') = 1$, ισχύει ότι $b'' \mid a'$.
Επομένως, από τις ιδιότητες της διαιρετότητας προκύπτει ότι

$$a' = b''.$$

Συνεπώς

$$\text{εκπ}(a, b) = a'b,$$

οπότε

$$\text{εκπ}(a, b)\gcd(a, b) = a'\gcd(a, b)b$$

και επειδή $a' \cdot \gcd(a, b) = a$ προκύπτει ότι

$$\text{εκπ}(a, b)\gcd(a, b) = ab. \qquad \square$$

Για παράδειγμα,

$$\text{εκπ}(12, 30) = \frac{12 \cdot 30}{\gcd(12, 30)} = \frac{360}{6} = 60.$$

5.1.13 Πρώτοι αριθμοί

Ένας φυσικός αριθμός p ονομάζεται **πρώτος αριθμός** αν ο p διαιρείται μόνο από το 1 και τον p. Στην περίπτωση που υπάρχουν και άλλοι διαιρέτες ο αριθμός p ονομάζεται **σύνθετος**. Για λόγους που θα εξηγήσουμε παρακάτω, ο αριθμός 1 δεν θεωρείται ούτε πρώτος ούτε σύνθετος.

Στον επόμενο πίνακα σημειώνονται με έντονα στοιχεία οι πρώτοι αριθμοί από το 1 εώς το 100, (συνολικά υπάρχουν 25 πρώτοι αριθμοί στο διάστημα 1 εώς 100).

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Οι πρώτοι αριθμοί βρίσκονται στην καρδιά της έρευνας στην Θεωρία Αριθμών. Στην ενότητα αυτή θα δούμε ορισμένα προκαταρκτικά αποτελέσματα σχετικά με τους πρώτους αριθμούς. Στις επόμενες ενότητες καθώς αποκτούμε περισσότερα εργαλεία θα εμπλουτίζουμε και τις γνώσεις μας σχετικά με τους πρώτους αριθμούς.

Πρόταση 5.13. *Κάθε φυσικός αριθμός $n \geq 2$ είναι πρώτος, ή γινόμενο πρώτων αριθμών.*

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή ως προς το n. Για $n = 2$ η πρόταση είναι αληθής, αφού ο 2 είναι πρώτος.

Έστω ότι κάθε αριθμός $k \leq n$ είναι πρώτος ή γινόμενο πρώτων αριθμών. Θα αποδείξουμε ότι το ίδιο ισχύει και για τον $n+1$.

Αν ο $n+1$ είναι πρώτος, τότε η πρόταση ισχύει.

Αν ο $n+1$ είναι σύνθετος, τότε υπάρχουν φυσικοί αριθμοί a, b ώστε

$$n+1 = ab, \text{ όπου } 2 \leq a, b \leq n.$$

Επειδή $2 \leq a, b \leq n$, από την υπόθεση της επαγωγής ο a είτε είναι πρώτος είτε γινόμενο πρώτων. Ομοίως, ο b είτε είναι πρώτος είτε είναι γινόμενο πρώτων. Συνεπώς, ο $ab = n+1$ είναι γινόμενο πρώτων. Άρα η πρόταση ισχύει για κάθε φυσικό αριθμό $n \geq 2$. □

Άραγε υπάρχουν άπειροι πρώτοι αριθμοί; Η απάντηση είναι καταφατική. Ο Ευκλείδης στο βιβλίο του Στοιχεία δίνει την επόμενη πρόταση.

Πρόταση 5.14. *Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.*

Απόδειξη. Έστω ότι δεν υπάρχουν άπειροι πρώτοι αριθμοί και έστω $p_1, p_2, \ldots, p_k$ όλοι οι πρώτοι αριθμοί, όπου $k \in \mathbb{N}^*$.

Θεωρούμε τον αριθμό

$$N = p_1 p_2 \cdots p_k + 1$$

Προφανώς, $N > p_i$ για κάθε $i \in [k]$.

Από την προηγούμενη πρόταση ο N είτε είναι πρώτος είτε γινόμενο πρώτων αριθμών.

Αν ο αριθμός N είναι πρώτος, τότε περιέχεται ανάμεσα στους $p_1, p_2, \ldots, p_k$, άτοπο.

Αν ο αριθμός N είναι σύνθετος, τότε υπάρχουν πρώτοι που είναι διαιρέτες του N. Αλλά, η διαίρεση του N με κάθε πρώτο αριθμό p_i αφήνει υπόλοιπο 1 επομένως $p_i \nmid N$ για κάθε $i \in [k]$, άτοπο. □

Πρόταση 5.15 (Λήμμα του Ευκλείδη). *Έστω p πρώτος αριθμός και $a, b \in \mathbb{Z}$. Τότε*

i) $p|a$ ή $\gcd(a, p) = 1$,

ii) Αν $p|ab$, τότε $p|a$ ή/και $p|b$.

Απόδειξη.

i) Οι μόνοι διαιρέτες του p είναι το 1 και το p. Άρα, $\gcd(a, p) = 1$ ή $\gcd(a, p) = p$.

Ισχύει ότι

$$\gcd(a, p) \mid a.$$

Επομένως,

$$p \mid a \text{ ή } \gcd(a, p) = 1.$$

ii) Έστω ότι $p|ab$ και $p \nmid a$. Τότε $\gcd(a, p) = 1$. Άρα υπάρχουν κέραιοι $s, t \in \mathbb{Z}$ τέτοιοι ώστε

$$1 = sa + tp.$$

Επομένως θα ισχύει ότι

$$b = bsa + btp.$$

Από την υπόθεση ισχύει ότι $p \mid ab$, επομένως $p \mid bsa$. Επίσης $p \mid btp$, επομένως $p \mid (bsa + btp)$, δηλαδή $p \mid b$. Με τον ίδιο τρόπο, αν $p \nmid b$ αποδεικνύεται ότι $p \mid a$. □

Παρατήρηση. Αν ο p δεν είναι πρώτος αριθμός τότε τα προηγούμενα αποτελέσματα ενδέχεται να μην ισχύουν. Πράγματι, αν $p = 4$, $a = 6$ και $b = 10$ έχουμε ότι αφενός $p \nmid a$ αλλά $\gcd(a, p) = 2 \neq 1$ και αφετέρου $p \mid ab$ δηλαδή $4 \mid 60$, αλλά $4 \nmid 6$ και $4 \nmid 10$.

Με την βοήθεια της προηγούμενης πρότασης εύκολα προκύπτουν τα επόμενα πορίσματα.

Πόρισμα 5.16. *Αν p είναι πρώτος αριθμός και $p \mid a_1 \cdot a_2 \cdots a_n$, τότε $p \mid a_i$ για κάποιο $i \in [n]$.*

Πόρισμα 5.17. *Αν p είναι πρώτος και $p | q_1 \cdot q_2 \cdots q_n$ όπου $q_1, q_2, \ldots, q_n$ είναι πρώτοι αριθμοί, τότε $q_i = p$ για κάποιο $i \in [n]$.*

Η επόμενη πρόταση αποδεικνύει ότι οι πρώτοι αριθμοί μπορούν να θεωρηθούν ως οι "δομικοί λίθοι" των φυσικών αριθμών.

Πρόταση 5.18 (Θεμελιώδες Θεώρημα της Αριθμητικής). *Κάθε φυσικός αριθμός $n \geq 2$ εκφράζεται κατά μοναδικό τρόπο ως γινόμενο πρώτων (χωρίς να μας ενδιαφέρει η σειρά με την οποία εμφανίζονται στο γινόμενο οι παράγοντες).*

Απόδειξη. Από την Πρόταση 5.13, κάθε αριθμός $n \geq 2$ γράφεται ως γινόμενο πρώτων αριθμών. Έστω

$$n = p_1 p_2 \cdots p_k,$$

όπου $p_1, p_2, \ldots, p_k$ είναι πρώτοι αριθμοί. Θα αποδειχθεί ότι το γινόμενο αυτό είναι μοναδικό. Έστω ότι

$$n = q_1 q_2 \cdots q_r,$$

όπου $q_1, q_2, \ldots, q_r$ είναι επίσης πρώτοι αριθμοί, δηλαδή

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r.$$

Αν διαγράψουμε όλους τους κοινούς παράγοντες των γινομένων της ισότητας και προκύψει $1 = 1$ το θεώρημα ισχύει. Σε αντίθετη περίπτωση έστω ότι μετά την διαγραφή των κοινών παραγόντων προκύπτει η ισότητα

$$p'_1 p'_2 \cdots p'_l = q'_1 q'_2 \cdots q'_s.$$

Επειδή $p_1 \mid q'_1 q'_2 \cdots q'_s$, από το προηγούμενο πόρισμα προκύπτει ότι $p_1 \mid q_i$ για κάποιο $i \in [s]$, άτοπο, αφού τα δύο γινόμενα δεν έχουν κοινούς παράγοντες. Επομένως, η ανάλυση σε πρώτους παράγοντες είναι μοναδική. □

Παρατήρηση. Από την προηγούμενη πρόταση προκύπτει ότι κάθε φυσικός αριθμός $n \geq 2$ παριστάνεται μονοσήμαντα ως

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

όπου p_1, p_2, ..., p_k είναι πρώτοι αριθμοί (διαφορετικοί ανά δύο) και a_1, a_2, ..., a_k είναι φυσικοί αριθμοί. Αυτή η ανάλυση ονομάζεται **κανονική παραγοντοποίηση** του αριθμού n.

Για παράδειγμα, ο αριθμός 84 αναλύεται ως γινόμενο

$$84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3 \cdot 7.$$

Ο αριθμός 2 εισέρχεται στην παραγοντοποίηση του 84 υψωμένος στο τετράγωνο, ενώ το 3 και το 7 στην πρώτη. Μπορούμε να υποθέσουμε ότι και το 5 εισέρχεται στην παραγοντοποίηση του 84 αλλά υψωμένο στην μηδενική δύναμη και γενικά ότι όλοι οι πρώτοι αριθμοί εισέρχονται σε μια παραγοντοποίηση αλλά μερικοί υψωμένοι στην μηδενική δύναμη. Καταλαβαίνουμε τώρα γιατί δεν είναι βολικό να θεωρούμε το 1 πρώτο αριθμό. Αυτός ο αριθμός μπορεί να περιληφθεί σε κάθε παραγοντοποίηση υψωμένος σε οποιαδήποτε δύναμη. Για παράδειγμα,

$$84 = 1^2 \cdot 2^2 \cdot 3 \cdot 7 = 1^{200} \cdot 2^2 \cdot 3 \cdot 7,$$

γεγονός που αναιρεί το μονοσήμαντο.

5.1.14 Ασκήσεις προς επίλυση

1) Να βρεθεί η κανονική παραγοντοποίηση του 20!.

2) Να δειχθεί ότι αν p είναι περιττός πρώτος αριθμός, τότε γράφεται κατά μοναδικό τρόπο ως διαφορά δύο τετραγώνων.

3) Να δειχθεί ότι ο αριθμός $4^{2n+1} + 1$ δεν είναι πρώτος για κανένα $n \in \mathbb{N}$.

4) Να δειχθεί ότι οι αριθμοί της μορφής $F_n = 2^{2^n} + 1$ δεν είναι όλοι πρώτοι.

5) Να κατασκευασθεί πρόγραμμα που ελέγχει αν ένας αριθμός είναι πρώτος. Να βρεθούν όλοι οι πρώτοι αριθμοί από το 2 έως το 10000.

6) Ένας πρώτος αριθμός p ονομάζεται υπερπρώτος αν κάθε πρόθεμα της δεκαδικής του αναπαράστασης είναι και αυτός πρώτος αριθμός. Για παράδειγμα, ο αριθμός 719333 είναι υπερπρώτος, διότι οι αριθμοί 7, 71, 719, 7193, 71933 και 719333 είναι πρώτοι αριθμοί.

   Οι υπερπρώτοι αριθμοί με 1 ψηφίο είναι οι: $2, 3, 5, 7$.

   Οι υπερπρώτοι αριθμοί με 2 ψηφία είναι οι: $23, 29, 31, 37, 53, 59, 71, 73, 79$.

   Να βρεθούν όλοι οι υπερπρώτοι αριθμοί μεταξύ του 2 και του 10^{20}.

∗7) Να δειχθεί ότι αν p, q είναι θετικοί ακέραιοι, τότε ο αριθμός

$$\left(p + \frac{1}{2}\right)^n + \left(q + \frac{1}{2}\right)^n$$

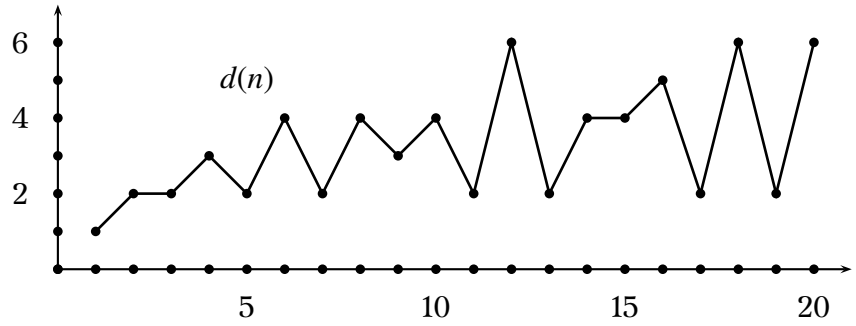
είναι ακέραιος μόνο για πεπερασμένο πλήθος φυσικών αριθμών n.

5.1.15 Παράρτημα: Πόσους διαιρέτες έχει ένας αριθμός;

Έστω $n \geq 2$ ένας φυσικός αριθμός. Ένα ενδιαφέρον ερώτημα είναι, πόσους διαιρέτες έχει ο αριθμός n; Για παράδειγμα, το 84 έχει 12 διαιρέτες τους 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84.

Το πλήθος των διαιρετών του n συμβολίζεται με $d(n)$ (ή $\tau(n)$). Άρα, $d(84) = 12$. Οι τιμές της $d(n)$ για κάθε n μικρότερο ή ίσο του 20 δίνονται στον επόμενο πίνακα.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6	2	6



Η συμπεριφορά της συνάρτησης $d(n)$ μοιάζει χαοτική. Είναι δυνατόν να εκφράσουμε την συνάρτηση $d(n)$ με κάποιο τύπο; Η απάντηση είναι καταφατική και είναι αρκετά απλή.

Ας εκφράσουμε τον αριθμό n στην κανονική παραγοντοποίησή του

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

όπου $p_1, p_2, \ldots, p_k$ πρώτοι αριθμοί και $a_1, a_2, \ldots, a_k$ φυσικοί αριθμοί.

Τότε, οι διαιρέτες του n είναι όλοι οι αριθμοί της μορφής

$$p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

όπου $0 \leq b_1 \leq a_1$, $0 \leq b_2 \leq a_2$, …, $0 \leq b_k \leq a_k$.

Κάθε διαιρέτης του n καθορίζεται μονοσήμαντα από τα $b_1, b_2, \ldots, b_k$.

Για το b_1 υπάρχουν $a_1 + 1$ επιλογές.

Για το b_2 υπάρχουν $a_2 + 1$ επιλογές.

…

Για το b_k υπάρχουν $a_k + 1$ επιλογές.

Επομένως, από την αρχή του γινομένου συνολικά υπάρχουν $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ επιλογές, δηλαδή για τον αριθμό $d(n)$ των διαιρετών του n ισχύει ότι

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1).$$

Χρησιμοποιώντας αυτόν τον τύπο μπορούμε να υπολογίσουμε το πλήθος των διαιρετών οποιουδήποτε αριθμού αφού όμως πρώτα τον αναλύσουμε σε γινόμενο πρώτων παραγόντων, ώστε να βρούμε τους εκθέτες $a_1, a_2, \ldots, a_n$. Αυτό όμως δεν είναι πάντα εύκολο – όταν ο αριθμός είναι μεγάλος είναι δύσκολο να βρούμε την κανονική παραγοντοποίησή του.

Για παράδειγμα, επειδή $84 = 2^2 \cdot 3^1 \cdot 7^1$ έπεται ότι

$$d(84) = (2 + 1)(1 + 1)(1 + 1) = 3 \cdot 2 \cdot 2 = 12.$$

Ασκήσεις προς επίλυση

1) Να ευρεθεί το πλήθος των διαιρετών των αριθμών 124, 650, και 7! και στη συνέχεια να ευρεθούν οι αντίστοιχοι διαιρέτες τους.

2) Να αποδειχθεί ότι αν n είναι σύνθετος τότε $d(n) > 2$.

3) Να βρεθεί η μέγιστη τιμή της $d(n)$ όταν $1 \leq n \leq 1000$.

4) Να αποδειχθεί ότι το πλήθος των διαιρετών του φυσικού αριθμού n είναι περιττό αν και μόνο αν το n είναι τέλειο τετράγωνο.

5) Να αποδειχθεί ότι για κάθε $a, b \in \mathbb{N}^*$ με $\gcd(a, b) = 1$ ισχύει ότι $d(ab) = d(a)d(b)$.

6) Να αποδειχθεί ότι αν η κανονική παραγοντοποίηση του n περιέχει k διαφορετικούς πρώτους παράγοντες, δηλαδή

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

τότε υπάρχουν ακριβώς $2^{k-1} - 1$ παραγοντοποιήσεις του n ως γινόμενο σχετικά πρώτων ακεραίων.

5.1.16 Παράρτημα: Πως ελέγχουμε αν ένας αριθμός είναι πρώτος;

Όπως φαίνεται και από το θεμελιώδες θεώρημα της αριθμητικής, οι πρώτοι αριθμοί είναι οι "δομικοί λίθοι" των φυσικών αριθμών. Πώς όμως βρίσκουμε τους πρώτους παράγοντες ενός αριθμού; Πριν απαντήσουμε στο πρόβλημα αυτό, πώς ελέγχουμε αν ένας αριθμός είναι πρώτος ή όχι;

Με τα εργαλεία που έχουμε μάθει μέχρι τώρα ο μόνος τρόπος για να αποφασίσουμε αν ένας αριθμός είναι πρώτος, είναι να τον διαιρέσουμε με τους μικρότερούς του φυσικούς αριθμούς και να ελέγξουμε αν κάποιος τον διαιρεί ή όχι.

Επομένως, αν $n = 173$ χρειάζονται $173 - 2 = 171$ διαιρέσεις (εξαιρούμε το 1 και το 173).

Μια απλή ιδέα για την βελτίωση αυτής μεθόδου μας δίνει η επόμενη πρόταση.

Πρόταση 5.19. *Αν ο φυσικός αριθμός n είναι σύνθετος, τότε τουλάχιστον ένας πρώτος διαιρέτης του είναι μικρότερος ή ίσος του $\sqrt{n}$.*

Απόδειξη. Αφού ο n είναι σύνθετος υπάρχουν φυσικοί αριθμοί a, b ώστε

$$n = ab, \text{ όπου } 2 \leq a, b \leq n.$$

Αν $a, b > \sqrt{n}$ τότε $ab > \sqrt{n}\sqrt{n} = n$, άτοπο. Άρα, τουλάχιστον ένας από τους a, b είναι μικρότερος ή ίσος του $\sqrt{n}$ και κατά συνέπεια οι πρώτοι διαιρέτες εκείνου, που είναι και πρώτοι διαιρέτες του n, θα είναι επίσης μικρότεροι ή ίσοι του $\sqrt{n}$. □

Επομένως, για να εξακριβώσουμε αν ένας αριθμός είναι πρώτος ή όχι, αρκεί να εξετάσουμε αν διαιρείται από τους πρώτους αριθμούς που είναι μικρότεροι ή ίσοι του $\sqrt{n}$, ή ισοδύναμα του $\lfloor \sqrt{n} \rfloor$.

Για παράδειγμα, ο αριθμός 173 είναι πρώτος. Πράγματι, αφού $13 < \sqrt{173} < 14$, αρκεί να ελέγξουμε αν 173 διαιρείται με κάποιον από τους πρώτους αριθμούς που είναι μικρότεροι ή ίσοι από το 13. Οι πρώτοι αριθμοί που είναι μικρότεροι ή ίσοι του 13 είναι οι 2, 3, 5, 7, 11 και 13. Κανένας από αυτούς δεν διαιρεί τον 173, άρα ο 173 είναι πρώτος.

Στην Κρυπτογραφία συχνά χρησιμοποιούνται αριθμοί με δεκάδες ή εκατοντάδες ψηφίων. Πόσες διαιρέσεις χρειαζόμαστε για να εξακριβώσουμε αν ένας αριθμός με k ψηφία είναι πρώτος ή όχι;

Πριν απαντήσουμε στο ερώτημα αυτό ας δούμε πρώτα πόσα ψηφία έχει ένας αριθμός n στην δεκαδική του αναπαράσταση.

Πρόταση 5.20. *Ο αριθμός n έχει $\lfloor \log_{10} n \rfloor + 1$ ψηφία.*

Απόδειξη. Έστω ότι ο αριθμός n έχει k ψηφία. Τότε θα ισχύει ότι

$$10^{k-1} \leq n < 10^k,$$

διότι ο ελάχιστος αριθμός με k ψηφία είναι ο αριθμός

$$1\underbrace{00\cdots0}_{k-1 \text{ φορές}} = 10^{k-1}$$

ενώ ο μέγιστος αριθμός με k ψηφία είναι ο αριθμός

$$\underbrace{99\cdots9}_{k \text{ φορές}} = 1\underbrace{00\cdots0}_{k \text{ φορές}} - 1 = 10^k - 1.$$

Επομένως,

$$k-1 \leq \log_{10} n \text{ και } \log_{10} n < k,$$

οπότε

$$\log_{10} n < k \leq 1 + \log_{10} n$$

και άρα

$$k = \lfloor \log_{10} n \rfloor + 1,$$

δηλαδή ο αριθμός n έχει $\lfloor \log_{10} n \rfloor + 1$ ψηφία. □

Για παράδειγμα, ο αριθμός $n = 77$ έχει $\lfloor \log_{10} 77 \rfloor + 1 = \lfloor 1.886 \rfloor + 1 = 1 + 1 = 2$ ψηφία.

Ο αριθμός $n = 1000$ έχει $\lfloor \log_{10} 1000 \rfloor + 1 = 3 + 1 = 4$ ψηφία.

Ο αριθμός $n = 77^{10}$ έχει $\lfloor \log_{10} 77^{10} \rfloor + 1 = \lfloor 10 \log_{10} 77 \rfloor + 1 = \lfloor 10 \cdot 1.886 \rfloor + 1 = \lfloor 18.66 \rfloor + 1 = 18 + 1 = 19$ ψηφία, (πράγματι $77^{10} = 73266804725862006 49$).

Παρατήρηση. Αν ο αριθμός n έχει k ψηφία, τότε $10^{(k-1)/2} \leq \sqrt{n} \leq 10^{k/2}$.

Πράγματι, επειδή, ο n έχει k ψηφία θα ισχύει ότι

$$10^{k-1} \leq n < 10^k$$

οπότε

$$10^{(k-1)/2} \leq \sqrt{n} \leq 10^{k/2}.$$

Επομένως, για να ελέγξουμε αν ένας αριθμός με 100 ψηφία είναι πρώτος ή όχι, θα χρειαστούμε να εκτελέσουμε περίπου $10^{100/2} = 10^{50}$ διαιρέσεις.

Για να εκτιμήσουμε το χρόνο που απαιτείται για να ολοκληρωθούν αυτές οι διαιρέσεις, ας υποθέσουμε ότι ένας υπολογιστής εκτελεί 10^{10} διαιρέσεις το δευτερόλεπτο, δηλαδή 10 δισεκατομύρια διαιρέσεις το δευτερόλεπτο. Τότε για να εκτελέσει 10^{50} διαιρέσεις θα χρειάστει $\frac{10^{50}}{10^{10}} = 10^{40}$ δευτερόλεπτα. Κάθε χρόνος έχει $365 \times 24 \times 60 \times 60 = 31536000$ δευτερόλεπτα, επομένως θα χρειαστεί περίπου $\frac{10^{40}}{31536000} = 3 \cdot 10^{32}$ χρόνια!

Είναι φανερό ότι η μέθοδος αυτή εφαρμοζεται μόνο για αριθμούς με μικρό αριθμό ψηφίων. Στις επόμενες ενότητες θα εφοδιαστούμε με εργαλεία που μας επιτρέπουν να αποφασίζουμε γρήγορα αν ένας αριθμός είναι πρώτος ή σύνθετος.

Ασκήσεις προς επίλυση

1) Να κατασκευασθεί πρόγραμμα που ελέγχει αν ένας αριθμός είναι πρώτος. Να βρεθούν όλοι οι πρώτοι αριθμοί από το 2 εως το 10000.

2) Να ευρεθεί το πλήθος των ψηφίων των επόμενων αριθμών.

   i) 10^{2011}.

   ii) 2^{10000}, (είναι γνωστό ότι $\log_{10} 2 \approx 0.30103$).

   iii) 702^{100}, (είναι γνωστό ότι $\log_{10} 702 \approx 2.846$).

   iv) 333^{20}, (είναι γνωστό ότι $\log_{10} 333 \approx 2.52244$).

   v) 130000^{10}, (είναι γνωστό ότι $\log_{10} 13 \approx 1.113943$).

   Ποιος από τους παραπάνω αριθμούς είναι ο μικρότερος;

5.1.17 Παράρτημα: Πως βρίσκουμε τους πρώτους αριθμούς;

Το πλήθος των πρώτων αριθμών είναι άπειρο, αλλά για κάθε σταθερό φυσικό αριθμό n υπάρχει πεπερασμένο πλήθος πρώτων αριθμών που είναι μικρότεροι ή ίσοι από αυτόν. Ποιοί είναι αυτοί οι πρώτοι αριθμοι; Δυστυχώς δεν είναι γνωστός κάποιος τύπος που κατασκευάζει διαδοχικά όλους τους πρώτους αριθμούς. Για το λόγο αυτό είναι ενδιαφέρον να βρεθούν αλγόριθμοι που βρίσκουν τους πρώτους αριθμούς.

Μια απλή και ευφυής μέθοδος εύρεσης όλων των πρώτων αριθμών που είναι μικρότεροι ή ίσοι ενός αριθμού n, είναι το λεγόμενο **κόσκινο του Ερατοσθένη**. [4]

Στην συνέχεια δίνεται μια περιγραφή της μεθόδου του Ερατοσθένη μέσω ενός παραδείγματος: Έστω ότι θέλουμε να βρούμε όλους τους πρώτους αριθμούς που είναι μικρότεροι ή ίσοι του 200. Τα βήματα που ακολουθούμε είναι τα εξής:

1. Γράφουμε στη σειρά τους αριθμούς από το 2 έως το 200.

2. Το 2 είναι ο μικρότερος πρώτος αριθμός. Διαγράφουμε από τον πίνακα κάθε δεύτερο αριθμό μετά το 2. Επομένως όλα τα πολλαπλάσια του 2.

3. Το 3 είναι ο επόμενος μεγαλύτερος αριθμός που δεν έχει διαγραφεί και είναι πρώτος. Στη συνέχεια αφήνουμε το 3 και διαγράφουμε κάθε τρίτο αριθμό μετα το 3.

4. Ο επόμενος αριθμός που δεν έχει διαγραφεί είναι ο αριθμός 5 ο οποίος δεν είναι πολλαπλάσιο ούτε του 2 ούτε του 3 (άρα πρώτος) και διαγράφουμε κάθε πέμπτο αριθμό μετά το 5.

5. Ο επόμενος αριθμός που δεν έχει διαγραφεί είναι ο αριθμός 7. Συνεχίζουμε διαγράφοντας κάθε έβδομο αριθμό μετά το 7.

6. Ο επόμενος αριθμός που δεν έχει διαγραφεί είναι το 11. Συνεχίζουμε διαγράφοντας κάθε εντέκατο αριθμό μετά τό 11.

7. Ο επόμενος αριθμός που δεν έχει διαγραφεί είναι το 13. Συνεχίζουμε διαγράφοντας κάθε δέκατο τρίτο αριθμό μετά το 13.

8. Ο επόμενος αριθμός που δεν έχει διαγραφεί είναι το 17.

Όμως, κάθε σύνθετος αριθμός n της λίστας έχει ως διαίρετη ένα πρώτο αριθμό $p \leq \sqrt{n}$.. Άρα, επειδή έχουμε διαγράψει τα πολλαπλάσια όλων των πρώτων που δεν υπερβαίνουν το $14 < \sqrt{200} < 15$, δηλαδή το 15, έπεται ότι έχουμε διαγράψει όλους τους σύνθετους μέχρι το 200 και όλοι οι εναπομείναντες είναι πρώτοι μικρότεροι ή ίσοι του 200. Επομένως η διαδικασία ολοκληρώνεται όταν διαγραφούν όλα τα πολλαπλάσια του 13.

[4] Ο **Ερατοσθένης** (271-194 π.Χ) σπούδασε στην Ακαδημία του Πλάτωνος στην Αθήνα. Ο Βασιλιάς Πτολεμαίος ο Β΄ τον προσκάλεσε στην Αλεξάνδρεια για να διδάξει τον γιο του, και από το 240 π.Χ. ανέλαβε επικεφαλής της βιβλιοθήκης της Αλεξάνδρειας. Οι γνώσεις του Ερατοσθένη είναι πολύπλευρες, με πλούσιο συγγραφικό έργο στα μαθηματικά, στη γεωγραφία, στην αστρονομία, στην ιστορία και στη φιλοσοφία. Εκτός από το έργο του στα μαθηματικά είναι γνωστός για τους υπολογισμούς του που αφορούν το μέγεθος της Γης και για την κατασκευή του πρώτου γνωστού χάρτη που στηριζόταν σε επιστημονικές βάσεις με παράλληλους και μεσημβρινούς, όπως επίσης για την χρονολόγηση της αρχαίας ιστορίας.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Παρατήρηση. Παραλλαγές της μεθόδου αυτής αποτελούν σήμερα τα πιο αποτελεσματικά εργαλεία για την δημιουργία πινάκων πρώτων αριθμών.

Άσκήσεις προς επίλυση

1) Να κατασκευασθεί πρόγραμμα που ελέγχει αν ένας αριθμός είναι πρώτος. Να βρεθούν όλοι οι πρώτοι αριθμοί από το 2 εως το 10000.

∗2) Να κατασκευασθεί πρόγραμμα που βρίσκει τον μεγαλύτερο πρώτο αριθμό που περιέχεται μέσα σε ένα διάστημα. Να βρεθεί ο μεγαλύτερος πρώτος αριθμός μεταξύ του 5000 και 6000.

5.1.18 Παράρτημα: Πόσοι είναι οι πρώτοι αριθμοί μέχρι το n;

Για κάθε πραγματικό αριθμό $x > 0$ συμβολίζουμε με $\pi(x)$ το πλήθος των πρώτων αριθμών p που είναι μικρότεροι ή ίσοι του x.

Για παράδειγμα

$$\pi(1) = 0, \quad \pi(2) = 1, \quad \pi(\frac{5}{2}) = 1,$$

$$\pi(\sqrt{24}) < \pi(5), \quad \text{δηλαδή} \quad \pi(\sqrt{24}) = 2.$$

Δεν είναι γνωστός κάποιος τύπος που να μας δίνει την συνάρτηση $\pi(x)$ συναρτήσει του x.

Το 1792 σε ηλικία 15 ετών ο Carl Friedrich Gauss παρατηρώντας πίνακες των πρώτων αριθμών που είναι μικρότεροι από το 102000, τους οποίους είχε συντάξει ο Johann Lamber, διατύπωσε μια εικασία για την $\pi(x)$.

Σχήμα 5.2: Ο Carl Friedrich Gauss (30 Απριλίου 1777 – 23 Φεβρουαρίου 1855)

Ο Gauss μέτρησε τους πρώτους αριθμούς που περιέχονται σε διαδοχικά διαστήματα φυσικών αριθμών τα οποία έχουν σταθερό μήκος. Έτσι, για παράδειγμα κατασκεύασε πίνακες της μορφής

x	$\pi(x)$	πρώτοι αριθμοί στο διάστημα $x-1000$ έως x	$\Delta(x)$
1000	168	168	0.168
2000	303	135	0.135
3000	430	127	0.127
4000	550	120	0.120
5000	669	119	0.119
6000	783	114	0.114
7000	900	117	0.117
8000	1007	107	0.107
9000	1117	110	0.110
10000	1227	112	0.112

Έστω $\Delta(x) = \frac{\pi(x)-\pi(x-1000)}{1000}$ η "συχνότητα" εμφάνισης πρώτων αριθμών στο διάστημα $x-1000$ εώς x. Κατασκεύαζοντας πολλούς τέτοιους πίνακες για διάφορα μήκη διαστημάτων, ο Gauss παρατήρησε ότι η $\Delta(x)$ μοιάζει να μειώνεται με αργό ρυθμό καθώς το x αυξάνει και άρχισε να την συγκρίνει με διάφορες στοιχειώδεις συναρτήσεις.

Για τον ανάστροφο του φυσικού λογάριθμου του x, δηλαδή για την συνάρτηση $\frac{1}{\ln x}$ και για διαστήματα με μήκος 1000 προκύπτει ο επόμενος πίνακας.

x	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000
$\Delta(x)$	0.168	0.135	0.137	0.120	0.119	0.114	0.117	0.107	0.110	0.112
$\frac{1}{\ln x}$	0.145	0.132	0.125	0.121	0.117	0.115	0.113	0.111	0.110	0.109

Το ταίριασμα των αντίστοιχων τιμών είναι εκπληκτικά καλό και οδήγησε τον Gauss να εικάσει ότι η $\Delta(x)$ είναι περίπου ίση με $\frac{1}{\ln x}$, δηλαδή

$$\Delta(x) \approx \frac{1}{\ln x}.$$

Επειδή η $\Delta(x)$ μπορεί να θεωρηθεί ως η κλίση μιας χορδής της γραφικής παράστασης της $y = \pi(x)$, ολοκληρώνοντας την παραπάνω σχέση προκύπτει ότι

$$\pi(x) \approx \int_2^x \frac{1}{\ln t} dt.$$

Το ολοκλήρωμα αυτό συμβολίζεται συνήθως με $Li(x)$.

Στον επόμενο πίνακα, δίδονται για σύγκριση, οι τιμές της $\pi(x)$ και του $Li(x)$ για διάφορες τιμές του x.

x	$\pi(x)$	$Li(x)$	$Li(x) - \pi(x)$	$\pi(x)/Li(x)$
10^3	168	178	10	0.94382
10^4	1229	1246	17	0.98636
10^5	9592	9630	38	0.99605
10^6	78498	78628	230	0.99835
10^7	664579	664918	339	0.99949
10^8	5761455	5762209	754	0.99987
10^9	50847534	50849235	1701	0.99997
10^{10}	455052512	455055614	3102	0.99999

Η εικασία του Gauss είναι ισοδύναμη προς το θεώρημα των πρώτων αριθμών.

Πρόταση 5.21. *(Το θεώρημα των πρώτων αριθμών)*

$$\lim_{x \to +\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Η πρώτη απόδειξη του θεωρήματος των πρώτων αριθμών δόθηκε το 1896 από τους Jacques Hadamard και Charles Jean de la Vallée Poussin αλλά ήταν πολύ δύσκολη.

Το 1949 ο Paul Erdős και ο Atle Selberg έκαναν μια απόδειξη αυτού του θεωρήματος που χαρακτηρίστηκε ως στοιχειώδης.

Τα προβλήματα που σχετίζονται με τους πρώτους αριθμούς και την συνάρτηση $\pi(x)$ περιλαμβάνουν πολύ μεγάλους αριθμούς. Ενδεικτικό είναι και το επόμενο πρόβλημα. Μια απλή παρατήρηση του προηγούμενου πίνακα είναι ότι ότι $Li(x) - \pi(x) > 0$. Όμως το 1914 ο John Littlewood απέδειξε ότι η διαφορά $Li(x) - \pi(x)$ μπορεί να πάρει και αρνητικές τιμές.

Με την παραδοχή ότι η υπόθεση του Bernard Riemann είναι αληθής, το 1933 ο Stanley Skewes απέδειξε ότι η πρώτη εναλλαγή στο πρόσημο της διαφοράς $Li(x) - \pi(x)$ συμβαίνει πριν το x φθάσει την τιμή

$$((e^e)^e)^{79} < ((10^{10})^{10})^{34}.$$

εν τούτοις δεν έχει βρεθεί ακόμα κάποια τιμή για την οποία συμβαίνει αυτό.

Τον αριθμό αυτό, ο οποίος ονομάζεται **αριθμός Skewes**, ο Άγγλος μαθηματικός Godfrey Harold G. H. Hardy τον χαρακτήρισε ως "τον μεγαλύτερο αριθμό, που είχε ποτέ αναφερθεί, και εξυπηρετεί κάποιο σκοπό στα μαθηματικά."

Αρκετά χρόνια μετά, το 1955, ο Skewes απέδειξε ότι ακόμα και αν η υπόθεση του Riemann δεν αληθεύει, η πρώτη εναλλαγή στο πρόσημο της διαφοράς $Li(x) - \pi(x)$ συμβαίνει πριν το x φθάσει την τιμή

$$(((e^e)^e)^e)^{7.705} < ((10^{10})^{10})^{963}.$$

Σήμερα, σε προβλήματα συνδυαστικής ανάλυσης, εμφανίζονται συχνά αριθμοί πολύ μεγαλύτεροι από αυτόν.

Ένας τρόπος υπολογισμού του πλήθους των πρώτων αριθμών που είναι μικρότεροι από έναν αριθμό είναι χρησιμοποιώντας την **αρχή εγκλεισμού-αποκλεισμού**, η οποία υπολογίζει τον πληθάριθμο της ένωσης πεπερασμένων συνόλων.

Επίσης, χρήσιμη είναι και η επόμενη πρόταση.

Πρόταση 5.22. *Τα πολλαπλάσια του a που είναι μικρότερα ή ίσα από το n ισούνται με $\lfloor \frac{n}{a} \rfloor$.*

Παράδειγμα. Προκειμένου να υπολογίσουμε το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι του 100, αρκεί να βρούμε πόσοι σύνθετοι αριθμοί περιέχονται στο ίδιο διάστημα και να τους αφαιρέσουμε από το 100.

Κάθε σύνθετος αριθμός που βρίσκεται στο σύνολο [100] διαιρείται τουλάχιστον από ένα πρώτο αριθμό που είναι μικρότερος ή ίσος 10, δηλαδή τους 2, 3, 5, 7

Επομένως, οι σύνθετοι αριθμοί είναι όσοι διαιρούνται με τουλάχιστον ένα από τους 2, 3, 5, 7.

Έστω A_1 το σύνολο των αριθμών του [100] που διαιρούνται με το 2, A_2 το σύνολο των του [100] που διαιρούνται με το 3, A_3 το σύνολο των αριθμών του [100] που διαιρούνται με το 5 και A_4 το σύνολο των αριθμών του [100] που διαιρούνται με το 7.

Τότε, το πλήθος των σύνθετων αριθμοί του [100] ισούται με τον πληθάριθμο της ένωσης $|A_1 \cup A_2 \cup A_3 \cup A_4| - 4$ (εξαιρούμε τους αριθμούς 2, 3, 5 και 7 που είναι πρώτοι).

Επομένως,

$$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4| =& |A_1| + |A_2| + |A_3| + |A_4| \\ & - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4| \\ & + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\ & - |A_1 \cap A_2 \cap A_3 \cap A_4|\end{aligned}$$

Το σύνολα A_1, A_2, A_3 και A_4 περιέχουν τα πολλαπλάσια του 2, 3, 5 και 7 αντίστοιχα.
Άρα $|A_1| = \lfloor \frac{100}{2} \rfloor = 50$, $|A_2| = \lfloor \frac{100}{3} \rfloor = 33$, $|A_3| = \lfloor \frac{100}{5} \rfloor = 20$, $|A_3| = \lfloor \frac{100}{7} \rfloor = 14$.
Το σύνολο $A_1 \cap A_2$ περιέχει τα πολλαπλάσια του 2 και 3, δηλαδή του 6.
Άρα $|A_1 \cap A_2| = \lfloor \frac{100}{6} \rfloor = 16$.
Το σύνολο $A_1 \cap A_3$ περιέχει τα πολλαπλάσια του 2 και 5, δηλαδή του 10.
Άρα $|A_1 \cap A_3| = \lfloor \frac{100}{10} \rfloor = 10$.
Το σύνολο $A_1 \cap A_4$ περιέχει τα πολλαπλάσια του 2 και 7, δηλαδή του 1.
Άρα $|A_1 \cap A_4| = \lfloor \frac{100}{14} \rfloor = 7$.
Το σύνολο $A_2 \cap A_3$ περιέχει τα πολλαπλάσια του 3 και 5, δηλαδή του 15.
Άρα $|A_2 \cap A_3| = \lfloor \frac{100}{15} \rfloor = 6$.
Το σύνολο $A_2 \cap A_4$ περιέχει τα πολλαπλάσια του 3 και 7, δηλαδή του 21.

Άρα $|A_2 \cap A_4| = \lfloor \frac{100}{21} \rfloor = 4$.
Το σύνολο $A_3 \cap A_4$ περιέχει τα πολλαπλάσια του 5 και 7, δηλαδή του 35.
Άρα $|A_3 \cap A_4| = \lfloor \frac{100}{35} \rfloor = 2$.
Το σύνολο $A_1 \cap A_2 \cap A_3$ περιέχει τα πολλαπλάσια του 2, 3 και 5, δηλαδή του 30.
Άρα $|A_1 \cap A_2 \cap A_3| = \lfloor \frac{100}{30} \rfloor = 3$.
Το σύνολο $A_1 \cap A_2 \cap A_4$ περιέχει τα πολλαπλάσια του 2, 3 και 7, δηλαδή του 42.
Άρα $|A_1 \cap A_2 \cap A_4| = \lfloor \frac{100}{42} \rfloor = 2$.
Το σύνολο $A_1 \cap A_3 \cap A_4$ περιέχει τα πολλαπλάσια του 2, 5 και 7, δηλαδή του 70.
Άρα $|A_1 \cap A_3 \cap A_4| = \lfloor \frac{100}{70} \rfloor = 1$.
Το σύνολο $A_2 \cap A_3 \cap A_4$ περιέχει τα πολλαπλάσια του 3, 5 και 7, δηλαδή του 105.
Άρα $|A_2 \cap A_3 \cap A_4| = \lfloor \frac{100}{105} \rfloor = 0$.
Το σύνολο $A_1 \cap A_2 \cap A_3 \cap A_4$ περιέχει τα πολλαπλάσια του 2, 3, 5 και 7, δηλαδή του 210.
Άρα $|A_1 \cap A_2 \cap A_3 \cap A_4| = \lfloor \frac{100}{210} \rfloor = 0$.
Επομένως,

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| =& |A_1| + |A_2| + |A_3| + |A_4| \\
& - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4| \\
& + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\
& - |A_1 \cap A_2 \cap A_3 \cap A_4| \\
=& 50 + 33 + 20 + 14 \\
& - (16 + 10 + 7 + 6 + 4 + 2) \\
& + 3 + 2 + 1 + 0 \\
& - 0 \\
=& 117 - 45 + 6 - 0 \\
=& 78.
\end{aligned}$$

Άρα, το πλήθος των σύνθετων αριθμών του συνόλου [100] είναι $78 - 4 = 74$. Επομένως, το πλήθος των πρώτων αριθμών θα είναι ίσο με $99 - 74 = 25$. (Αφαιρέσαμε από το 99 και όχι από το 100 διότι ο αριθμός 1 δεν είναι ούτε πρώτος ούτε σύνθετος).

Ασκήσεις προς επίλυση

1) Να βρεθεί με την αρχή εγκλεισμού–αποκλεισμού το πλήθος των πρώτων αριθμών που είναι μικρότεροι ή ίσοι του 140.

∗2) Να βρεθεί με την αρχή εγκλεισμού–αποκλεισμού το πλήθος των πρώτων αριθμών που περιέχονται μεταξύ του 100 και του 200.

5.2 Ισοτιμίες

Έστω n ένας σταθερός φυσικός αριθμός. Οι ακέραιοι a, b καλούνται **ισότιμοι** (**modulo** n), ή **ισότιμοι κατά μέτρο** n, ή **ισοϋπόλοιποι modulo** n και γράφουμε $\mathbf{a \equiv b} \pmod{\mathbf{n}}$ αν και μόνο αν η διαφορά $a - b$ διαιρείται από τον n, δηλαδή

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b).$$

Αν $n \nmid (a - b)$, γράφουμε $a \not\equiv b \pmod{n}$ και λέμε ότι ο a είναι **ανισότιμος προς τον** b (**modulo** n).

Για παράδειγμα, έχουμε

$$15 \equiv 10 \pmod{5} \text{ αφού ισχύει ότι } 5 \mid (15 - 10),$$

$$27 \equiv 7 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (27 - 7),$$

$$7 \equiv 27 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (7 - 27),$$

$$27 \equiv 3 \pmod{3} \text{ αφού ισχύει ότι } 3 \mid (27 - 3),$$

$$7 \equiv 3 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (7 - 3),$$

$$27 \equiv -1 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (27 - (-1)),$$

$$21 \equiv 0 \pmod{3} \text{ αφού ισχύει ότι } 3 \mid (21 - 0),$$

$$25 \not\equiv 12 \pmod{7} \text{ αφού ισχύει ότι } 7 \nmid (25 - 12).$$

Παρατήρηση. Είναι πολύ συνηθισμένο το σύμβολο $a \bmod n$ να χρησιμοποιείται όχι μόνο ως σύμβολο της ισοτιμίας αλλά να συμβολίζει και το υπόλοιπο της διαίρεσης του a από το n. Στην περίπτωση αυτή χρησιμοποιείται συνήθως η γραφή $a \bmod n = b$ ή $b = a \bmod n$ αντί του συμβόλου $\equiv$. Όπως θα δούμε στην συνέχεια, αυτή η διπλή χρήση είναι δικαιολογημένη.

Πρόταση 5.23. *Δύο ακέραιοι a, b είναι ισότιμοι modulo n, δηλαδή ισχύει $a \equiv b \pmod{n}$ αν και μόνο αν διαιρούμενοι με τον n έχουν το ίδιο υπόλοιπο.*

Απόδειξη. Έστω δύο ακέραιοι a, b οι οποίοι διαιρούμενοι με το n έχουν υπόλοιπο υ, δηλαδή ισχύει ότι

$$a = \pi_1 n + \upsilon \text{ και } b = \pi_2 n + \upsilon \text{ όπου } 0 \leq \upsilon < n.$$

Τότε

$$a - b = (\pi_1 - \pi_2)n,$$

δηλαδή $n|(a - b)$, επομένως $a \equiv b \pmod{n}$.

Αντίστροφα, έστω ότι $a \equiv b \bmod n$ τότε $n|(a - b)$ δηλαδή ότι $a - b = \pi n$ όπου $\pi \in \mathbb{Z}$. Άρα

$$a = b + \pi n.$$

Αν διαιρέσουμε τον b με τον n προκύπτει ότι

$$b = \pi' n + \upsilon \text{ όπου } 0 \leq \upsilon < n$$

οπότε

$$a = \pi n + \pi' n + \upsilon = (\pi + \pi')n + \upsilon \text{ όπου } 0 \leq \upsilon \leq n.$$

Επομένως, οι ακέραιοι a, b διαιρουμένοι δια του n αφήνουν το ίδιο υπόλοιπο. □

Παρατήρηση. Οι ακέραιοι a οι οποίοι είναι ισότιμοι με b modulo n, δίνονται από τον τύπο

$$a = b + kn$$

όπου $k = 0, \pm 1, \pm 2, \ldots$.

Για παράδειγμα, οι ακέραιοι x οι οποίοι είναι ισότιμοι με 1 modulo 10, δηλαδή είναι λύσεις της εξίσωσης

$$x \equiv 1 \pmod{10}$$

είναι της μορφής

$$x = 10 \cdot k + 1, \text{ όπου } k = 0, \pm 1, \pm 2, \ldots.$$

Για $k = 0, 1, 2, 3, \ldots$ προκύπτει ότι

$$x = 1, 11, 21, 31, \ldots$$

και για $k = -1, -2, -3, \ldots$ προκύπτει ότι

$$x = -9, -19, -29, \ldots$$

Επομένως, οι ακέραοι είναι x οι οποίοι είναι ισότιμοι με 1 modulo 10 είναι οι εξής:

$$x = \ldots, -29, -19, -9, 1, 11, 21, 31, \ldots.$$

Πρόταση 5.24. *Η σχέση ισοτιμίας* mod$n$ *είναι μια σχέση ισοδυναμίας στο σύνολο* $\mathbb{Z}$.

Απόδειξη. Αρκεί να αποδειχθεί ότι ισχύει η ανακλαστική, η συμμετρική και η μεταβατική ιδιότητα.

Πράγματι, για κάθε $a \in \mathbb{Z}$ ισχύει ότι $n \mid (a - a)$ επομένως $a \equiv a \pmod{n}$, δηλαδή ισχύει η ανακλαστική ιδιότητα.

Αν $a \equiv b \pmod{n}$ τότε $n \mid (a - b)$, επομένως ισχύει ότι $n \mid -(a - b)$ δηλαδή $n \mid (b - a)$, οπότε $b \equiv a \pmod{n}$, δηλαδή ισχύει η συμμετρική ιδιότητα.

Αν $a \equiv b \pmod{n}$ και $b \equiv c \pmod{n}$, τότε $n \mid (a - b)$ και $n \mid b - c$ οπότε $n \mid (a - b) + (b - c) = a - c$. Επομένως $a \equiv c \pmod{n}$, δηλαδή ισχύει η μεταβατική ιδιότητα. □

Παρατηρήσεις.

1. Με τη βοήθεια της σχέσης ισοτιμίας modulo n, όλοι οι ακέραιοι αριθμοί μπορούν να διαμεριστούν σε κλάσεις οι οποίες ονομάζονται **κλάσεις υπολοίπων** mod n. Οι κλάσεις αυτές έχουν την ιδιότητα ότι όλα τα στοιχεία που είναι στην ίδια κλάση είναι ανά δύο ισότιμα modulo n. Για κάθε $a \in \mathbb{Z}$ ορίζουμε την κλάση

   $$\{x \in \mathbb{Z} : x \equiv a \pmod{n}\},$$

   και την συμβολίζουμε με $\bar{a}$ ή $[a]$.

2. Κάθε ακέραιος αριθμός είναι ισουπόλοιπος mod$n$ με έναν ακριβώς από τους αριθμούς: 0, 1, 2, …, $n - 1$. Επομένως το σύνολο των ακεραίων χωρίζεται σε n κλάσεις mod$n$ τέτοιες ώστε:

$$\begin{aligned}
[0] &= \{\ldots, -2 \cdot n, -n, \ 0, \ n, \ 2 \cdot n, \ \ldots\}, \\
[1] &= \{\ldots, -2 \cdot n + 1, -n + 1, \ 1, \ n + 1, \ 2 \cdot n + 1, \ \ldots\}, \\
[2] &= \{\ldots, -2 \cdot n + 2, -n + 2, \ 2, \ n + 2, \ 2 \cdot n + 2, \ \ldots\}, \\
&\vdots \\
[n - 1] &= \{\ldots, -n - 1, \ -1, \ n - 1, \ 2 \cdot n - 1, \ 3 \cdot n - 1, \ \ldots\}.
\end{aligned}$$

Άρα

$$\begin{aligned}[a] &= \{b \in \mathbb{Z} : a \equiv b \pmod{n}\} \\ &= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}.\end{aligned}$$

Με $\mathbb{Z}_n$ συμβολίζουμε το **σύνολο κλάσεων** modulo n

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\} = \{[0], [1], [2], \ldots, [n-1]\}.$$

Εφαρμογές των ισοτιμιών

Η έννοια της ισοτιμίας έχει πολλές εφαρμογές τόσο σε μαθηματικές όσο και σε καθημερινές χρήσεις. Πριν μελετήσουμε τις ιδιότητες των ισοτιμιών ας δούμε ορισμένες εφαρμογές τους οι οποίες βασίζονται στον ορισμό τους.

1. **Ανίχνευση σφαλμάτων στην μνήμη ενός υπολογιστή.** Μια από τις πιο απλές χρήσεις της ισοτιμίας είναι για την ανίχνευση σφαλμάτων στην μνήμη ενός υπολογιστή μέσω της χρήσης ενός bit μνήμης ως bit ελέγχου.

   Η βασική ιδέα είναι ότι σε κάθε καταχωρητή μνήμης, (π.χ. 32-μπιτο ή 64-μπιτο καταχωρητή) ο αριθμός των bits με τιμή 1 πρέπει είναι πάντα άρτιος (ή να είναι πάντα περιττός).

   Για να γίνει αυτό, αρκεί να θυσιάσουμε ένα bit μνήμης το οποίο να χρησιμοποιείται για την αποθήκευση του bit ελέγχου. Επειδή τα bit έχουν δύο τιμές αυτό ονομάζεται bit αρτιότητας ή parity bit.

   Για παράδειγμα, αν σε ένα 8-μπιτο καταχωρητή θέλουμε να αποθηκεύσουμε την τιμή 0101011 πρέπει στην όγδοη θέση να περιέχεται η τιμή 0, ενώ όταν θέλουμε να αποθηκεύσουμε την τιμή 0101111 πρέπει στην όγδοη θέση να περιέχεται η τιμή 1. Επομένως, αν κάποιος καταχωρητής περιέχει την τιμή 011100000 συμπεραίνουμε ότι υπάρχει κάποιο σφάλμα μνήμης. Δυστυχώς, δεν μπορούμε να ανακαλύψουμε πού βρίσκεται το σφάλμα ώστε να το διορθώσουμε. Επίσης, αν υπάρχουν δύο ή περισσότερα σφάλματα, πιθανόν να μην είναι ανιχνεύσιμα. Για παράδειγμα αν αντί για την τιμή 0101011 αποθηκευθούν οι τιμές 01100110 ή 00000000 δεν ανιχνεύονται τα σφάλματά τους.

   Το άθροισμα των bit με τιμή 1 που αποθηκεύονται στους καταχωρητές είναι αριθμοί που έχουν την ίδια ισοτιμία modulo 2, και συγκεκριμένα είναι ισότιμοι με 0 mod 2.

2. **Έλεγχος εγκυρότητας ISBN.** Μια άλλη καθημερινή χρήση της ιδέας της ισοτιμίας είναι στην κατασκευή των αριθμών ISBN (International System Book Number) οι οποίοι είναι μοναδικοί για κάθε βιβλίο. Οι αριθμοί ISBN πριν το 2007 ήταν 10ψήφιοι αριθμοί (ISBN–10), ενώ μετά την 1η Ιανουαρίου 2007, έχουν γίνει 13ψήφιοι (ISBN–13). Τα ψηφία των αριθμών ISBN–10 χωρίζονται σε 4 ομάδες μεταβλητού μήκους, οι οποίες διαχωρίζονται από παύλες –. Για παράδειγμα, ένας αριθμός ISBN-10 είναι ο επόμενος:

   $$0 – 486 – 27709 – 7,$$

   ενώ τα ψηφία των αριθμών ISBN-13 χωρίζονται σε 5 ομάδες[5], για παράδειγμα

   $$978 – 960 – 7996 – 33 – 6.$$

[5] Η πρώτη ομάδα προστέθηκε επειδή θα εξαντληθούν οι αριθμοί ISBN–10· μέχρι σήμερα η πρώτη ομάδα του ISBN–13 περιέχει τα ψηφία 978.

Στους αριθμούς ISBN–10 τα ψηφία της πρώτης ομάδας κωδικοποιούν την χώρα ή την περιοχή ή τις περιοχές που ομιλείται μια συγκεκριμένη γλώσσα στην οποία ανήκει ο εκδότης του βιβλίου. Για παράδειγμα, το 0 κωδικοποιεί τις χώρες με γλώσσα τα Αγγλικά, ενώ το 960 κωδικοποιεί τις Ελληνικές εκδόσεις.

Τα ψηφία της δεύτερης ομάδας κωδικοποιούν τον εκδότη αυτής της περιοχής.

Τα ψηφία της τρίτης ομάδας κωδικοποιούν ένα συγκεκριμένο βιβλίο.

Τέλος, στην τέταρτη ομάδα περιέχεται μόνο ένα ψηφίο, το οποίο είναι ψηφίο ελέγχου, και υπολογίζεται από τα υπόλοιπα ψηφία. Στο ISBN–10 το τελευταίο ψηφίο υπολογίζεται ώστε το άθροισμα των ψηφίων του αριθμού ISBN–10 πολλαπλασιασμένα με κατάλληλους αριθμούς να είναι ισότιμο 0 mod 11. Συγκεκριμένα, για τον αριθμό ISBN–10

$$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$$

ισχύει ότι

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + 1 \cdot x_{10} \equiv 0 \bmod 11.$$

Πράγματι, για τον αριθμό ISBN–10 0-486-27709-7 ισχύει ότι

$$10 \cdot 0 + 4 \cdot 9 + 8 \cdot 8 + 7 \cdot 6 + 6 \cdot 2 + 5 \cdot 7 + 4 \cdot 7 + 3 \cdot 0 + 2 \cdot 9 + 1 \cdot 7 = 242 \equiv 0 \pmod{11},$$

αφού $242 = 22 \cdot 11$.

Χρησιμοποιώντας τις ιδιότητες των υπολοίπων μπορούμε να δείξουμε ότι το δέκατο ψηφίο x_{10} μπορεί να υπολογισθεί από τον τύπο

$$x_{10} = (1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8 \cdot x_8 + 9 \cdot x_9) \bmod 11.$$

Επειδή τα δυνατά υπόλοιπα της διαίρεσης ενός αριθμού με το 11 είναι 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 στην περίπτωση που $x_{10} = 10$ χρησιμοποιείται αντ' αυτού το γράμμα X.

Αποδεικνύεται ότι ο κώδικας αυτός αναγνωρίζει όχι μόνο σφάλματα σε κάποιο ψηφίο αλλά και σφάλματα αντιμετάθεσης, όπως για παράδειγμα να γράψουμε 14 αντί για 41.

Στον ISBN–13 το τελευταίο ψηφίο δίνεται με διαφορετικό τρόπο. Συγκεκριμένα για τον αριθμό ISBN–13

$$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12}x_{13}$$

ισχύει ότι

$$x_{13} = (10 - (x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12}) \bmod 10) \bmod 10.$$

Ο κώδικας αυτός, σε αντίθεση με τον ISBN–10 δεν εντοπίζει πάντα σφάλματα αντιμετάθεσης.

3. **Έλεγχος εγκυρότητας ΑΦΜ.** Η ίδια ιδέα με τον αριθμό ISBN βρίσκεται στην κατασκευή των αριθμών φορολογικού μητρώου (ΑΦΜ). Οι ΑΦΜ είναι 9 ψήφιοι αριθμοί στους οποίους το τελευταίο ψηφίο είναι ψηφίο ελέγχου.

   Συγκεκριμένα, σε κάθε ΑΦΜ $x_1x_2x_3x_4x_5x_6x_7x_8x_9$ ισχύει ότι

$$x_9 = ((x_8 \cdot 2^1 + x_7 \cdot 2^2 + x_6 \cdot 2^3 + x_5 \cdot 2^4 + x_4 \cdot 2^5 + x_3 \cdot 2^6 + x_2 \cdot 2^7 + x_1 \cdot 2^8) \bmod 11) \bmod 10.$$

Για παράδειγμα, ο αριθμός 123456783 ανήκει στους παραπάνω αριθμούς αφού

$$8 \cdot 2^1 + 7 \cdot 2^2 + 6 \cdot 2^3 + 5 \cdot 2^4 + 4 \cdot 2^5 + 3 \cdot 2^6 + 4 \cdot 2^7 + 1 \cdot 2^8 = 1004.$$

Ισχύει ότι $1004 = 91 \cdot 11 + 3$ άρα $1004 \bmod 11 = 3$ και $3 \bmod 10 = 3 = x_9$.

Φυσικά, ο παραπάνω έλεγχος είναι έλεγχος ορθότητας και δεν ελέγχει αν αυτός ο αριθμός είναι σε χρήση ή όχι.

Οι βασικές ιδιότητες της ισοτιμίας modulo n δίνονται στην επόμενη πρόταση.

Πρόταση 5.25. *Αν n είναι ένας σταθερός φυσικός αριθμός και a, b, c, d ακέραιοι, ισχύουν τα ακόλουθα:*

1. *Αν $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$, τότε*
$$a + c \equiv b + d \pmod{n} \text{ και } a \cdot c \equiv b \cdot d \pmod{n}.$$
2. *Αν $a \equiv b \pmod{n}$, τότε*
$$a + c \equiv b + c \pmod{n} \text{ και } a \cdot c \equiv b \cdot c \pmod{n}.$$
3. *Αν $a \equiv b \pmod{n}$, τότε*
$$a^k \equiv b^k \pmod{n} \text{ για κάθε } k \in \mathbb{N}.$$
4. *Αν $p(x) = c_0 + c_1 x + \ldots + c_k x^k$ είναι ένα πολυωνύμο με ακέραιους συντελεστές και $a \equiv b \pmod{n}$, τότε*
$$p(a) \equiv p(b) \pmod{n}.$$

Εφαρμογές

Με τη βοήθεια των προηγούμενων ιδιοτήτων των ισοτιμιών μπορούμε να μειώσουμε σημαντικά το κόστος υπολογισμού που απαιτείται κατά τις πράξεις αριθμών modulo n. Στη συνέχεια δίδονται ορισμένα χαρακτηριστικά παραδείγματα εφαρμογής των ιδιοτήτων των ισοτιμιών, κυρίως για τον υπολογισμό δυνάμεων ακεραίων modulo n.

Εφαρμογή 5.2.1. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$2^{100} \equiv x \pmod{7}.$$

Λύση. Παρατηρούμε ότι $2^3 \equiv 8 \equiv 1 \pmod{7}$ επομένως

$$2^{100} \equiv 2^{3 \cdot 33 + 1} \equiv (2^3)^{33} \cdot 2 \equiv 1^{33} \cdot 2 \equiv 2 \pmod{7}.$$

Άρα, $x = 2$. Δηλαδή, το υπόλοιπο της διαίρεσης του 2^{100} με το 7 ισούται με 2. □

Εφαρμογή 5.2.2. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$2^{100} \equiv x \pmod{9}.$$

Λύση. Παρατηρούμε ότι $2^3 \equiv 8 \equiv -1 \pmod 9$ επομένως

$$2^{100} \equiv 2^{3\cdot 33+1} \equiv (2^3)^{33} \cdot 2 \equiv (-1)^{33} \cdot 2 \equiv -2 \equiv 7 \pmod 9.$$

Άρα, $x = 7$. Δηλαδή, το υπόλοιπο της διαίρεσης του 2^{100} με το 9 ισούται με 7. □

Εφαρμογή 5.2.3. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$3^{100} \equiv x \pmod{11}.$$

Λύση. Ισχύει ότι

$$3^{100} \equiv (3^2)^{50} \equiv 9^{50} \equiv (9^2)^{25} \equiv 81^{25} \pmod{11}.$$

Επειδή $81 \equiv 4 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 4^{25} \equiv (4^2)^{12} \cdot 4 \equiv 16^{12} \cdot 4 \pmod{11}.$$

Επειδή $16 \equiv 5 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 5^{12} \cdot 4 \equiv (5^2)^6 \cdot 4 \equiv 25^6 \cdot 4.$$

Επειδή $25 \equiv 3 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 3^6 \cdot 4 \equiv (3^2)^3 \cdot 4 \equiv 9^3 \cdot 4 \pmod{11} \equiv 9^2 \cdot 9 \cdot 4 \equiv 81 \cdot 36 \pmod{11}.$$

Επειδή $81 \equiv 4 \pmod{11}$ και $36 \equiv 3 \pmod{11}$, προκύπτει ότι

$$3^{100} \equiv 4 \cdot 3 \equiv 12 \equiv 1 \pmod{11}.$$

Άρα, $x = 1$. Δηλαδή, το υπόλοιπο της διαίρεσης του 3^{100} με το 11 ισούται με 1. □

Εφαρμογή 5.2.4. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$7^{1000} \equiv x \pmod{13}.$$

Λύση. Ισχύει ότι

$$7^{1000} \equiv (7^2)^{500} \equiv 49^{500} \pmod{13}.$$

Επειδή $49 \equiv 10 \pmod{13}$, προκύπτει ότι

$$7^{1000} \equiv 10^{500} \equiv (10^2)^{250} \equiv 100^{250} \pmod{13}.$$

Επειδή $100 \equiv 9 \pmod{13}$, προκύπτει ότι

$$7^{1000} \equiv 9^{250} \equiv (9^2)^{125} \equiv 81^{125} \pmod{13}.$$

Επειδή $81 \equiv 3 \pmod{13}$, προκύπτει ότι

$$7^{1000} \equiv 3^{125} \pmod{13}.$$

Παρατηρούμε ότι $3^3 \equiv 27 \equiv 1 \pmod{13}$ και επομένως

$$7^{1000} \equiv 3^{125} \equiv 3^{3\cdot 41+2} \equiv (3^3)^{41} \cdot 9 \equiv 1^{41} \cdot 9 \equiv 9 \pmod{13}.$$

Άρα, $x = 9$. Δηλαδή, το υπόλοιπο της διαίρεσης του 7^{1000} με το 13 ισούται με 9. □

Εφαρμογή 5.2.5. *Να δειχθεί ότι αν ένας εξαψήφιος αριθμός τελειώνει σε 74 τότε αποκλείεται να είναι τέλειο τετράγωνο.*

Λύση. Κάθε εξαψήφιος αριθμός n που τελειώνει σε 74 γράφεται στη μορφή

$$X_1X_2X_3X_474$$

Ισχύει ότι

$$X_1X_2X_3X_474 = 100 \cdot X_1X_2X_3X_4 + 74.$$

Παρατηρούμε ότι αν n είναι ένας αριθμός, τότε το υπόλοιπο της διαίρεσης του n^2 από το 4 ισούται με 0 ή 1.

Πράγματι, για κάθε μια από τις 4 περιπτώσεις έχουμε ότι:
Αν $n \equiv 0 \pmod 4$, τότε $n^2 \equiv 0 \cdot 0 \equiv 0 \pmod 4$.
Αν $n \equiv 1 \pmod 4$, τότε $n^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$.
Αν $n \equiv 2 \pmod 4$, τότε $n^2 \equiv 2 \cdot 2 \equiv 4 \equiv 0 \pmod 4$.
Αν $n \equiv 3 \pmod 4$, τότε $n^2 \equiv 3 \cdot 3 \equiv 9 \equiv 1 \pmod 4$.
Όμως, επειδή $100 \equiv 0 \pmod 4$ και $74 \equiv 2 \pmod 4$, προκύπτει ότι

$$X_1X_2X_3X_474 \equiv (100 \cdot X_1X_2X_3X_4 + 74) \equiv (0 \cdot X_1X_2X_3X_4 + 2) \equiv 2 \pmod 4.$$

Επομένως ο αριθμός $X_1X_2X_3X_474$ δεν είναι τέλειο τετράγωνο. □

Εφαρμογή 5.2.6. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$41^{100} + 41^{50} + 41^{25} + 1 \equiv x \pmod 7.$$

Λύση. Παρατηρούμε ότι $41 \equiv -1 \pmod 7$, επομένως

$$41^{100} + 41^{50} + 41^{25} + 1 \equiv (-1)^{100} + (-1)^{50} + (-1)^{25} + 1 \equiv 1 + 1 - 1 + 1 \equiv 2 \pmod 7.$$ □

Στις επόμενες προτάσεις δίνονται ορισμένες επιπλέον ιδιότητες της ισοτιμίας.

Πρόταση 5.26. *Έστω ο ακέραιος $c \neq 0$. Τότε $a \equiv b \pmod n$ αν μόνο αν $ca \equiv cb \pmod{nc}$.*

Απόδειξη. Έστω ότι $a \equiv b \pmod n$. Τότε $n \mid (a - b)$, δηλαδή $nc \mid ca - cb$. Άρα $ca \equiv cb \pmod{nc}$.

Αντίστροφα, έστω ότι $ca \equiv cb \pmod{nc}$. Επομένως, έχουμε $cn \mid ca - cb$ και αφού $c \neq 0$, τότε $n \mid a - b$. Άρα $a \equiv b \pmod n$. □

Πρόταση 5.27. *Αν $d = \gcd(c, n)$, τότε $ca \equiv cb \pmod n$ αν και μόνο αν $a \equiv b \pmod{\frac{n}{d}}$.*

Για παράδειγμα, έστω ότι γνωρίζουμε την ισοδυναμία

$$50 \equiv 20 \pmod{15}.$$

Ισχύει ότι $50 = 5 \cdot 10$ και $20 = 2 \cdot 10$. Για $c = 10$, $n = 15$ και $d = \gcd(c, n) = \gcd(10, 15) = 5$, προκύπτει ότι

$$5 \equiv 2 \pmod 3.$$

Πρόταση 5.28 (Νόμος της διαγραφής). *Αν* $ca \equiv cb \pmod{n}$ *και* $\gcd(c, n) = 1$, *τότε* $a \equiv b \pmod{n}$.

Για παράδειγμα, έστω ότι γνωρίζουμε την ισοδυναμία

$$35 \equiv 20 \pmod{3}.$$

Ισχύει ότι $35 = 5 \cdot 7$, $20 = 5 \cdot 4$ και $\gcd(5, 3) = 1$, οπότε έχουμε ότι

$$7 \equiv 4 \pmod{3}.$$

Πόρισμα 5.29. *Έστω* p *πρώτος αριθμός. Αν*

$$ca \equiv cb \pmod{p}$$

με $p \nmid c$, *τότε* $a \equiv b \pmod{p}$.

Απόδειξη. Αφού $p \nmid c$ όπου p πρώτος αριθμός, προκύπτει ότι $\gcd(p, c) = 1$. Επομένως, από την προηγούμενη πρόταση προκύπτει ότι $a \equiv b \pmod{p}$. □

Για παράδειγμα, έστω ότι γνωρίζουμε την ισοδυναμία

$$35 \equiv 20 \pmod{3}.$$

Αφού $35 = 5 \cdot 7$, $20 = 5 \cdot 4$ και $\gcd(5, 3) = 1$, προκύπτει ότι

$$7 \equiv 4 \pmod{3}.$$

5.2.1 Η συνάρτηση ϕ του Euler

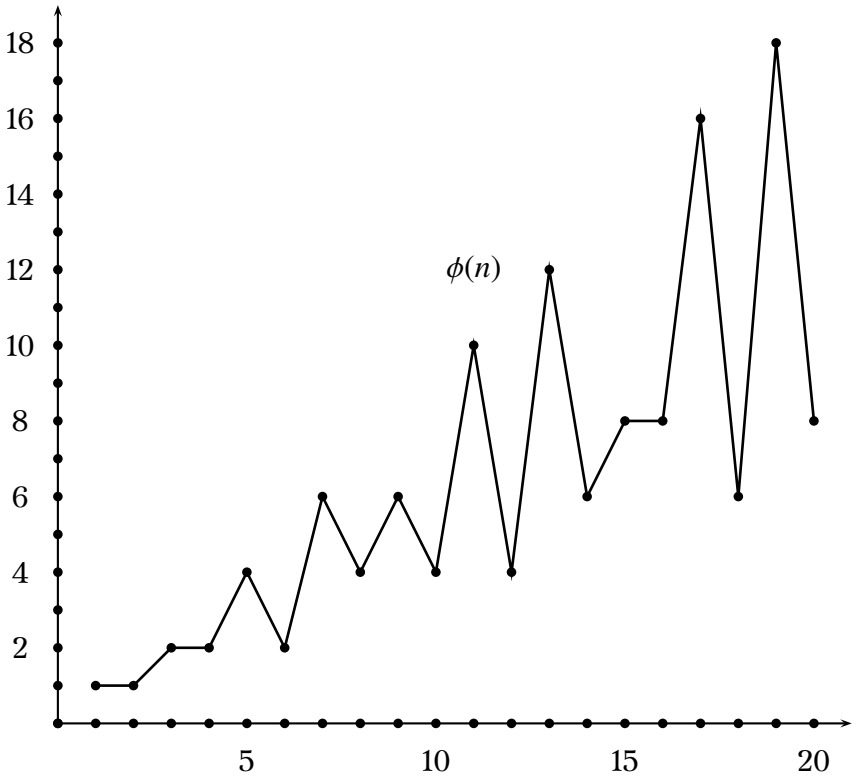
Στην ενότητα αυτή θα μελετήσουμε το ερώτημα πόσοι είναι οι αριθμοί που είναι μικρότεροι από κάποιο αριθμό και είναι σχετικά πρώτοι με αυτόν;

Έστω $\phi(n)$ το πλήθος των αριθμών m που είναι μικρότεροι ή ίσοι από το n και ισχύει ότι $\gcd(n, m) = 1$, δηλαδή τα n και m είναι σχετικά πρώτοι μεταξύ τους.

Για παράδειγμα, $\phi(12) = 4$, διότι από τους αριθμούς $1, 2, \ldots, 12$ το 12 είναι σχετικά πρώτο με τους αριθμούς 1, 5, 7, 11 (δεν είναι με το 8 διότι αν και το 8 δεν διαιρεί το 12 εν τούτοις ισχύει ότι $\gcd(12, 8) = 4$).

Οι τιμές της $\phi(n)$ για κάθε n μικρότερο ή ίσο του 20 δίνονται στον επόμενο πίνακα.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8



Υπάρχει τύπος για την συνάρτηση $\phi(n)$; Η απάντηση είναι καταφατική.

Πριν φτάσουμε στην τελική απάντηση ας εξετάσουμε βήμα-βήμα ορισμένες ειδικές περιπτώσεις για τον αριθμό n.

Αν $n = p$ όπου p είναι πρώτος, τότε όλοι οι αριθμοί m οι οποίοι είναι μικρότεροι από το p είναι σχετικά πρώτοι με το p. Άρα στην περίπτωση $n = p$, όπου p είναι πρώτος, προκύπτει ότι

$$\phi(n) = \phi(p) = p - 1.$$

Αν $n = p^2$ όπου p είναι πρώτος, τότε όλοι οι αριθμοί m που είναι μικρότεροι από το p^2 είναι πρώτοι σχετικά με το p^2, εκτός από τους αριθμούς p, $2p$, $3p$, $4p$, …, $(p-1)p$. Επομένως

$$\phi(n) = \phi(p^2) = p^2 - 1 - (p - 1) = p^2 - p.$$

Αντίστοιχα, αν $n = p^k$ όπου p είναι πρώτος και $k \in N^*$, τότε όλοι οι αριθμοί m που είναι μικρότεροι από το p^k είναι πρώτοι σχετικά με το p^k εκτός από τους αριθμούς p, $2p$, $3p$, …, $(p^{k-1} - 1)p$. Επομένως

$$\phi(n) = \phi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}.$$

Αν $n = pq$ όπου p, q είναι πρώτοι αριθμοί με $p \neq q$, τότε όλοι οι αριθμοί m που είναι μικρότεροι από το pq είναι πρώτοι σχετικά με το pq εκτός από τους αριθμούς p, $2p$, $3p$, $4p$, …, $(q-1)p$ και τους αριθμούς q, $2q$, $3q$, $4q$, …, $(p-1)q$, οι οποίοι είναι όλοι διάφοροι μεταξύ τους (γιατί;). Επομένως

$$\phi(n) = \phi(pq) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1).$$

Από την προηγούμενη ισότητα παρατηρούμε ότι, αν $p \neq q$, ισχύει ότι

$$\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q).$$

(Αυτή η ιδιότητα δεν ισχύει όταν $p = q$ αφού $\phi(p^2) = p^2 - p$ ενώ $\phi(p)\phi(p) = (p-1)^2$.)

Ισχύει η επόμενη πρόταση.

Πρόταση 5.30. *Έστω m, n φυσικοί αριθμοί με $\gcd(m, n) = 1$. Τότε*

$$\phi(mn) = \phi(m)\phi(n).$$

Απόδειξη. Άσκηση. □

Από την προηγούμενη πρόταση άμεσα προκύπτει μια έκφραση για τον υπολογισμό της τιμής $\phi(n)$ όταν γνωρίζουμε την κανονική παραγοντοποίηση του n.

Πρόταση 5.31. *Έστω n ένας φυσικός αριθμός με κανονική παραγοντοποίηση*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

όπου $p_1, p_2, \ldots, p_k$ είναι πρώτοι αριθμοί και $a_1, a_2, \ldots, a_k$ είναι φυσικοί αριθμοί. Τότε

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}).$$

Παράδειγμα 5.2.1. *Να βρεθούν οι παρακάτω τιμές του $\phi(n)$.*

Για $n = 120$ είναι $120 = 2^3 \cdot 3 \cdot 5$, οπότε

$$\phi(120) = \phi(2^3)\phi(3)\phi(5) = (2^3 - 2^2)(3-1)(5-1) = 4 \cdot 2 \cdot 4 = 32.$$

Επομένως, υπάρχουν 32 αριθμοί μικρότεροι από το 120 που είναι σχετικά πρώτοι με αυτό.

Για $n = 6!$ είναι $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 = 2^4 \cdot 3^2 \cdot 5$, οπότε

$$\phi(6!) = \phi(2^4)\phi(3^2)\phi(5) = (2^4 - 2^3)(3^2 - 3^1)(5-1) = 8 \cdot 6 \cdot 4 = 192.$$

Επομένως, υπάρχουν 192 αριθμοί μικρότεροι από το $6! = 720$ που είναι σχετικά πρώτοι με αυτό.

Εφαρμογή 5.2.7. *Να βρεθούν οι πρώτοι αριθμοί p, q για τους οποίους ισχύει ότι $pq = 7093$ και $\phi(pq) = 6880$.*

Λύση. Προφανώς, $p \neq q$ αφού το 7093 δεν είναι τέλειο τετράγωνο. Επομένως,

$$\phi(pq) = (p-1)(q-1) = pq - (p+q) + 1,$$

οπότε

$$6880 = 7093 - (p+q) + 1 \Leftrightarrow p + q = 214.$$

Άρα, γνωρίζουμε το γινόμενο και το άθροισμα των pq, επομένως τα p, q είναι οι ρίζες της δευτεροβάθμιας εξίσωσης

$$x^2 - 214x + 7093 = 0.$$

Έχουμε ότι

$$p, q = \frac{214 \pm \sqrt{214^2 - 4 \cdot 7093}}{2} = \frac{214 \pm \sqrt{45796 - 28372}}{2} = \frac{214 \pm \sqrt{17424}}{2} = \frac{214 \pm 132}{2} = 107 \pm 66.$$

Άρα, οι ζητούμενοι πρώτοι αριθμοί είναι οι 173 και 41.

Πράγματι, $173 \cdot 41 = 7093$ και $\phi(173 \cdot 41) = (173-1)(41-1) = 6880$. □

5.2.2 Θεώρημα Euler-Fermat

Πρόταση 5.32 (Θεώρημα του Euler). *Αν a, m είναι φυσικοί αριθμοί και $\gcd(a, m) = 1$, τότε ισχύει ότι*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Με τη βοήθεια του θεωρήματος του Euler προκύπτει η επόμενη πρόταση.

Πρόταση 5.33 (Μικρό θεώρημα του Fermat). *Αν p είναι πρώτος αριθμός και n φυσικός αριθμός, τότε*

$$n^p \equiv n \pmod{p}.$$

Απόδειξη. Διακρίνουμε δύο περιπτώσεις. Αν $p \mid n$, τότε $n \equiv 0 \pmod{p}$, οπότε

$$n^p \equiv 0^p \equiv 0 \equiv n \pmod{p}.$$

Αν $p \nmid n$, τότε $\gcd(n, p) = 1$, οπότε

$$n^{\phi(p)} \equiv 1 \pmod{p}.$$

Αλλά $\phi(p) = p - 1$, διότι p είναι πρώτος, οπότε

$$n^{p-1} \equiv 1 \pmod{p}.$$

Πολλαπλασιάζοντας και τα δύο μέλη με n προκύπτει ότι

$$n^p \equiv n \pmod{p}.$$ □

Εφαρμογές

Εφαρμογή 5.2.8. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$x \equiv 3^{1000} \pmod{41}.$$

Λύση. Επειδή $\gcd(41, 3) = 1$, έπεται ότι

$$3^{\phi(41)} \equiv 1 \pmod{41}.$$

Ο 41 είναι πρώτος, οπότε $\phi(41) = 41 - 1 = 40$.
Επομένως, $3^{40} \equiv 1 \pmod{41}$, οπότε

$$x \equiv 3^{1000} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1 \pmod{41}.$$ □

Εφαρμογή 5.2.9. *Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$x \equiv 17^{812} \pmod{110}.$$

Λύση. Επειδή $\gcd(110, 17) = 1$, έπεται ότι

$$17^{\phi(110)} \equiv 1 \pmod{110}.$$

Επίσης, $\phi(110) = \phi(2 \cdot 5 \cdot 11) = 1 \cdot 4 \cdot 10 = 40$.
Επομένως, $17^{40} \equiv 1 \pmod{110}$, οπότε

$$\begin{aligned} x &\equiv 17^{812} \equiv 17^{20 \cdot 40 + 12} \equiv (17^{40})^{20} \cdot 17^{12} \equiv 1^{20} \cdot 17^{12} \\ &\equiv 17^{12} \equiv (17^2)^6 \equiv 289^6 \equiv 69^6 \equiv (69^2)^3 \equiv 4761^3 \\ &\equiv 31^3 \equiv 31 \cdot 31^2 \equiv 31 \cdot 961 \equiv 31 \cdot 81 \equiv 2511 \equiv 91 \pmod{110}. \end{aligned}$$ □

Εφαρμογή 5.2.10. *Να αποδειχθεί ότι το* 13 *διαιρεί το* $2^{70} + 3^{70}$.

Λύση. Θα βρούμε τις λύσεις των εξισώσεων

$$x \equiv 2^{70} \pmod{13}$$

$$y \equiv 3^{70} \pmod{13}$$

Επειδή $\gcd(2, 13) = \gcd(3, 13) = 1$, έπεται ότι

$$2^{\phi(13)} \equiv 3^{\phi(13)} \equiv 1 \pmod{13}.$$

Ισχύει ότι $\phi(13) = 13 - 1 = 12$, οπότε

$$2^{12} \equiv 3^{12} \equiv 1 \pmod{13}.$$

Επομένως, έχουμε ότι

$$x \equiv 2^{70} \equiv (2^{12})^5 \cdot 2^{10} \equiv 1^5 \cdot (2^2)^5 \equiv 4^5 \equiv 16 \cdot 16 \cdot 4 \equiv 3 \cdot 3 \cdot 4 \equiv 36 \equiv 10 \pmod{13}$$

και

$$y \equiv 3^{70} \equiv (3^{12})^5 \cdot 3^{10} \equiv 1^5 \cdot (3^2)^5 \equiv 9^5 \equiv 81 \cdot 81 \cdot 9 \equiv 3 \cdot 3 \cdot 9 \equiv 81 \equiv 3 \pmod{13}$$

Άρα,

$$2^{70} + 3^{70} \equiv 10 + 3 \equiv 0 \pmod{13},$$

δηλαδή $13 \mid 2^{70} + 3^{70}$. □

Εφαρμογή 5.2.11. *Να αποδειχθεί ότι* $7 \mid a^{55} - a$*, για κάθε ακέραιο* a*.*

Λύση. Αρκεί να αποδειχθεί ότι

$$a^{55} \equiv a \pmod 7.$$

Πράγματι

$$7 \mid a^{55} - a \text{ ανν } a^{55} - a \equiv 0 \pmod 7.$$

Επειδή το 7 είναι πρώτος αριθμός, από το μικρό θεώρημα του Fermat, προκύπτει ότι

$$a^7 \equiv a \pmod 7.$$

Επομένως

$$a^{55} \equiv (a^7)^7 \cdot a^6 \equiv a^7 \cdot a^6 \equiv a \cdot a^6 \equiv a^7 \equiv a \pmod 7.$$

Για παράδειγμα, ισχύει ότι $7 \mid 2^{55} - 2$. □

Εφαρμογή 5.2.12. *Να αποδειχθεί ότι* $30 \mid a^{25} - a$*, για κάθε ακέραιο* a*.*

Λύση. Παρατηρούμε ότι $30 = 2 \cdot 3 \cdot 5$, οπότε αρκεί να αποδειχθεί ότι

$$2 \mid a^{25} - a, \qquad 3 \mid a^{25} - a, \qquad 5 \mid a^{25} - a$$

ή ισοδύναμα ότι

$$a^{25} \equiv a \pmod 2,$$

$$a^{25} \equiv a \pmod 3,$$

$$a^{25} \equiv a \pmod 5.$$

Πράγματι, επειδή $2, 3, 5$ είναι πρώτοι, από το μικρό θεώρημα του Fermat, προκύπτει ότι

$$a^2 \equiv a \pmod 2,$$

$$a^3 \equiv a \pmod 3,$$

$$a^5 \equiv a \pmod 5,$$

οπότε

$$a^{25} \equiv (a^2)^{12} \cdot a \equiv a^{12} \cdot a \equiv (a^2)^6 \cdot a \equiv a^6 \cdot a \equiv (a^2)^3 \cdot a \equiv a^3 \cdot a \equiv a^4 \equiv (a^2)^2 \equiv a^2 \equiv a \pmod 2$$

$$a^{25} \equiv (a^3)^8 \cdot a \equiv a^8 \cdot a \equiv a^9 \equiv (a^3)^3 \equiv a^3 \equiv a \pmod 3$$

$$a^{25} \equiv (a^5)^5 \equiv a^5 \equiv a \pmod 5.$$

Επομένως, $30 \mid a^{25} - a$ για κάθε ακέραιο a. □

5.2.3 Ασκήσεις προς επίλυση

1) Να βρεθεί ποιο είναι το ψηφίο ελέγχου για τους επόμενους αριθμούς ISBN–10: 960 – 351 – 034–?, 960 – 7510 – 22–?, 960 – 524 – 225–?. και να ελεγχθεί αν οι επόμενοι αριθμοί ISBN–10 είναι έγκυροι: 0 – 486 – 65537 – 7, 960 – 7778 – 74 – 8.

2) Να γραφεί πρόγραμμα που υπολογίζει το τελευταίο ψηφίο των αριθμών ISBN–10 και ISBN–13.

3) Να γραφεί πρόγραμμα που να ελέγχει την εγκυρότητα ενός αριθμού ΑΦΜ.

4) Για ποιους φυσικούς αριθμούς m ισχύουν οι ισοδυναμίες

   i) $35 \equiv 2 \pmod{m}$.

   ii) $1000 \equiv 1 \pmod{m}$.

   iii) $347 \equiv 0 \pmod{m}$.

5) Να βρεθεί η τιμή της συνάρτησης ϕ για τους φυσικούς αριθμούς

   i) 31, 125, 55, 124, 650, 7!, 10!, $\binom{10}{6}$.

   ii) 2^m, 30^m, 20^{10m}, $2^m 3^n$, $10^m 20^n$, όπου $m, n \in \mathbb{N}^*$.

6) Να βρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί τις εξισώσεις

   i) $x \equiv 2^{303} \pmod{7}$.

   ii) $x \equiv 15^{101} \pmod{8}$.

   iii) $x \equiv 15^{2011} \pmod{3}$.

   iv) $x \equiv 20^{640} \pmod{17}$.

   v) $x \equiv 20^{322} \pmod{17}$.

   vi) $x \equiv 11^{481} \pmod{45}$.

   vii) $x \equiv 13^{802} \pmod{55}$.

7) Να δειχθεί ότι

   i) το 13 διαιρεί τον $2^{70} + 3^{70}$.

   ii) το 44 διαιρεί τον $19^{19} + 69^{69}$.

   iii) το 31 διαιρεί τον $30^{99} + 61^{100}$.

   iv) το 66 διαιρεί τον $43^{101} + 23^{101}$.

   v) το 100 διαιρεί τον $11^{10} - 1$.

   vi) το 143 διαρεί τον $7^{120} - 1$.

8) Να δειχθεί ότι ο $11 \cdot 31 \cdot 61$ διαιρεί τον $20^{15} - 1$.

9) Να δειχθεί ότι αν a, b είναι περιττοί αριθμοί, τότε ο $a^2 - b^2$ διαιρείται από το 8.

10) Έστω p ένας πρώτος αριθμός. Να αποδειχθούν οι επόμενες προτάσεις

   i) Για κάθε φυσικό αριθμό n με $0 < n < p$ ισχύει ότι $p \mid \binom{p}{n}$.

   ii) Για κάθε φυσικό αριθμό n ισχύει ότι $p \mid n^p - n$.

   iii) Για κάθε ζεύγος φυσικών αριθμών a, b ισχύει ότι $a^p + b^p \equiv (a + b)^p \pmod{p}$.

11) Να δειχθεί ότι το 15 διαιρεί τον $2^{2^n} - 1$, για κάθε $n \geq 2$.

12) Να δειχθεί ότι το 9 διαιρεί τον $2^{4n+1} - 2^{2n} - 1$, για κάθε $n \in \mathbb{N}^*$.

13) Να δειχθεί ότι για κάθε $n \in \mathbb{N}^*$, ο αριθμός $3^{4n+1} + 1$ είναι άθροισμα τριών τετραγώνων.

14) Να βρεθεί το υπόλοιπο της διαίρεσης του αριθμού 2^{2048} με το 974849.

15) Να βρεθούν τα τελευταία 1000 ψηφία του αριθμού $1 + 50 + 50^2 + \cdots + 50^{999}$.

16) Να δειχθεί ότι αν κανένας από τρεις κύβους δεν διαιρείται από το 7 ή το 13, τότε το άθροισμα των τριών αυτών κύβων δεν διαιρείται ούτε από το 7 ούτε από το 13.

17) Να δειχθεί ότι γινόμενο οκτώ διαδοχικών φυσικών αριθμών δεν είναι ποτέ τέταρτη δύναμη.

18) Να βρεθούν οι πρώτοι αριθμοί p, q για τους οποίους ισχύει ότι $pq = 7697$ και $\phi(pq) = 7476$.

5.2.4 Παράρτημα: Κριτήρια διαιρετότητας

Μια από τις χαρακτηριστικότερες εφαρμογές της ισοτιμίας είναι στην εύρεση κριτηρίων διαιρετότητας. Στις επόμενες δύο προτάσεις δίνονται κριτήρια διαιρετότητας για ορισμένες ειδικές περιπτώσεις.

Πρόταση 5.34. *Έστω ότι* $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$ *είναι η παράσταση του φυσικού αριθμού* n *στο δεκαδικό σύστημα, με* $0 \leq a_k < 10$, *όπου* $k = 0, 1, \ldots, m$ *και*

$$S(n) = a_m + a_{m-1} + \cdots + a_1 + a_0$$

$$T(n) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m.$$

Τότε
$n \pmod 3 \equiv (a_m + a_{m-1} + \cdots + a_1 + a_0) \pmod 3$, *δηλαδή* $3|n$ *αν και μόνο αν* $3 \mid S(n)$,
$n \pmod 9 \equiv (a_m + a_{m-1} + \cdots + a_1 + a_0) \pmod 9$, *δηλαδή* $9|n$ *αν και μόνο αν* $9 \mid S(n)$,
$n \pmod{11} \equiv (a_0 - a_1 + a_2 - \cdots + (-1)^m a_m) \pmod{11}$, *δηλαδή* $11|n$ *αν και μόνο αν* $11 \mid T(n)$.

Απόδειξη. Θεωρούμε το πολυώνυμο

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m.$$

Επειδή $10 \equiv 1 \pmod 3$, ισχύει ότι

$$f(10) \equiv f(1) \pmod 3.$$

Αλλά,

$$f(10) = n \text{ και } f(1) = S(n),$$

οπότε

$$n \equiv S(n) \pmod 3.$$

Επομένως

$$3 \mid n, \text{ δηλαδή } n \equiv 0 \pmod 3 \text{ αν και μόνο αν } S(n) \equiv 0 \pmod 3, \text{ δηλαδή } 3 \mid S(n).$$

Ομοίως, επειδή $10 \equiv 1 \pmod 9$ προκύπτει ότι $f(10) \equiv f(1) \pmod 9$ και $n \equiv S(n) \pmod 9$. Επομένως

$$9 \mid n, \text{ δηλαδή } n \equiv 0 \pmod 9 \text{ αν και μόνο αν } S(n) \equiv 0 \pmod 9, \text{ δηλαδή } 9 \mid S(n).$$

Επειδή $10 \equiv -1 \pmod{11}$ ισχύει ότι

$$f(10) \equiv f(-1) \pmod{11}.$$

Αλλά

$$f(10) = n \text{ και } f(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T(n),$$

οπότε

$$n \equiv T(n) \pmod{11}.$$

Επομένως

$$11 \mid n, \text{ δηλαδή } n \equiv 0 \pmod{11} \text{ αν και μόνο αν } T(n) \equiv 0 \pmod{11}, \text{ δηλαδή } 11 \mid T(n). \qquad \square$$

Παραδείγματα

1. Ο αριθμός 35686534572 διαιρείται από το 9 (και το 3) αφού

$$S(35686534572) = 3+5+6+8+6+5+3+4+5+7+2 = 54$$

και $3 \mid 54$ και $9 \mid 54$.

Ο αριθμός 3568653457230 διαιρείται από το 3 αλλά όχι από το 9 αφού

$$S(3568653457230) = 3+5+6+8+6+5+3+4+5+7+2+3+0 = 57$$

και $3 \mid 57$, ενώ $9 \nmid 57$.

2. Ο αριθμός 5172839405164728 διαιρείται από το 11 αφού

$$T(5172839405164728) = 8-2+7-4+6-1+5-0+4-9+3-8+2-7+1-5 = 0$$

και $11 \mid 0$.

Ο αριθμός 7893 δεν διαιρείται από το 11 αφού

$$T(7893) = 3-9+8-7 = -5$$

και $11 \nmid -5$.

Πρόταση 5.35. *Έστω ότι ο φυσικός αριθμός n γράφεται με την μορφή*

$$n = 10a_1 + a_0$$

όπου $0 \leq a_0 < 10$. Τότε
$7 \mid n$ *αν και μόνο αν* $7 \mid a_1 - 2a_0$,
$13 \mid n$ *αν και μόνο αν* $13 \mid a_1 - 9a_0$.

Απόδειξη. Παρατηρούμε ότι

$$7 \mid n \text{ αν και μόνο αν } 7 \mid 2n.$$

Επειδή $20 \equiv -1 \pmod 7$ προκύπτει ότι

$$20a_1 \equiv -a_1 \pmod 7,$$

οπότε

$$2n \equiv 20a_1 + 2a_0 \equiv -(a_1 - 2a_0) \pmod 7.$$

Επομένως

$$2n \equiv 0 \pmod 7 \text{ αν και μόνο αν } a_1 - 2a_0 \equiv 0 \pmod 7.$$

Τελικά

$$7 \mid n \text{ αν και μόνο αν } 7 \mid a_1 - 2a_0.$$

Αντίστοιχα, παρατηρούμε ότι

$$13 \mid n \text{ αν και μόνο αν } 13 \mid 9n.$$

Επειδή $90 \equiv -1 \pmod{13}$ προκύπτει ότι

$$90a_1 \equiv -a_1 \pmod{13},$$

οπότε

$$9n \equiv 90a_1 + 9a_0 \equiv -(a_1 - 9a_0) \pmod{13}.$$

Επομένως

$$9n \equiv 0 \pmod{13} \text{ αν και μόνο αν } a_1 - 9a_0 \equiv 0 \pmod{13}.$$

Τελικά

$$13 \mid n \text{ αν και μόνο αν } 13 \mid a_1 - 9a_0. \qquad \square$$

Η αξία αυτών των κριτηρίων είναι ότι μπορούν να εφαρμοσθούν επαναληπτικά. Για παράδειγμα, ο αριθμός 2481443 δεν διαιρείται από το 7. Πράγματι, αν $7 \mid 2481443$ τότε ισχύουν οι ισοδυναμίες

$$\begin{aligned} 7 \mid 2481443 &\Leftrightarrow 7 \mid 248144 - 2 \cdot 3 = 248138 \\ &\Leftrightarrow 7 \mid 24813 - 2 \cdot 8 = 24797 \\ &\Leftrightarrow 7 \mid 2479 - 2 \cdot 7 = 2465 \\ &\Leftrightarrow 7 \mid 246 - 2 \cdot 5 = 236 \\ &\Leftrightarrow 7 \mid 23 - 2 \cdot 6 = 11, \end{aligned}$$

το οποίο είναι άτοπο αφού $7 \nmid 11$.

Ο αριθμός 12987 διαιρείται από το 13. Πράγματι, $13 \mid 12987$ ισοδυναμεί με $13 \mid 1298 - 9 \cdot 7$ που σημαίνει ότι $13 \mid 1298 - 63 = 1235$. Συνεπώς $13 \mid 123 - 9 \cdot 5$, δηλαδή $13 \mid 123 - 45 = 78 = 13 \cdot 6$, οπότε $13 \mid 78$.

Παρατήρηση Για τους αριθμούς 2 και 5 εύκολα μπορεί να αποδειχθεί ότι διαιρούν μόνο τους αριθμούς που τελειώνουν σε $0, 2, 4, 6, 8$ και $0, 5$ αντίστοιχα.

5.2.5 Αντιστροφή modulo n

Έστω n σταθερός φυσικός αριθμός με $n \geq 2$. Οι ακέραιοι αριθμοί a, b ονομάζονται **αντίστροφοι modulo** n αν και μόνο αν $ab \equiv 1 \pmod{n}$.

Για παράδειγμα, οι αριθμοί $5, 3$ είναι αντίστροφοι modulo 7 διότι $5 \cdot 3 \equiv 15 \equiv 1 \pmod{7}$.

Αν για τον ακέραιο a υπάρχει ακέραιος b ώστε οι a, b να είναι αντίστροφοι modulo n, τότε λέμε ότι ο a **αντιστρέφεται modulo** n και ο b είναι **ένας αντίστροφος του** a. (Προφανώς και ο b αντιστρέφεται modulo n και ο a είναι ένας αντίστροφος του b.)

Δεν έχουν όλοι οι αριθμοί αντίστροφο modulo n. Πράγματι, αν $n = 2$, τότε οι άρτιοι αριθμοί a δεν έχουν αντίστροφο modulo n διότι για κάθε $b \in \mathbb{Z}$ ισχύει ότι

$$ab \equiv 0 \pmod{2}.$$

Επίσης, αν οι αριθμοί a, b είναι αντίστροφοι modulo n τότε υπάρχουν άπειροι αριθμοί c που είναι αντίστροφοι του a. Πράγματι, για κάθε $k \in \mathbb{Z}$ έστω $c = b + kn$. Τότε

$$ac \equiv a(b + kn) \equiv ab + akn \equiv ab + 0 \equiv ab \equiv 1 \pmod{n}.$$

Μπορούμε να θέσουμε επιπλέον περιορισμούς για τον αντίστροφο ενός αριθμού, όταν υπάρχει, έτσι ώστε να είναι μοναδικός.

Στην επόμενη πρόταση δίδεται μια αναγκαία και ικανή συνθήκη για την αντιστροφή modulo n.

Πρόταση 5.36 (Αντιστροφή modulo n). *Έστω a, n δύο ακέραιοι αριθμοί με $n \geq 2$. Αν a και n είναι πρώτοι προς αλλήλους, τότε υπάρχει μοναδικός ακέραιος υ τέτοιος ώστε $a \cdot \upsilon \equiv 1 \pmod{n}$ και $0 < \upsilon < n$.*

Απόδειξη. Έστω ότι $\gcd(a, n) = 1$. Σύμφωνα με την Πρόταση 5.3 υπάρχουν ακέραιοι s, t τέτοιοι ώστε

$$sa + tn = 1.$$

Διαιρώντας το s με το n έχουμε ότι υπάρχουν $\pi, \upsilon \in \mathbb{Z}$ με

$$s = \pi n + \upsilon, \text{ όπου } 0 < \upsilon < n - 1.$$

(Ισχύει ότι $\upsilon \neq 0$ διότι η εξίσωση $\pi na + tn = 1$ δεν έχει ακέραιες λύσεις (π, t).)

Επομένως, ισχύει ότι

$$(\pi n + \upsilon)a + tn = 1, \text{ όπου } \upsilon \in [n - 1]$$

δηλαδή,

$$\upsilon a - 1 = -(t + \pi a)n.$$

Άρα, $n \mid \upsilon a - 1$, οπότε

$$a\upsilon \equiv 1 \pmod{n},$$

δηλαδή ο $\upsilon \in [n - 1]$ είναι αντίστροφος του a modulo n.

Σημειώστε ότι ο υ είναι το υπόλοιπο της διαίρεσης του s με το n, δηλαδή $\upsilon = s \bmod n$.

Αντίστροφα, έστω ότι υπάρχει $\upsilon \in [n - 1]$ τέτοιο ώστε

$$a\upsilon \equiv 1 \pmod{n},$$

οπότε υπάρχει ακέραιος αριθμός k ώστε

$$a\upsilon = 1 + kn$$

ή, ισοδύναμα

$$av + (-k)n = 1,$$

δηλαδή, ο 1 εκφράζεται ως γραμμικός συνδυασμός των a, n με ακέραιους συντελεστές. Επειδή, ο μκδ των a, n είναι ο ελάχιστος θετικός αριθμός με αυτή την ιδιότητα έπεται ότι $\gcd(a, n) = 1$, δηλαδή οι a, n είναι πρώτοι προς αλλήλους.

Ο αριθμός v είναι μοναδικός στο διάστημα $[n-1]$. Πράγματι, έστω ότι υπάρχει $c \in [n-1]$ με $c \neq v$ τέτοιο ώστε

$$a \cdot c \equiv 1 \pmod{n}.$$

Τότε,

$$v \cdot a \cdot c \equiv v \pmod{n}$$

$$c \equiv v \pmod{n}.$$

Επομένως,

$$n|(c - v).$$

Αλλά $0 < v, c < n$ και επομένως $0 \leq |c - v| < n$. Ο μοναδικός αριθμός που διαιρεί ο n σ' αυτό το διάστημα είναι το 0, επομένως $|c - v| = 0$, δηλαδή $c = v$. □

Ο αριθμός $v \in [n-1]$ συμβολίζεται με a^{-1} και ονομάζεται **ο αντίστροφος του** a **modulo** n.

Μέθοδος εύρεσης του αντίστροφου modulo n

Από την προηγούμενη απόδειξη προκύπτει ότι στην περίπτωση όπου $\gcd(a, n) = 1$, ο αντίστροφος του a είναι μοναδικός στο διάστημα $[n-1]$ και αν s, t είναι ακέραιοι με

$$as + nt = 1$$

τότε $a^{-1} = s \bmod n$.

Επομένως, η εύρεση του αντίστροφου ανάγεται στην εύρεση των s, t.

Για το σκοπό αυτό χρησιμοποιούμε την διαδικασία του αλγόριθμου του Ευκλείδη.

Παράδειγμα 5.2.2. *Να βρεθεί, αν υπάρχει, ο αντίστροφος του* 7 *modulo* 18.

Λύση. Επειδή $\gcd(7, 18) = 1$, ο αντίστροφος του 7 modulo 18 υπάρχει και είναι μοναδικός.

Για να τον υπολογίσουμε, αρχικά εκτελούμε τις διαιρέσεις των βημάτων του αλγορίθμου του Ευκλείδη.

$$18 = 2 \cdot 7 + 4$$
$$7 = 1 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1,$$

έπειτα λύνουμε τις ισότητες ως προς τα υπόλοιπα κάθε διαίρεσης

$$1 = 4 - 1 \cdot 3$$
$$3 = 7 - 1 \cdot 4$$
$$4 = 18 - 2 \cdot 7,$$

και στη συνέχεια κάνουμε διαδοχικές αντικαστάσεις των πηλίκων και υπολοίπων, όπως παρακάτω:

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) = -1 \cdot 7 + 2 \cdot 4 \\ &= -1 \cdot 7 + 2 \cdot (18 - 2 \cdot 7) \\ &= -5 \cdot 7 + 2 \cdot 18 \\ &= (13 - 18) \cdot 7 + 2 \cdot 18 \\ &= 13 \cdot 7 + 1 \cdot 18. \end{aligned}$$

Επομένως, ο αντίστροφος του 7 modulo 18 είναι το 13.
Πράγματι, $7 \cdot 13 = 91$ και $91 \equiv 1 \bmod 18$, αφού $91 - 1 = 5 \cdot 18$. □

Παρατήρηση. Αν έχουμε υπολογίσει και γνωρίζουμε τον αντίστροφο του a modulo n τότε μπορούμε να λύσουμε άμεσα κάθε εξίσωση της μορφής $ax \equiv b \pmod{n}$. Πράγματι, πολλαπλασιάζοντας κατά μέλη με a^{-1} έχουμε ότι $x \equiv a^{-1}b \pmod{n}$, δηλαδή οι λύσεις της είναι οι αριθμοί $x = a^{-1}b + kn$, $k \in \mathbb{Z}$.

Παράδειγμα 5.2.3. *Να λυθεί η εξίσωση* $7x \equiv 5 \bmod 18$.

Λύση. Στο προηγούμενο παράδειγμα, υπολογίσαμε ότι ο αντίστροφος του 7 modulo 18 είναι το 13, δηλαδή $7 \cdot 13 \equiv 1 \bmod 18$.

Πολλαπλασιάζοντας την εξίσωση κατά μέλη με το 13 έχουμε ότι

$$x \equiv 5 \cdot 13 \equiv 65 \equiv 11 \bmod 18.$$

Άρα, οι λύσεις της εξίσωσης είναι όλα τα $x = 11 + 18k$, $k \in \mathbb{Z}$. □

Παρατήρηση. Το θεώρημα Euler-Fermat είναι χρήσιμο για την μείωση του εκθέτη σε παραστάσεις της μορφής $a^k \bmod n$, όταν $\gcd(a, n) = 1$ και $k \geq \phi(n)$. Στην περίπτωση όπου $k < \phi(n)$ μπορούμε (αν μας συμφέρει υπολογιστικά) και πάλι να αξιοποιήσουμε το θεώρημα Euler-Fermat χρησιμοποιώντας την τεχνική που παρουσιάζεται στο επόμενο παράδειγμα.

Παράδειγμα 5.2.4. *Να βρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση*

$$x \equiv 7^{38} \bmod 100.$$

Λύση. Επειδή $\gcd(7, 100) = 1$ και $\phi(100) = \phi(2^2 \cdot 5^2) = 40$ από το θεώρημα Euler-Fermat έπεται ότι

$$7^{40} \equiv 1 \bmod 100$$

Επειδή, ο εκθέτης του 7 είναι μικρότερος από 40 δεν μπορούμε να χρησιμοποιήσουμε άμεσα το θεώρημα Euler-Fermat. Θα υπολογίσουμε τον αντίστροφο του 7 modulo 100 και με τη βοήθεια αυτού εύκολα θα υπολογίσουμε το x. Από τον αλγόριθμο του Ευκλείδη έχουμε ότι

$$\begin{aligned} 100 &= 14 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

οπότε

$$1 = 1 \cdot 7 + (-3) \cdot 2 = 1 \cdot 7 + (-3)(1 \cdot 100 + (-14) \cdot 7) = (-3) \cdot 100 + 43 \cdot 7.$$

Άρα, ο αντίστροφος του 7 modulo 100 είναι το 43. Ισχύει ότι

$$x \equiv 7^{38} \equiv 7^{38} \cdot 1^2 \equiv 7^{38} \cdot (7 \cdot 43)^2 \equiv 7^{40} \cdot 43^2 \equiv 1^{40} \cdot 1849 \equiv 49 \bmod 100.$$

Εναλλακτικά, αντί του αντιστρόφου μπορούμε να χρησιμοποιήσουμε το γνωστό τέχνασμα του υποδιπλασιασμού των δυνάμεων:

$$x = 7^{38} \equiv (7^2)^{19} \equiv 49^{19} \equiv 49 \cdot 49^{18} \equiv 49 \cdot (49^2)^9 \equiv 49 \cdot (2401)^9 \equiv 49 \cdot 1^9 \equiv 49 \bmod 100. \qquad \square$$

Ασκήσεις προς επίλυση

1) Να βρεθούν οι αντίστροφοι των 3 mod 14, 4 mod 17 και 6 mod 13.

2) Να λυθούν οι εξισώσεις $3x \equiv 7 \bmod 14$, $4x \equiv 5 \bmod 17$ και $6x \equiv 11 \bmod 13$.

3) Να βρεθεί ο ελάχιστος φυσικός αριθμός x που είναι λύση των παρακάτω εξισώσεων

   i) $x \equiv 13^{90} \bmod 360$.

   ii) $x \equiv 73^{30} \bmod 120$.

5.2.6 Παράρτημα: Το σύστημα κρυπτογράφησης RSA

Το σύστημα κρυπτογράφησης RSA επινοήθηκε το 1976 από τους Ronald **R**ivest, Adi **S**hamir και Leonard **A**dleman.

Το σύστημα κρυπτογράφησης RSA βασίζεται στην εξής ιδέα:

Έστω p, q δύο πρώτοι αριθμοί και $n = pq$.
Επίσης, έστω e ένας αριθμός έτσι ώστε $\gcd((p-1)(q-1), e) = 1$. Τότε υπάρχει αριθμός d έτσι ώστε $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Για παράδειγμα, αν $p = 43$ και $q = 47$, τότε $n = 2021$.

Επίσης, για $e = 13$ ισχύει ότι $\gcd((43-1)(47-1), 13) = 1$. Τότε, ο αντίστροφος του $e = 13$ modulo (43-1)(47-1) = 1932 είναι το $d = 1189$.

Από το θεώρημα του Euler, για κάθε φυσικό αριθμό M με $\gcd(M, n) = 1$ ισχύει η ιδιότητα

$$M^{\phi(n)} \equiv 1 \pmod{n}.$$

Όμως

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1),$$

και επομένως

$$M^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

Η παραπάνω ισοτιμία είναι η κεντρική ιδέα του αλγορίθμου RSA.

Ένα άτομο A επιλέγει μυστικά τους αριθμούς p, q και δημοσιεύει τους αριθμούς n και e.

Ο B για να στείλει με ασφάλεια το μήνυμα M στην A αρκεί να στείλει το αποτέλεσμα

$$C = M^e \pmod{n}.$$

Ο A για να διαβάσει το μήνυμα M αρκεί να υπολογίσει το αποτέλεσμα

$$C^d \pmod{n}.$$

Πράγματι,

$$C^d \equiv (M^e)^d \equiv M^{ed} \pmod{n}.$$

Επειδή $ed \equiv 1 \pmod{(p-1)(q-1)}$, εξ ορισμού προκύπτει ότι

$$ed = k(p-1)(q-1) + 1, \text{ για κάποιο } k \in \mathbb{N},$$

οπότε

$$M^{ed} \equiv M^{k(p-1)(q-1)+1} \pmod{n} \equiv (M^{(p-1)(q-1)})^k \cdot M \pmod{n} \equiv M \mod n,$$

δηλαδή, προκύπτει το αρχικό μήνυμα M.

Για το προηγούμενο παράδειγμα, για να στείλει με ασφάλεια ο B το μήνυμα $M = 501$ στον A αρκεί να στείλει το αποτέλεσμα

$$C = 501^{13} \pmod{2021} = 77.$$

Ο A για να διαβάσει το μήνυμα M αρκεί να υπολογίσει το αποτέλεσμα

$$77^{1189} \pmod{2021} = 501.$$

Η ασφάλεια του συστήματος RSA βασίζεται στην δυσκολία παραγοντοποίησης ενός αριθμού n της μορφής $n = pq$, όταν οι p, q έχουν εκατοντάδες ψηφία. Ακόμη και αν κάποιος υποκλέψει το κρυπτογραφημένο μήνυμα C είναι επίσης δύσκολο να λυθεί το πρόβλημα υπολογισμού κάποιου X έτσι ώστε $X^e = C \pmod{n}$. Μία μικρή λεπτομέρεια στον αλγόριθμο RSA είναι ότι πρέπει $\gcd(M, n) = 1$, το οποίο στην πράξη συμβαίνει πάντα.

5.2.7 Το κινέζικο θεώρημα υπολοίπων

Πρόταση 5.37 (Κινέζικο θεώρημα υπολοίπων). *Έστω $n_1, n_2, \ldots, n_k$ θετικοί ακέραιοι ανά δύο σχετικά πρώτοι μεταξύ τους, και $a_1, a_2, \ldots, a_n$ ακέραιοι. Το σύστημα γραμμικών ισοτιμιών*

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k \end{aligned}$$

έχει μοναδική λύση $\mod n_1 n_2 \cdots n_k$. *Η λύση δίνεται από τον τύπο*

$$x = \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \cdots + \frac{n}{n_k} b_k a_k \pmod{n_1 \cdot n_2 \cdots n_k}$$

όπου b_i είναι ο αντίστροφος του $\dfrac{n}{n_i}$ modulo n_i.

Απόδειξη. Έστω $n = n_1 n_2 \cdots n_k$. Για κάθε $i = 1, 2, \ldots, k$ ισχύει ότι

$$\gcd\left(\frac{n}{n_i}, n_i\right) = 1$$

και επομένως υπάρχει b_i ώστε

$$\frac{n}{n_i} b_i \equiv 1 \mod n_i.$$

Επίσης, ισχύει ότι

$$\frac{n}{n_i} b_i \equiv 0 \mod n_j, \text{ για κάθε } i \neq j.$$

Ο αριθμός

$$x = \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \cdots + \frac{n}{n_k} b_k a_k$$

είναι λύση του δοθέντος συστήματος ισοτιμιών, αφού για κάθε $i = 1, 2, \ldots, k$ έχουμε ότι

$$\begin{aligned} x &\equiv \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \cdots + \frac{n}{n_k} b_k a_k \mod n_i \\ &\equiv \frac{n}{n_i} b_i a_i \mod n_i \\ &\equiv a_i \mod n_i. \end{aligned}$$

Αν τώρα x, x' είναι δύο λύσεις του συστήματος, τότε $x \equiv x' \mod n_i$ οπότε $n_i \mid (x - x')$ για κάθε $i = 1, 2, \ldots, k$. Αφού οι $n_1, n_2, \ldots, n_k$ είναι σχετικά πρώτοι ανά δύο, προκύπτει ότι $n \mid (x - x')$, δηλαδή $x' \equiv x \mod n$. Συνεπώς, η λύση είναι μοναδική ως προς $\mod n$. □

Παρατήρηση. Η απόδειξη του Κινέζικου θεωρήματος υπολοίπων μας δίνει και μια μέθοδο για την εύρεση της λύσης του συστήματος

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k. \end{aligned}$$

Για κάθε n_i, όπου $i \in [k]$, βρίσκουμε τον αντίστροφο b_i του $\frac{n}{n_i}$ modulo n_i.
Η λύση του συστήματος είναι το άθροισμα

$$x = \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \cdots + \frac{n}{n_k} b_k a_k \pmod{n_1 \cdot n_2 \cdots n_k}.$$

Εφαρμογές

Εφαρμογή 5.2.13. *Σε ένα καλάθι βρίσκονται μήλα. Αν τα χωρίσουμε σε τριάδες περισσεύουν δύο, αν τα χωρίσουμε σε πεντάδες περισσεύουν τρία και αν τα χωρίσουμε σε επτάδες περισσεύουν τέσσερα. Πόσα μήλα βρίσκονται στο καλάθι;*

Το πρόβλημα ανάγεται στην εύρεση της λύσης του συστήματος ισοτιμιών

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 7. \end{aligned}$$

Επειδή οι αριθμοί 3, 5, 7 είναι σχετικά πρώτοι ανά δύο, από το Κινέζικο θεώρημα υπολοίπων το σύστημα έχει μοναδική λύση αν $x \leq 3 \cdot 5 \cdot 7 = 105$. Αρκεί να βρεθούν ακέραιοι b_1, b_2, b_3 με

$$5 \cdot 7 \cdot b_1 \equiv 1 \mod 3$$

$$3 \cdot 7 \cdot b_2 \equiv 1 \mod 5$$

$$3 \cdot 5 \cdot b_3 \equiv 1 \mod 7,$$

ή ισοδύναμα

$$35 \cdot b_1 \equiv 1 \mod 3$$

$$21 \cdot b_2 \equiv 1 \mod 5$$

$$15 \cdot b_3 \equiv 1 \mod 7.$$

Επειδή $35 \equiv 2 \mod 3$, $21 \equiv 1 \mod 5$ και $15 \equiv 1 \mod 7$, προκύπτουν οι ισοδύναμες εξισώσεις

$$2 \cdot b_1 \equiv 1 \mod 3$$

$$1 \cdot b_2 \equiv 1 \mod 5$$

$$1 \cdot b_3 \equiv 1 \mod 7.$$

Εύκολα προκύπτει ότι $b_1 = 2$, $b_2 = b_3 = 1$.
Επομένως, η ζητούμενη λύση είναι

$$\begin{aligned} x &= \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \frac{n}{n_3} b_3 a_3 \mod 105 \\ &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 4 = 140 + 63 + 60 \mod 105 \\ &= 263 \mod 105 \\ &= 53. \end{aligned}$$

Δηλαδή, στο καλάθι βρίσκονται 53 μήλα.

Ασκήσεις προς επίλυση

1) Να εφαρμοστεί το κινέζικο θέωρημα υπολοίπων στα παρακάτω συστήματα γραμμικών ισοτιμιών

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 4 \pmod{11} \end{aligned}$$

$$\begin{aligned} x &\equiv 2 \pmod{15} \\ x &\equiv 5 \pmod{14} \end{aligned}$$

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 5 \pmod 3 \\ x &\equiv 1 \pmod 2 \end{aligned}$$

2) Να λυθεί το παρακάτω σύστημα γραμμικών ισοτιμιών

$$\begin{aligned} 5x &\equiv 3 \pmod 7 \\ 3x &\equiv 4 \pmod{11} \end{aligned}$$

5.2.8 Παράρτημα: Αναπαράσταση αριθμών modulo $n_1, n_2, \ldots, n_k$

Επειδή η λύση του συστήματος

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k \end{aligned}$$

είναι μοναδική modulo $n_1 n_2 \cdots n_k$, προκύπτει ότι τα $a_1, a_2, \ldots, a_k$ μπορούν να χρησιμοποιηθούν ως μοναδική αναπαράσταση κάθε αριθμού x στο διάστημα $[n_1 n_2 \cdots n_k]$, (όπως αντίστοιχα τα ψηφία $\{0, 1, \ldots, 9\}$ χρησιμοποιούνται για να αναπαραστήσουν ένα αριθμό στο δεκαδικό σύστημα).

Παράδειγμα 5.2.5. *Να βρεθεί η αναπαράσταση όλων των αριθμών από* 1 *εώς* 105 mod 105.

Παρατηρούμε ότι $105 = 3 \cdot 5 \cdot 7$, όπου $\gcd(3,5) = \gcd(3,7) = \gcd(5,7) = 1$, και επομένως από το κινέζικο θεώρημα υπολοίπων οι εξισώσεις

$$\begin{aligned} x &\equiv a_1 \mod 3 \\ x &\equiv a_2 \mod 5 \\ x &\equiv a_3 \mod 7 \end{aligned}$$

έχουν μοναδική λύση για κάθε $x \in [105]$. Επομένως κάθε $x \in [105]$ αναπαρίστανται μονοσήμαντα από την τριάδα (a_1, a_2, a_3)

Στον επόμενο πίνακα δίνονται οι αναπαραστάσεις από τριάδες όλων των αριθμών από το 1 εώς το 105

1 (1,1,1)	2 (2,2,2)	3 (0,3,3)	4 (1,4,4)	5 (2,0,5)
6 (0,1,6)	7 (1,2,0)	8 (2,3,1)	9 (0,4,2)	10 (1,0,3)
11 (2,1,4)	12 (0,2,5)	13 (1,3,6)	14 (2,4,0)	15 (0,0,1)
16 (1,1,2)	17 (2,2,3)	18 (0,3,4)	19 (1,4,5)	20 (2,0,6)
21 (0,1,0)	22 (1,2,1)	23 (2,3,2)	24 (0,4,3)	25 (1,0,4)
26 (2,1,5)	27 (0,2,6)	28 (1,3,0)	29 (2,4,1)	30 (0,0,2)
31 (1,1,3)	32 (2,2,4)	33 (0,3,5)	34 (1,4,6)	35 (2,0,0)
36 (0,1,1)	37 (1,2,2)	38 (2,3,3)	39 (0,4,4)	40 (1,0,5)
41 (2,1,6)	42 (0,2,0)	43 (1,3,1)	44 (2,4,2)	45 (0,0,3)
46 (1,1,4)	47 (2,2,5)	48 (0,3,6)	49 (1,4,0)	50 (2,0,1)
51 (0,1,2)	52 (1,2,3)	53 (2,3,4)	54 (0,4,5)	55 (1,0,6)
56 (2,1,0)	57 (0,2,1)	58 (1,3,2)	59 (2,4,3)	60 (0,0,4)
61 (1,1,5)	62 (2,2,6)	63 (0,3,0)	64 (1,4,1)	65 (2,0,2)
66 (0,1,3)	67 (1,2,4)	68 (2,3,5)	69 (0,4,6)	70 (1,0,0)
71 (2,1,1)	72 (0,2,2)	73 (1,3,3)	74 (2,4,4)	75 (0,0,5)
76 (1,1,6)	77 (2,2,0)	78 (0,3,1)	79 (1,4,2)	80 (2,0,3)
81 (0,1,4)	82 (1,2,5)	83 (2,3,6)	84 (0,4,0)	85 (1,0,1)
86 (2,1,2)	87 (0,2,3)	88 (1,3,4)	89 (2,4,5)	90 (0,0,6)
91 (1,1,0)	92 (2,2,1)	93 (0,3,2)	94 (1,4,3)	95 (2,0,4)
96 (0,1,5)	97 (1,2,6)	98 (2,3,0)	99 (0,4,1)	100 (1,0,2)
101 (2,1,3)	102 (0,2,4)	103 (1,3,5)	104 (2,4,6)	105 (0,0,0)

Πρόταση 5.38. *Έστω $n_1, n_2, \ldots, n_k$ ακέραιοι αριθμοί ανά δύο σχετικά πρώτοι μεταξύ τους, και $n = n_1 n_2 \cdots n_k$. Αν $(a_1, a_2, \ldots, a_k)$ είναι η αναπαράσταση του x και $(b_1, b_2, \ldots, b_k)$ είναι η αναπαράσταση του y, τότε η αναπαράσταση του $(x + y) \bmod n$ είναι η*

$$((a_1 + b_1) \bmod n_1,\ (a_2 + b_2) \bmod n_2,\ \ldots,\ (a_k + b_k) \bmod n_k)$$

και η αναπαράσταση του $xy \bmod n$ είναι η

$$((a_1 \cdot b_1) \bmod n_1,\ (a_2 \cdot b_2) \bmod n_2,\ \ldots,\ (a_k \cdot b_k) \bmod n_k).$$

Η αξία της παραπάνω πρότασης είναι ότι ο υπολογισμός της αναπαράστασης του αθροίσματος (και του γινομένου) μπορεί να γίνει παράλληλα ανεξάρτητα για κάθε όρο της τριάδας.

5.2.9 Παράρτημα: RSA και κινέζικο θεώρημα υπολοίπων

Με την χρήση του κινέζικου θεωρήματος υπολοίπων προκύπτει μια μικρή βελτίωση της μεθόδου αποκρυπτογράφησης του αλγορίθμου RSA. (Για τους συμβολισμούς βλέπε σελ. 262.)

Αν $\gcd(M, n) = 1$, τότε $\gcd(M, p) = 1$ και $\gcd(M, q) = 1$

Επομένως, προκύπτει ότι

$$C^d \equiv M^{ed} \equiv M^{k(p-1)(q-1)+1} \equiv (M^{(p-1)})^{k(q-1)} \cdot M \equiv (M^{\phi(p)})^{k(q-1)} \cdot M \equiv 1 \cdot M \equiv M \pmod{p}$$

$$C^d \equiv M^{ed} \equiv M^{k(p-1)(q-1)+1} \equiv (M^{(q-1)})^{k(p-1)} \cdot M \equiv (M^{\phi(q)})^{k(q-1)} \cdot M \equiv 1 \cdot M \equiv M \pmod{q}$$

ή, ισοδύναμα

$$M \equiv C^d \pmod{p}$$

$$M \equiv C^d \pmod{q}.$$

Από το κινέζικο θεώρημα υπολοίπων προκύπτει ότι[6]

$$M \equiv C^d \pmod{pq}.$$

Για το προηγούμενο παράδειγμα, (βλέπε σελίδα 262), ο A για να διαβάσει το μύνημα M υπολογίζει πρώτα τα αποτελέσματα

$$77^{1189} \pmod{43} = 28$$

$$77^{1189} \pmod{47} = 31.$$

Επομένως, το M είναι η λύση του συστήματος

$$M \equiv 28 \pmod{43}$$

$$M \equiv 31 \pmod{47}.$$

Αρκεί να βρεθούν ακέραιοι b_1, b_2 έτσι ώστε

$$47 \cdot b_1 \equiv 1 \pmod{43}$$

$$43 \cdot b_2 \equiv 1 \pmod{47}$$

ή, ισοδύναμα

$$4 \cdot b_1 \equiv 1 \pmod{43}$$

$$43 \cdot b_2 \equiv 1 \pmod{47}.$$

Από τον αλγόριθμο του Ευκλείδη προκύπτει ότι $b_1 = 11$ και $b_2 = 35$.

Επομένως,

$$M \equiv \frac{43 \cdot 47}{43} \cdot 11 \cdot 28 + \frac{43 \cdot 47}{47} \cdot 35 \cdot 31 \equiv 61131 \equiv 501 \pmod{2021}.$$

[6] Επειδή $M \equiv C^d \pmod{p}$ έπεται ότι υπάρχει a_1 ώστε $C_d \equiv a_1 \pmod{p}$ και $M \equiv a_1 \pmod{p}$. Ανάλογα υπάρχει a_2 ώστε $C_d \equiv a_2 \pmod{q}$ και $M \equiv a_2 \pmod{q}$. Αλλά το σύστημα $x \equiv a_1 \pmod{p}$, $x \equiv a_2 \pmod{q}$ έχει μοναδική λύση $\pmod{pq}$, και επομένως $M \equiv C^d \pmod{pq}$.

5.2.10 Παράρτημα: Ψηφιακό κορώνα ή γράμματα

Η υπολογιστική δυσκολία που παρουσιάζουν ορισμένα προβλήματα της θεωρίας αριθμών μπορεί να αξιοποιηθεί για την κατασκευή πρωτόκολλων που αφορούν τομείς της ασφάλειας, όπως η εμπιστευτικότητα, η αυθεντικότητα, η εγκυρότητα και η διαθεσιμότητα.

Στην παράγραφο αυτή παρουσιάζεται ένα πρωτόκολλο για την υλοποίηση ενός ψηφιακού παιχνιδιού ΚΟΡΩΝΑ ή ΓΡΑΜΜΑΤΑ, η εγκυρότητα του οποίου βασίζεται αποκλειστικά στη δυσκολία του *προβλήματος της παραγοντοποίησης μεγάλων αριθμών*.[7]

Η βασική ιδέα του πρωτοκόλλου είναι η εξής:

Ο παίκτης A επιλέγει (μυστικά) δύο μεγάλους πρώτους αριθμούς p, q και υπολογίζει το γινόμενό τους $n = pq$, το οποίο ανακοινωνεί στον παίκτη B.

Ο παίκτης B καλείται να βρει τους παράγοντες του n. Αν το πετύχει αυτό, τότε κερδίζει, αλλιώς κερδίζει ο παίκτης A.

Προφανώς, όπως αναφέραμε, αν ο n είναι αρκετά μεγάλος αριθμός, τότε ο στόχος αυτός είναι ανέφικτος για τον B και επομένως το πρωτόκολλο είναι άδικο γι᾽ αυτόν. Απαιτείται να δοθεί στον B κάποια επιπλέον πληροφορία σχετικά με τον αριθμό n.

Η πληροφορία αυτή πρέπει να είναι τέτοια ώστε ο B να μην μπορεί να βρει πάντα τους παράγοντες του n, για την ακρίβεια πρέπει να πετυχαίνει το στόχο του μόλις στις μισές περιπτώσεις.

Ποια πρέπει να είναι αυτή η πληροφορία;

Η βασική ιδέα δίδεται στην επόμενη πρόταση

Πρόταση 5.39. *Έστω $n = pq$, όπου p, q είναι πρώτοι αριθμοί με $p \equiv q \equiv 3 \pmod 4$, τότε για κάθε φυσικό $1 \leq a < n$ ισχύει ότι*

- *Η εξίσωση*
$$x^2 \equiv a \pmod n$$
έχει ακριβώς δύο ακέραιες λύσεις x_1, x_2 στο σύνολο $\{1, 2, \ldots, n-1\}$.

- *Από τις λύσεις x_1, x_2 μπορούμε να υπολογίσουμε τα p και q.*
Συγκεκριμένα, $\gcd(x_1 - x_2, n) = p$ ή q.

- *Ο υπολογισμός των δύο λύσεων x_1, x_2 είναι υπολογιστικά εφικτός μόνο αν γνωρίζουμε τα p και q.*
Συγκεκριμένα, αν $sp + tq = 1$ και $p_1 = (x^2)^{((p+1)/4)} \pmod p$ και $q_1 = (x^2)^{((q+1)/4)} \pmod q$, τότε
$$x_1 = q_1 sp + p_1 tq \pmod n$$
και
$$x_2 = q_1 sp - p_1 tq \pmod n.$$

Το πρωτόκολλο Blum

1. Ο παίκτης A επιλέγει μυστικά δύο πρώτους p, q και ανακοινώνει στον παίκτη B το γινόμενό τους $n = pq$.

2. Ο παίκτης B επιλέγει μυστικά έναν αριθμό x και ανακοινώνει στον παίκτη A τον αριθμό $a = x^2 \pmod n$.

[7] Αν δοθεί ένας μεγάλος αριθμός $n \in \mathbb{N}^*$ θεωρείται "δύσκολο" να βρεθούν οι πρώτοι παράγοντες του n. (Πρόβλημα παραγοντοποίησης.)

3. Ο παίκτης A λύνει την εξίσωση $a \equiv x^2 \pmod{n}$ και στέλνει στον παίκτη B μία από τις δύο λύσεις της $x_1 = x$ και x_2.

4. - Αν ο παίκτης B λάβει τη λύση $x_2 \neq x$, τότε ο αριθμός $\gcd(x - x_2, n)$ είναι ένας από τους δυο πρώτους παράγοντες του n, και άρα κερδίζει.
   - Αν ο παίκτης B λάβει την ίδια λύση, δεν μπορεί να βρει τους παράγοντες του n και χάνει.

Παράδειγμα.

1. Ο παίκτης A επιλέγει τους πρώτους αριθμούς $p = 16017259$ και $q = 19354351$ για τους οποίους $p \equiv q \equiv 3 \pmod{4}$ και ανακοινώνει στον παίκτη B το γινόμενό τους $n = 16017259 \cdot 19354351 = 310003652743909$.

2. Ο παίκτης B επιλέγει τον αριθμό $x = 43543331$ και στέλνει στον παίκτη A τον αριθμό $x^2 \pmod{n} = 35999758112107$.

3. Ο παίκτης A βρίσκει s, t ώστε $sp + tq = 1$ (χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη). Στο παράδειγμα, $s = 9467907$ και $t = -11440484$.

   Επίσης, υπολογίζει τους αριθμούς $p_1 = (x^2)^{((p+1)/4)} \pmod{p}$ και $q_1 = (x^2)^{((q+1)/4)} \pmod{q}$. Στο παράδειγμα, $p_1 = 14519722$ και $q_1 = 11508813$.

4. Άρα, ο A υπολογίζει ότι οι λύσεις της εξίσωσης είναι αριθμοί $x_1 = q_1sp + p_1tq \pmod{n}$ και $x_2 = q_1sp - p_1tq \pmod{n}$ Στο παράδειγμα,

$$x_1 = 283264644285230 \text{ και } x_2 = 43543331$$

5. - Αν ο B λάβει τη λύση x_1 τότε υπολογίζει το $\gcd(x_1 - x, n)$ και βρίσκει ότι $\gcd(283264644285230 - 43543331, 310003652743909) = 16017259 = p$. Άρα, βρίσκει τους παράγοντες του n και κερδίζει.
   - Αν ο B λάβει τη λύση x_2 τότε δεν μπορεί να παραγοντοποιήσει το n και χάνει.

Ασκήσεις προς επίλυση

1) Να κατασκευασθεί ένα πρωτόκολλο για ένα ψηφιακό ζάρι στο οποία πρέπει να κερδίζουμε 1 στις 6 φορές.

2) Να κατασκευασθεί ένα πρωτόκολλο για μια ψηφιακή ρουλέτα στην οποία πρέπει να κερδίζουμε 1 στις 32 φορές.

5.2.11 Παράρτημα: Το τεστ του Fermat

Έστω $n \in \mathbb{N}^*$ με $n \geq 2$. Ορίζουμε το σύνολο $U_n \subseteq [n]$ ως εξής:

$$a \in U_n \text{ αν και μόνο αν } \gcd(a, n) = 1.$$

Μια πολύ σημαντική παρατήρηση είναι ότι αν $\gcd(a, n) \neq 1$ τότε

$$a^k \not\equiv 1 \bmod n, \text{ για κάθε } k \in \mathbb{N}^*.$$

Ο λόγος είναι ότι αν υπάρχει $k \geq 2$ ώστε $a^k \equiv 1 \bmod n$, τότε το a^{k-1} είναι το συμμετρικό (αντίστροφο) του a, άρα $a \in U_n$, οπότε $\gcd(a, n) = 1$, το οποίο είναι άτοπο. (Δεν εξετάζουμε την περίπτωση όπου $k = 1$, διότι αφού $\gcd(a, n) \neq 1$, έπεται ότι $a \not\equiv 1 \bmod n$.)

Από το θεώρημα Fermat ισχύει ότι αν p είναι πρώτος αριθμός, τότε

$$a^{p-1} \equiv 1 \bmod p, \text{ για κάθε } a \in U_n.$$

Η ισότητα αυτή, αποτελεί τη βαση για μια μέθοδο ελέγχου, αν ένας φυσικός αριθμός n είναι πρώτος ή όχι, διότι από αυτή προκύπτει η επόμενη πρόταση:

Πρόταση 5.40. *Αν για κάποιο φυσικό αριθμό n υπάρχει ακέραιος αριθμός $a \in \{1, \ldots, n-1\}$ ώστε $a^{n-1} \not\equiv 1 \bmod n$, τότε ο αριθμός n είναι σύνθετος.*

Απόδειξη. Θα χρησιμοποιήσουμε εις άτοπο απαγωγή. Έστω ότι ο n είναι πρώτος.

Διακρίνουμε δύο περιπτώσεις:

α) $a \in U_n$. Τότε $a^{n-1} \equiv 1 \bmod n$, το οποίο είναι άτοπο.

β) $a \notin U_n$. Τότε $\gcd(a, n) \neq 1$, επομένως ο n δεν είναι πρώτος, το οποίο είναι άτοπο.

Άρα, ο n είναι σύνθετος. □

Στην περίπτωση όπου για κάποιο αριθμό n βρούμε ένα a ώστε $a^{n-1} \not\equiv 1 \bmod n$, τότε αμέσως συμπεραίνουμε ότι ο n είναι σύνθετος.

Η πρόταση αυτή δεν μας λέει τι είναι ο n στην περίπτωση όπου για κάποιο $a \in \{1, \ldots, n-1\}$ ισχύει ότι $a^{n-1} \equiv 1 \bmod n$.
Παρόλα αυτά, η ύπαρξη ενός $a \in \{1, \ldots, n-1\}$ για το οποίο $a^{n-1} \equiv 1 \bmod n$ μας δίνει μια σημαντική πληροφορία. Ο λόγος είναι η επομενη πρόταση.

Πρόταση 5.41. *Αν υπάρχει τουλάχιστον ένα $a \in U_n$ με $a^{n-1} \not\equiv 1 \bmod n$, τότε υπάρχουν περισσότερα από $n/2$ τέτοια $a \in \{1, \ldots, n-1\}$.*

Απόδειξη. [8] Έστω

$$H = \{a \in U_n : a^{n-1} \equiv 1 \bmod n\}.$$

Επειδή η ομάδα U_n είναι αβελιανή, εύκολα προκύπτει ότι το H είναι υποομάδα της U_n. Επειδή υπάρχει $a \in U_n$ με $a \notin H$, έπεται ότι $H \neq U_n$. Άρα, αφού $|H| \mid |U_n|$, έπεται ότι $|H| \leq |U_n|/2$, ή ισοδύναμα $|H| \leq \phi(n)/2$.

[8] Η απόδειξη χρησιμοποιεί στοιχειώδεις γνώσεις από τη θεωρία ομάδων, όπως το θεώρημα Lagrange.

Έστω x ο αριθμός των $a \in \{1, \ldots, n-1\}$ με $a^{n-1} \not\equiv 1 \bmod n$. Ισχύει ότι

$$\begin{aligned} x &= |\{1, \ldots, n-1\} \setminus U_n| + |U_n \setminus H| \\ &= (n - 1 - |U_n|) + (|U_n| - |H|) \\ &\geq n - 1 - \phi(n)/2 \\ &\geq n - 1 - (n-2)/2 = n/2. \end{aligned}$$

Άρα $x \geq n/2$. □

Η προηγούμενη πρόταση μας λέει ότι αν ο n είναι σύνθετος αριθμός (και υπάρχει ένα τουλάχιστον $a \in U_n$ με $a^{n-1} \not\equiv 1 \bmod n$), τότε υπάρχει μεγάλη πιθανότητα (πάνω από 1/2) να βρούμε ένα τέτοιο a που μας αποδεικνύει ότι ο n είναι σύνθετος αριθμός, αφού περισσότερα από τα μισά a από 1 εώς $n-1$ έχουν αυτή την ιδιότητα.

Αντίθετα, αν δεν βρίσκουμε ένα τέτοιο a, η πιθανότητα ο n να είναι πρώτος είναι μεγάλη (πάνω από 1/2).

Η ιδέα είναι να επιλέξουμε με τυχαίο τρόπο μερικά a ανάμεσα στο 1 και στο $n-1$.

Αν ο αριθμός n είναι σύνθετος και επιλέξουμε k τυχαία a η πιθανότητα να μην βρούμε κάποιο που αποδεικνύει ότι ο n είναι σύνθετος είναι μικρότερη από $1/2^k$, ή ισοδύναμα αν για k τυχαίες τιμές του a επαληθεύεται η ισότητα $a^{n-1} \equiv 1 \bmod n$ η πιθανότητα ο n να είναι πρώτος αριθμός είναι μεγαλύτερη από $1 - 1/2^k$. Πρακτικά, μετά από 20 επιτυχείς δοκιμές, η πιθανότητα ο αριθμός n να είναι σύνθετος είναι μικρότερη από 1 στο 1000000.

Η μέθοδος αυτή ονομάζεται τεστ του Fermat.

Με τη μέθοδο αυτή δεν είμαστε βέβαιοι αν ένας αριθμός είναι πρώτος, αλλά έχουμε μεγάλη πιθανότητα να είμαστε σωστοί.

Εν τούτοις, η μέθοδος αυτή αποτυγχάνει για κάποιους σύνθετους αριθμούς, τους λεγόμενους **αριθμούς Carmicael**. Οι αριθμοί αυτοί έχουν την ιδιότητα

$$a^{n-1} \equiv 1 \bmod n$$

για κάθε $a \in U_n$, όπου n είναι αριθμός Carmicael.

Συνεπώς, τα $a \in \{1, 2, \ldots, n-1\}$ για τα οποία $a^{n-1} \not\equiv 1 \bmod n$ είναι πολύ λίγα σε σχέση με τα στοιχεία του $\{1, \ldots, n-1\}$ και άρα είναι απίθανο να βρεθούν.

Για τους αριθμούς Carmicael ισχύει η επόμενη ιδιότητα: Ένας περιττός σύνθετος αριθμός n είναι αριθμός Carmicael αν και μόνο αν ο n δεν διαιρείται από το τετράγωνο κάποιου πρώτου και κάθε πρώτος p διαιρέτης του n είναι τέτοιος ώστε $p - 1 \mid n - 1$.

Οι επτά μικρότεροι αριθμοί Carmicael είναι οι: $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$, $8911 = 7 \cdot 19 \cdot 67$.

5.2.12 Παράρτημα: Το πρόβλημα του κύκλου του Gauss

Έστω $r_2(n)$ ο αριθμός των τρόπων με τους οποίου μπορούμε να εκφράσουμε τον φυσικό αριθμό n ως άθροισμα δύο τετραγώνων a^2 και b^2 όπου a, b είναι ακέραιοι αριθμοί, δηλαδή στη μορφή

$$n = a^2 + b^2.$$

Παρατήρηση Θεωρούμε ότι οι εκφράσεις $a^2 + b^2$ και $b^2 + a^2$ είναι διαφορετικές, δηλαδή οι λύσεις είναι διατεταγμένα ζεύγη.

Για παράδειγμα, ο αριθμός 5 εκφράζεται με οκτώ διαφορετικούς τρόπους ώς άθροισμα δύο τετραγώνων:

$$5 = 2^2 + 1^2 = 1^2 + 2^2 = (-2)^2 + 1^2 = 1^2 + (-2)^2 = (-2)^2 + (-1)^2 = (-1)^2 + 2^2 = 2^2 + (-1)^2 = (-1)^2 + (-2)^2,$$

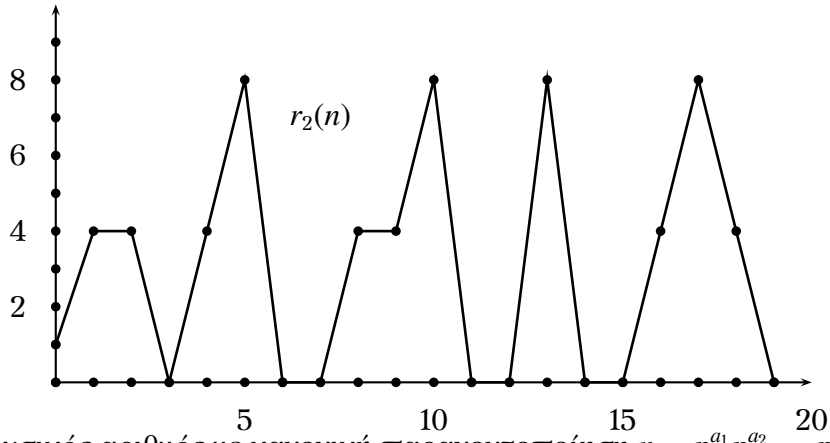
ο αριθμός 9 εκφράζεται ως άθροισμα δύο τετραγώνων με τέσσερις διαφορετικούς τρόπους

$$9 = 3^2 + 0^2 = 0^2 + 3^2 = (-3)^2 + 0^2 = 0^2 + (-3)^2$$

ενώ ο αριθμός 3 δεν είναι δυνατόν να εκφραστεί ως άθροισμα δύο τετραγώνων, οπότε $r_2(5) = 8$, $r_2(9) = 4$ και $r_2(3) = 0$.

Οι τιμές της $r_2(n)$ για κάθε n μικρότερο ή ίσο του 19 δίνονται στον επόμενο πίνακα:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$r_2(n)$	4	4	0	4	8	0	0	4	4	8	0	0	8	0	0	4	8	4	0



Έστω n ένας φυσικός αριθμός με κανονική παραγοντοποίηση $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, όπου $p_1, p_2, \ldots, p_k$ είναι πρώτοι αριθμοί και $a_1, a_2, \ldots, a_k$ είναι φυσικοί αριθμοί. Αποδεικνύεται ότι ο n εκφράζεται ως άθροισμα δύο τετραγώνων αν και μόνο αν για κάθε περιττό a_i, $i \in [k]$ ισχύει ότι $p_i \not\equiv 3 \pmod 4$.

Για παράδειγμα, ο αριθμός $129 = 2 \cdot 3^2 \cdot 7$ δεν εκφράζεται ως άθροισμα δύο τετραγώνων διότι $2 \equiv 2 \pmod 4$ αλλά $7 \equiv 3 \pmod 4$.

Ο αριθμός $242 = 2 \cdot 11^2$ εκφράζεται ως άθροισμα δύο τετραγώνων, διότι $2 \equiv 2 \pmod 4$. Πράγματι,

$$242 = 2 \cdot 11^2 = (1^2 + 1^2)(11^2 + 0^2) = 11^2 + 11^2.$$

Ο αριθμός $65 = 5 \cdot 13$ εκφράζεται ως άθροισμα δύο τετραγώνων, διότι $5 \equiv 1 \pmod 4$ και $13 \equiv 1 \pmod 4$. Πράγματι,

$$\begin{aligned} 65 &= 5 \cdot 13 \\ &= (2^2 + 1^2)(3^2 + 2^2) \\ &\overset{9}{=} (2 \cdot 3 + 1 \cdot 2)^2 + (2 \cdot 2 - 1 \cdot 3)^2 \\ &= 8^2 + 1^2. \end{aligned}$$

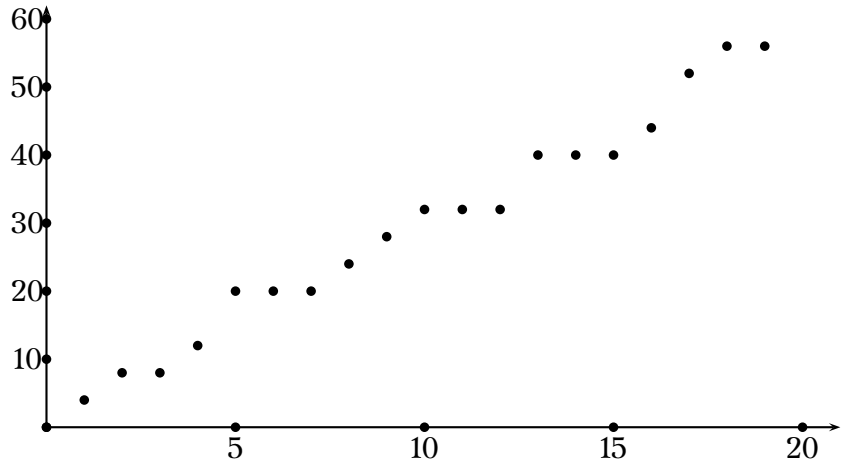
[9] Χρησιμοποιούμε την ταυτότητα $(x^2 + y^2)(v^2 + w^2) = (xv + yw)^2 + (xw - yv)^2$.

Η συνάρτηση $r_2(n)$, όπως και οι περισσότερες αριθμητικές συναρτήσεις, για μεμονωμένες τιμές, συμπεριφέρεται χαοτικά. Εν τούτοις, η συνάρτηση των μερικών αθροισμάτων των τιμών της $r_2(n)$, δηλαδή η συνάρτηση

$$\sum_{k=0}^{n} r_2(k)$$

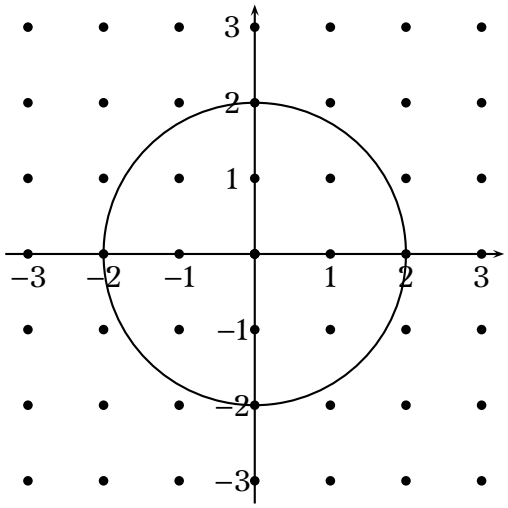
καθώς το n αυξάνει προσεγγίζεται από μια ευθεία.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$r_2(n)$	4	4	0	4	8	0	0	4	4	8	0	0	8	0	0	4	8	4	0
$\sum_{k=0}^{n} r_2(k)$	4	8	8	12	20	20	20	24	28	32	32	32	40	40	40	44	52	56	56



Στη συνέχεια θα υπολογίσουμε μια εκτίμηση της συνάρτησης των μερικών αθροισμάτων της $r_2(n)$.

Έστω $C(n)$ το σύνολο όλων των σημείων του επιπέδου με ακέραιες συντεταγμένες τα οποία βρίσκονται στο εσωτερικό ή στην περιφέρεια του κύκλου $x^2 + y^2 = n$.



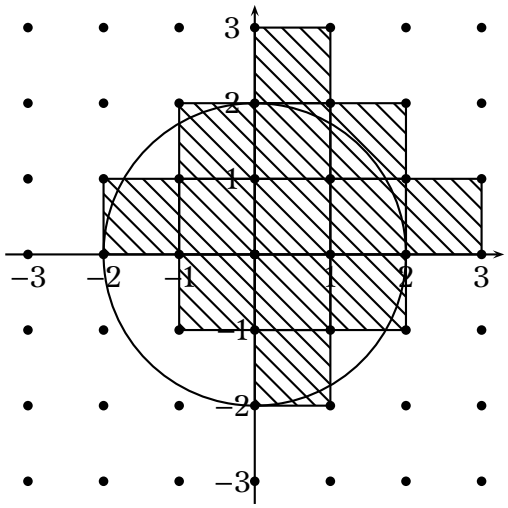
Το $r_2(n)$ ισούται με τον αριθμό των σημείων με ακέραιες συντεταγμένες τα οποία βρίσκονται στην περιφέρεια του κύκλου $x^2 + y^2 = n$.

Επειδή κάθε κύκλος με εξίσωση $x^2 + y^2 = k$, όπου $k \leq n$ περιέχεται στον κύκλο $x^2 + y^2 = n$, προκύπτει ότι

$$\sum_{k=0}^{n} r_2(k) = |C(n)|,$$

δηλαδή το $\sum_{k=0}^{n} r_2(k)$ ισούται με το πλήθος των σημείων με ακέραιες συντεταγμένες τα οποία περιέχονται στον κύκλο $x^2 + y^2 = n$.

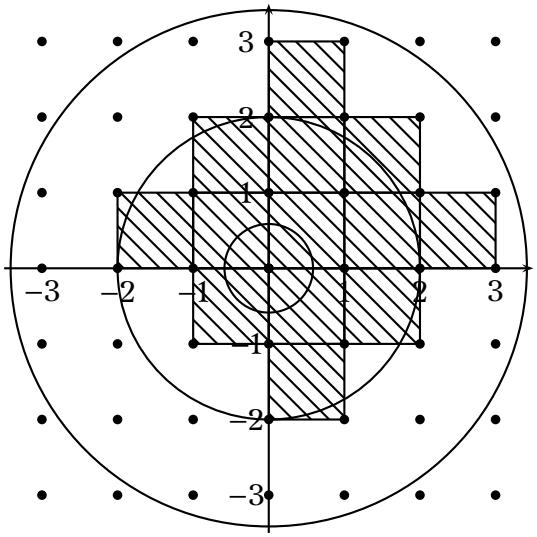
Κάθε σημείο (a, b) του $C(n)$ μπορεί να θεωρηθεί ως αριστερή κάτω γωνία ενός τετραγώνου με μοναδιαίο μήκος, έτσι ώστε σε κάθε σημείο του $C(n)$ να αντιστοιχεί ακριβώς ένα μοναδιαίο τετράγωνο.



Παρατηρούμε, ότι ο αριθμός των σημείων του $C(n)$ ισούται με το συνολικό εμβαδό όλων αυτών των τετραγώνων και άρα ισούται με $\sum_{k=0}^{n} r_2(k)$.

Επειδή, η διαγώνιος αυτών των τετραγώνων έχει μήκος $\sqrt{1^2 + 1^2} = \sqrt{2}$, προκύπτει ότι κάθε σημείο αυτών των τετραγώνων περιέχεται στο εσωτερικό ή στην περιφέρεια του κύκλου με εξίσωση $x^2 + y^2 = (\sqrt{n} + \sqrt{2})^2$.

Επίσης, κάθε σημείο του κύκλου με εξίσωση $x^2 + y^2 = (\sqrt{n} - \sqrt{2})^2$ περιέχεται σε κάποιο από αυτά τα τετράγωνα.



Επομένως, το εμβαδόν αυτών των τετραγώνων, και άρα και το άθροισμα $\sum_{k=0}^{n} r_2(n)$ φράσσεται από τα εμβαδά των δύο κύκλων, δηλαδή ισχύει ότι

$$\pi(\sqrt{(n)} - \sqrt{2})^2 < \sum_{k=0}^{n} r_2(k) < \pi(\sqrt{n} + \sqrt{2})^2.$$

Ισοδύναμα, προκύπτει ότι

$$\pi(1-\frac{\sqrt{2}}{\sqrt{n}})^2 < \frac{1}{n}\sum_{k=0}^{n} r_2(k) < \pi(1+\frac{\sqrt{2}}{\sqrt{n}})^2.$$

Αν το n τείνει στο άπειρο, τότε χρησιμοποιώντας την προηγούμενη ανισότητα, προκύπτει ότι

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=0}^{n} r_2(k) = \pi,$$

δηλαδή, η μέση τιμή της συνάρτησης $r_2(n)$ καθώς το n τείνει στο άπειρο ισούται με π.

Κεφάλαιο 6

Στοιχεία μαθηματικής λογικής

Το μεγαλύτερο μέρος των σημειώσεων αυτού του κεφαλαίου βασίζεται σε υλικό του βιβλίου
"Στοιχεία Μαθηματικής Λογικής"
Αθ. Τζουβάρα
Εκδόσεις ΖΗΤΗ, Θεσσαλονίκη

6.1 Εισαγωγή

Αριστοτέλης: "Σχήματα" συλλογισμών

Π.χ.: Όλοι οι άνθρωποι είναι θνητοί.
Ο Σωκράτης είναι άνθρωπος.
᾽ρα ο Σωκράτης είναι θνητός.

Η αλήθεια του παραπάνω συλλογισμού δεν εξαρτάται από το υποκείμενο (Σωκράτης), ή από το κατηγόρημα (θνητός). Γενικά, το "σχήμα" αυτό είναι σωστό:

Κάθε Μ είναι Κ
Το Υ είναι Μ
᾽ρα το Υ είναι Κ

ή σε γραφή που "ταιριάζει" με τη Λογική:

Αν p τότε q
p
᾽ρα q

Αριστοτέλειες αρχές (αξιώματα)

1. **Αρχή της ταυτότητας**: Κάθε πράγμα ταυτίζεται με τον εαυτό του.

2. **Αρχή της απόκλεισης του τρίτου ενδεχόμενου**: Κάθε πράγμα ή έχει την ιδιότητα Α, ή δεν την έχει. Δεν υπάρχει τρίτη δυνατότητα.

Τα παραπάνω αποτελούν την αφετηρία της **δίτιμης** μαθηματικής λογικής.

Στη σύγχρονη εποχή αναπτύσσεται πάντως και η **πλειονότιμη** (ασαφής) λογική (με εφαρμογές και στη Φυσική, την Κοινωνιολογία, τα Δυναμικά Συστήματα - Θεωρία του Χάους κ.λπ.).

Στα Μαθηματικά, οι βασικές αρχές παραμένουν σταθερές - εκφράζονται ικανοποιητικά από την Αριστοτέλεια Λογική.

Leibniz, Boole (μέσα 19ου αιώνα).
Peano, Russel - Θεωρία συνόλων (τέλη 19ου αιώνα, αρχές 20ου αιώνα).
Hilbert, Godel - Σύγχρονη Μαθηματική Λογική (20ος αιώνας).

Μαθηματική (ή συμβολική) Λογική

Χρησιμοποιεί μαθηματικές μεθόδους. Είναι μέρος των Μαθηματικών: Θεωρία συνόλων, μοντέλων, αποδείξεων, αναδρομής κ.λπ.

Γλώσσα της Μαθηματικής Λογικής

Ένα καθορισμένο σύνολο συμβόλων.

Μεταγλώσσα

Η κοινή (π.χ. η ελληνική) γλώσσα και κάποια σύμβολα (σαφώς διαφορετικά από εκείνα της γλώσσας της λογικής).

Μελέτη προτάσεων

Πρώτο (στοιχειώδες) επίπεδο: **Προτασιακός λογισμός (Propositional calculus)**.

Δεύτερο (πιο πολύπλοκο) επίπεδο: **Κατηγορικός (ή κατηγορηματικός) λογισμός (Predicate calculus)**. Αυτός προσφέρει μεγαλύτερες δυνατότητες έκφρασης και συμπερασματολογίας.

Για παράδειγμα, στον προτασιακό λογισμό:

p : Υπάρχουν άπειροι πρώτοι αριθμοί,
q : Υπάρχει πρώτος αριθμός μεγαλύτερος του 10^{10}.

Στον κατηγορικό λογισμό:

$$p: \quad (\forall x)(\exists y)(y > x \wedge \Pi(y)),$$
$$q: \quad (\exists y)(y > 10^{10} \wedge \Pi(y)).$$

Σημασιολογικές έννοιες

Έχουν σχέση με τη "σημασία" (αλήθεια ή ψεύδος) των προτάσεων.

Συντακτικές έννοιες

Έχουν σχέση με τη "σύνταξη" (τη συμβολική γραφή) των προτάσεων, το μηχανικό τρόπο παραγωγής προτάσεων από άλλες (αξίωμα, απόδειξη, κανόνες παραγωγής κ.λπ.).

Υπάρχει αντιστοιχία μεταξύ των παραπάνω δύο εννοιών. Κατά συνέπεια, υπάρχουν δύο τρόποι αντιμετώπισης των προβλημάτων: **Θεωρία μοντέλων - Θεωρία αποδείξεων**.

6.2 Γλώσσα του προτασιακού λογισμού

Στον προφορικό και στο γραπτό λόγο σχηματίζουμε (χρησιμοποιώντας λέξεις, και με βάση κανόνες του συντακτικού) γλωσσικές οντότητες με αυτοτελές νόημα, τις φράσεις.

Π.χ.: Σου εύχομαι χρόνια πολλά. (Ευχή)
Πόσων χρόνων είσαι; (Ερώτηση)
Είμαι 55 χρόνων. (Διαπίστωση) κ.λπ

Η λογική ασχολείται μόνο με αποφαντικές φράσεις (δηλαδή φράσεις που εκφράζουν διαπιστώσεις), οι οποίες λέγονται προτάσεις.

Π.χ.: Ο αριθμός 10 είναι άρτιος.
Ο Α είναι συμφοιτητής του Β.
$2 + 5 = 7$.
$4 + 4 = 10$.

Οι προτάσεις δέχονται **τιμή αληθείας** (αληθής, ψευδής).

Προσπαθούμε να βρούμε ένα ελάχιστο σύνολο προτάσεων (από τις οποίες μπορούμε να συνθέσουμε τις υπόλοιπες), καθώς επίσης και τους βασικούς κανόνες σύνθεσης. Υπάρχουν λοιπόν κάποιες προτάσεις που δεν μπορούν να διασπαστούν σε απλούστερες υποπροτάσεις. Αυτές λέγονται **απλές προτάσεις** (ή **ατομικές προτάσεις**, ή **άτομα**).

Π.χ.: Ο αριθμός 7 είναι πρώτος.
Κάθε φοιτητής ξέρει σκάκι.
Η κόρη μου είναι μεγαλύτερη από το γιό μου.

Αντίθετα, η πρόταση

Αν ο x είναι άρτιος, τότε ο $x + 3$ είναι περιττός

αναλύεται σε (απλές) υποπροτάσεις. Άρα, δεν είναι άτομο αλλά **σύνθετη πρόταση**.

Χρησιμοποιούμε τους εξής συνδέσμους για να συνθέσουμε μια πρόταση (χρησιμοποιώντας άτομα):

και, ή, όχι, αν ... τότε, αν και μόνο αν.

Για να "τυποποιήσουμε" λοιπόν τη λογική των προτάσεων, αρκεί να εισάγουμε σύμβολα

1. για τις απλές προτάσεις,
2. για τους παραπάνω συνδέσμους.

Τα σύμβολα αυτά (και μερικά άλλα, βοηθητικά) αποτελούν μια Τυπική Γλώσσα (formal language) του Προτασιακού Λογισμού (σε αντίθεση με τις φυσικές γλώσσες).

Ορισμός. *Μια **τυπική γλώσσα** L **του Προτασιακού Λογισμού** αποτελείται από:*

1. *Τα σύμβολα των ατόμων: $p_1, p_2, p_3, \ldots$ (αριθμήσιμα σε πλήθος).*
2. *Τα σύμβολα των συνδέσμων:*

$\wedge$:	*και*	*(σύζευξη)*
$\vee$:	*ή*	*(διάζευξη)*
$\neg$:	*όχι*	*(άρνηση)*
$\rightarrow$:	*αν ... τότε*	*(συνεπαγωγή)*
$\leftrightarrow$:	*αν και μόνο αν*	*(ισοδυναμία)*

3. *Τις παρενθέσεις: (,).*

Έκφραση λέγεται κάθε πεπερασμένη ακολουθία συμβόλων της L.

Π.χ.: $(p_1 \wedge p_5)\neg(p_1 \wedge p_2)$
$\neg(p_1 \wedge p_2) \leftrightarrow (\neg p_1 \vee \neg p_2)$
$p_1(p_2(p_3(p_4)))$

Προτάσεις της L είναι εκφράσεις που κατασκευάζονται βάσει κάποιων συγκεκριμένων κανόνων (**κανόνες σχηματισμού**) που δίδονται στον επόμενο ορισμό:

Ορισμός.

1. *Τα $p_i, i \in \mathbb{N}^*$, είναι προτάσεις.*
2. *Αν οι φ, y είναι προτάσεις, τότε και οι εκφράσεις*

$$(\varphi) \wedge (y), \quad (\varphi) \vee (y), \quad (\varphi) \rightarrow (y), \quad (\varphi) \leftrightarrow (y), \quad \neg(\varphi)$$

είναι προτάσεις.

3. *Δεν υπάρχουν άλλες προτάσεις.*

Συμβολισμοί
$\mathbf{P}_0 = \{p_1, p_2, p_3, \ldots\}$ (δηλαδή το σύνολο των ατόμων της L).
$\mathbf{P}$: το σύνολο όλων των προτάσεων της L.

Η σημασία των παρενθέσεων

Οι προτάσεις $(p_1 \vee p_2) \wedge p_3$ και $p_1 \vee (p_2 \wedge p_3)$ είναι διαφορετικές.

Π.χ.: p_1 : Το 2 είναι άρτιος.
p_2 : Το 2 είναι περιττός.
p_3 : Το 2 είναι αρνητικός.

Τότε, η πρόταση $(p_1 \vee p_2) \wedge p_3$ είναι ψευδής, ενώ η πρόταση $p_1 \vee (p_2 \wedge p_3)$ είναι αληθής.

Προτεραιότητα συνδέσμων

1. Ο $\neg$ έχει προτεραιότητα εφαρμογής έναντι όλων των άλλων συνδέσμων.
2. Οι $\wedge, \vee$ έχουν προτεραιότητα εφαρμογής έναντι των $\rightarrow, \leftrightarrow$.
3. Οι $\wedge, \vee$ έχουν ίση προτεραιότητα μεταξύ τους.

4. Οι $\rightarrow, \leftrightarrow$ έχουν ίση προτεραιότητα μεταξύ τους.

Έτσι, για παράδειγμα, γράφουμε:

1. $\neg\varphi \vee y$ αντί για $(\neg\varphi) \vee y$,

2. $\varphi \rightarrow \psi \wedge \sigma$ αντί για $\varphi \rightarrow (\psi \wedge \sigma)$,

3. $\neg\neg p_1 \rightarrow (p_2 \wedge p_3 \leftrightarrow p_4 \vee p_5)$ αντί για $(\neg(\neg p_1)) \rightarrow ((p_2 \wedge p_3) \leftrightarrow (p_4 \vee p_5))$.

Παρατήρηση. Η προτεραιότητα των συνδέσμων μειώνει τις παρενθέσεις, αλλά φυσικά δεν τις απαλείφει πάντοτε όλες. Έτσι, το (μοναδικό) ζεύγος παρενθέσεων στην πρώτη γραφή της πρότασης του τελευταίου παραδείγματος δεν μπορούμε να το παραλείψουμε, αφού δεν μπορούμε να διακρίνουμε αν η έκφραση

$$\neg\neg p_1 \rightarrow p_2 \wedge p_3 \leftrightarrow p_4 \vee p_5$$

είναι η πρόταση

$$(\neg\neg p_1 \rightarrow p_2 \wedge p_3) \leftrightarrow p_4 \vee p_5$$

ή, η πρόταση

$$\neg\neg p_1 \rightarrow (p_2 \wedge p_3 \leftrightarrow p_4 \vee p_5).$$

Ομοίως, δεν μπορούμε να παραλείψουμε τις παρενθέσεις της πρότασης $(p_1 \vee p_2) \wedge p_3$, αφού η $p_1 \vee p_2 \wedge p_3$ δεν είναι σαφές αν είναι η $(p_1 \vee p_2) \wedge p_3$, ή η $p_1 \vee (p_2 \wedge p_3)$.

Η προτεραιότητα εφαρμογής των συνδέσμων επεκτείνεται από ορισμένους συγγραφείς, οι οποίοι απλά θεωρούν την εξής προτεραιότητα:

$$\neg, \quad \wedge, \quad \vee, \quad \rightarrow, \quad \leftrightarrow .$$

Έτσι, η πρόταση

$$((p_1 \wedge p_2) \rightarrow p_3) \leftrightarrow ((\neg p_1) \rightarrow (p_2 \vee (p_3 \wedge p_4)))$$

που σύμφωνα με την αρχική προτεραιότητα γράφεται

$$(p_1 \wedge p_2 \rightarrow p_3) \leftrightarrow (\neg p_1 \rightarrow p_2 \vee (p_3 \wedge p_4)),$$

μπορεί επίσης να γραφεί (εφαρμόζοντας την επέκταση της προτεραιότητας)

$$p_1 \wedge p_2 \rightarrow p_3 \leftrightarrow \neg p_1 \rightarrow p_2 \vee p_3 \wedge p_4.$$

Και πάλι πάντως, δεν μπορούμε να απαλείψουμε πάντοτε τις παρενθέσεις. Για παράδειγμα, δεν μπορούμε να απαλείψουμε την παρένθεση της πρότασης $\neg(\varphi \wedge y)$ αφού η πρόταση $\neg\varphi \wedge y$ είναι η $(\neg\varphi) \wedge y$.

Στα παρακάτω, θα εφαρμόσουμε την αρχική προτεραιότητα και όχι την επέκτασή της.

Ονομάζουμε **προτασιακές μεταβλητές** τα σύμβολα $\varphi, \psi, \sigma, y, w, z, \ldots$ με τα οποία συμβολίζουμε, χάριν απλούστευσης και συντομίας, τυχαίες προτάσεις. Τονίζουμε πάντως ότι τα σύμβολα αυτά *δεν είναι* στοιχεία της τυπικής γλώσσας L. Μπορούμε να χρησιμοποιούμε προτασιακές μεταβλητές $p, q, \ldots$ (αντί για $p_1, p_2, \ldots$) και για τα άτομα.

Οι σύνδεσμοι μπορούν να θεωρηθούν ως (εσωτερικές) πράξεις στο σύνολο E των εκφράσεων της L: Οι σύνδεσμοι $\wedge, \vee, \rightarrow, \leftrightarrow$ θεωρούνται διμελείς πράξεις, ενώ ο $\neg$ μονομελής.

Πράγματι, για κάθε ζεύγος $(\varphi, y) \in E \times E$, οι εκφράσεις

$$\varphi \wedge y, \quad \varphi \vee y, \quad \varphi \rightarrow y, \quad \varphi \leftrightarrow y, \quad \neg\varphi$$

είναι εκφράσεις του E. Μπορούμε λοιπόν να θεωρήσουμε ότι το P είναι το **ελάχιστο** σύνολο που περιέχει το P_0 και είναι κλειστό ως προς τις πράξεις $\wedge, \vee, \rightarrow, \leftrightarrow, \neg$.

Έλεγχος για προτάσεις

1. Αν η έκφραση ε δεν έχει μια από τις μορφές: $p_i, \varphi_1 \wedge \varphi_2, \varphi_1 \vee \varphi_2, \varphi_1 \to \varphi_2, \varphi_1 \leftrightarrow \varphi_2, \neg\varphi$, τότε δεν είναι πρόταση.

2. Αν έχει μια από τις παραπάνω μορφές, ελέγχουμε ομοίως τις $\varphi_1, \varphi_2, \varphi$.

Παράδειγμα. Οι εκφράσεις

$$\neg p_1 \vee p_2, \quad (p_1 \to p_2) \vee (p_3 \wedge (p_4 \to p_5))$$

είναι προτάσεις, ενώ οι εκφράσεις

$$(p_1 \wedge p_2) \to (p_3 \neg p_4), \quad p_2 \wedge (\to (p_1 \wedge p_1))$$

δεν είναι προτάσεις.

Αντιστοιχία κατασκευής

Σύνολο $\mathbb{N}$ (φυσικοί αριθμοί)	Σύνολο P (προτάσεις της L)
$0 \in \mathbb{N}$	$p_1, p_2, p_3, \ldots \in P$
$n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$	$\varphi, y \in P \Rightarrow \begin{cases} \varphi \wedge y \in P \\ \varphi \vee y \in P \\ \varphi \to y \in P \\ \varphi \leftrightarrow y \in P \\ \neg\varphi \in P \end{cases}$

Παρατήρηση. Συχνά θα χρησιμοποιούμε το σύμβολο $\square$, θεωρώντας ότι συμβολίζει οποιονδήποτε από τους (διμελείς) συνδέσμους $\wedge, \vee, \to, \leftrightarrow$.

Έτσι, αντί για $\begin{cases} \varphi \wedge y \in P \\ \varphi \vee y \in P \\ \varphi \to y \in P \\ \varphi \leftrightarrow y \in P \\ \neg\varphi \in P \end{cases}$ μπορούμε να γράψουμε απλούστερα $\begin{cases} \varphi \square y \in P \\ \neg\varphi \in P \end{cases}$.

Επαγωγική απόδειξη στο $\mathbb{N}^*$ (μέθοδος της επαγωγής)

Αν για την πρόταση $A(n)$ ισχύουν:

1. $A(1)$: αληθής
2. $A(n) \Rightarrow A(n+1)$,

τότε η $A(n)$ ισχύει για κάθε $n \in \mathbb{N}^*$.

Επαγωγικός (αναδρομικός) ορισμός στο $\mathbb{N}^*$

Θέλουμε να ορίσουμε το $f(n)$, για κάθε $n \in \mathbb{N}^*$ (δηλαδή θέλουμε να ορίσουμε μια συνάρτηση (ακολουθία) $f : \mathbb{N}^* \to V$, όπου V ένα τυχαίο σύνολο). Αρκεί:

1. Να ορίσουμε την $f(1)$, και
2. Να διαθέτουμε έναν κανόνα που να μας δίνει την τιμή $f(n+1)$ συναρτήσει της $f(n)$.

Πιο αυστηρά, αν $a \in V$ και $G : V \to V$ τότε υπάρχει μοναδική συνάρτηση $f : \mathbb{N}^* \to V$ με $f(1) = a$ και $f(n+1) = G(f(n))$.

Παράδειγμα

Αν θέλουμε να ορίσουμε επαγωγικά τη συνάρτηση (ακολουθία)

$$f(n) = 3^n, \quad n \in \mathbb{N}^*,$$

θεωρούμε $V = \mathbb{N}^*$, $a = 3 \in \mathbb{N}^*$ και $G : \mathbb{N}^* \to \mathbb{N}^*$ με $G(u) = 3u$, για κάθε $u \in \mathbb{N}^*$, οπότε ορίζεται η συνάρτηση

$$f : \mathbb{N}^* \to \mathbb{N}^* \text{ με } f(1) = 3 \text{ και } f(n+1) = G(f(n)) = 3f(n),$$

δίνοντας $f(1) = 3$, $f(2) = 3f(1) = 3 \cdot 3 = 3^2$, $f(3) = 3f(2) = 3 \cdot 3^2 = 3^3$, κλπ., που δεν είναι άλλη από την ακολουθία $f(n) = 3^n$.

Πρόταση 6.1 (Αρχή της επαγωγικής απόδειξης στο P). *Έστω $A(\varphi)$ μια ιδιότητα της μεταγλώσσας, η οποία αφορά προτάσεις της τυπικής γλώσσας L. Αν ισχύουν οι παρακάτω τρεις προτάσεις:*

i) Η $A(p)$ ισχύει για κάθε $p \in P_0$,

ii) Αν για δύο προτάσεις $\varphi, y \in P$ ισχύουν οι $A(\varphi), A(y)$ τότε ισχύει και η $A(\varphi \square y)$,

iii) Αν για μια πρόταση $\varphi \in P$ ισχύει η $A(\varphi)$ τότε ισχύει και η $A(\neg\varphi)$,

τότε η $A(\varphi)$ ισχύει για κάθε $\varphi \in P$.

Απόδειξη. Έστω $\Sigma = \{\varphi \in P : A(\varphi)\} \subseteq P$. Από τις $i), ii), iii)$ έπεται ότι το Σ περιέχει όλα τα άτομα και είναι κλειστό ως προς τις $\square$ και $\neg$. Αλλά γνωρίζουμε ότι το P είναι το *ελάχιστο* τέτοιο σύνολο. Άρα $P \subseteq \Sigma$. Αφού λοιπόν $\Sigma \subseteq P$ και $P \subseteq \Sigma$, συνεπάγεται ότι $\Sigma = P$. Ώστε για κάθε $\varphi \in P$ ισχύει ότι $\varphi \in \Sigma$, δηλαδή για κάθε $\varphi \in P$ ισχύει η $A(\varphi)$. $\square$

Παράδειγμα 6.2.1. *Έστω $\alpha(\varphi)$ ο αριθμός των θέσεων της φ όπου εμφανίζεται άτομο και $\beta(\varphi)$ ο αριθμός των θέσεων όπου εμφανίζεται διμελής σύνδεσμος. Να δειχθεί ότι $\alpha(\varphi) = \beta(\varphi) + 1$.*

Λύση. Πράγματι, έστω $A(\phi)$ η ιδιότητα $\alpha(\varphi) = \beta(\varphi) + 1$.

i) Αν η ϕ είναι άτομο, τότε $\alpha(\phi) = 1 = 0 + 1 = \beta(\phi) + 1$.

ii) Αν για τις $\phi, \psi \in P$ ισχύουν οι $A(\phi)$, $A(\psi)$, δηλαδή αν $\alpha(\phi) = \beta(\phi) + 1$ και $\alpha(\psi) = \beta(\psi) + 1$, τότε

$$\begin{aligned}\alpha(\phi \square \psi) &= \alpha(\phi) + \alpha(\psi)\\ &= (\beta(\phi) + 1) + (\beta(\psi) + 1)\\ &= (\beta(\phi) + \beta(\psi) + 1) + 1\\ &= \beta(\phi \square \psi) + 1.\end{aligned}$$

iii) Αν για την ϕ ισχύει η $A(\phi)$, δηλαδή $\alpha(\phi) = \beta(\phi) + 1$, τότε $\alpha(\neg\phi) = \alpha(\phi) = \beta(\phi) + 1 = \beta(\neg\phi) + 1$. □

Δίνουμε επίσης μια διαδικασία για τον επαγωγικό ορισμό στο P.

Πρόταση 6.2 (Αρχή του επαγωγικού ορισμού στο P). *Έστω V τυχόν σύνολο και $f : P_0 \to V$ τυχούσα συνάρτηση. Αν για κάθε $\square$ και για τον $\neg$ υπάρχουν συναρτήσεις $G_\square : V \times V \to V$, $G_\neg : V \to V$ αντίστοιχα, τότε υπάρχει μοναδική συνάρτηση $\bar{f} : P \to V$ με*

i) $\bar{f}(p_i) = f(p_i)$, για κάθε $p_i \in P_0$,

ii) $\bar{f}(\varphi \square y) = G_\square(\bar{f}(\varphi), \bar{f}(y))$,

iii) $\bar{f}(\neg\varphi) = G_\neg(\bar{f}(\varphi))$.

Δηλαδή, για να ορίσουμε στο P μια "έννοια", δηλαδή για να αντιστοιχίσουμε σε κάθε πρόταση του P μια ιδιότητα (ένα "χαρακτηριστικό" της, ένα στοιχείο του V) αρκεί να αντιστοιχίσουμε σε κάθε άτομο την έννοια αυτή και να έχουμε "κανόνες" (τους $G_\square, G_\neg$) που να καθορίζουν το "πέρασμα" της έννοιας στις αμέσως συνθετότερες προτάσεις $\varphi \square y$ και $\neg\varphi$.

Απόδειξη. Έστω μια g η οποία ικανοποιεί τις *i*), *ii*), *iii*). Η g είναι προφανώς συνάρτηση με τιμές στο V (αφού οι $f, G_\square, G_\neg$ είναι συναρτήσεις με τιμές στο V). Θα δείξουμε ότι

α) $P \subseteq \mathrm{dom}(g)$, και

β) ότι η g είναι μοναδική στο P,

(άρα ο περιορισμός της g στο P είναι η ζητούμενη $\bar{f}$).

Για το α) έχουμε:

Η *i*) συνεπάγεται ότι $P_0 \subseteq \mathrm{dom}(g)$, δηλαδή $p_i \in \mathrm{dom}(g)$, για κάθε $i = 1, 2, \ldots$,

Η *ii*) συνεπάγεται ότι αν $\varphi, y \in \mathrm{dom}(g)$ τότε $\varphi \square y \in \mathrm{dom}(g)$,

Η *iii*) συνεπάγεται ότι αν $\varphi \in \mathrm{dom}(g)$ τότε $\neg\varphi \in \mathrm{dom}(g)$.

Άρα (με χρήση της αρχής επαγωγικής απόδειξης) $P \subseteq \mathrm{dom}(g)$. Ώστε, πράγματι η g ορίζεται σε ολόκληρο το P.

Για το β) θεωρούμε g_1, g_2 δύο τέτοιες συναρτήσεις και

$$B = \{\varphi \in P : g_1(\varphi) = g_2(\varphi)\} \subseteq P.$$

Η *i*) συνεπάγεται ότι για κάθε $p \in P_0$ έχουμε $g_1(p) = f(p) = g_2(p)$, άρα $p \in B$.
Η *ii*) συνεπάγεται ότι αν $\varphi, y \in B$ τότε $\varphi \square y \in B$. Πράγματι, $g_1(\varphi) = g_2(\varphi)$ και $g_1(y) = g_2(y)$. Άρα

$$g_1(\varphi \square y) = G_\square(g_1(\varphi), g_1(y)) = G_\square(g_2(\varphi), g_2(y)) = g_2(\varphi \square y).$$

Η *iii*) συνεπάγεται ότι αν $\varphi \in B$ τότε $\neg\varphi \in B$. Πράγματι, $g_1(\varphi) = g_2(\varphi)$. Άρα

$$g_1(\neg\varphi) = G_\neg(g_1(\varphi)) = G_\neg(g_2(\varphi)) = g_2(\neg\varphi).$$

Άρα (και πάλι λόγω της αρχής της επαγωγικής απόδειξης) για κάθε $\varphi \in P$ ισχύει ότι $\varphi \in B$. Άρα $P \subseteq B$ και συνεπώς (αφού και $B \subseteq P$) έχουμε $B = P$. Επομένως, $g_1(\varphi) = g_2(\varphi)$, για κάθε $\varphi \in P$, δηλαδή η g είναι μοναδική στο P. □

Παραδείγματα επαγωγικού ορισμού

1. Ορισμός. Η **τάξη** (rank) της φ, $r(\varphi)$ είναι ένας φυσικός αριθμός με:
i) $r(p_i) = 0$, για κάθε $p_i \in P_0$,
ii) $r(\varphi \square y) = \max\{r(\varphi), r(y)\} + 1$,
iii) $r(\neg\varphi) = r(\varphi) + 1$.

Παρατήρηση. Στον επαγωγικό αυτό ορισμό έχουμε:

$$\begin{cases} V = \mathbb{N}, \\ f : P_0 \to \mathbb{N}, \text{ με } f(p_i) = 0, \text{ για κάθε } p_i \in P_0, \\ \bar{f} \text{ είναι η } r : P \to \mathbb{N}, \\ G_\square : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \text{ με } G_\square(m, n) = \max\{m, n\} + 1, \\ G_\neg : \mathbb{N} \to \mathbb{N}, \text{ με } G_\neg(n) = n + 1. \end{cases}$$

Το $r(\varphi)$ είναι προφανώς ένα μέτρο πολυπλοκότητας της φ. Όσο πιο μεγάλο είναι το $r(\varphi)$ τόσο πιο "πολύπλοκη" είναι η φ.

Παραδείγματα

1. Για τη $\varphi = p_1 \vee (p_2 \wedge p_3)$ είναι $r(\varphi) = 2$.
2. Για τη $\varphi = (p_1 \to p_2) \vee (p_1 \wedge p_2 \leftrightarrow \neg p_3)$ είναι $r(\varphi) = 3$.

Ένα άλλο μέτρο πολυπλοκότητας της φ δίδεται από το σύνολο των υποπροτάσεών της.

2. Ορισμός. Το σύνολο **sub(φ)** των υποπροτάσεων της φ ορίζεται ως εξής:

i) $\text{sub}(p_i) = \{p_i\}$, για κάθε $p_i \in P_0$,

ii) $\text{sub}(\varphi \square y) = \text{sub}(\varphi) \cup \text{sub}(y) \cup \{\varphi \square y\}$,

iii) $\text{sub}(\neg\varphi) = \text{sub}(\varphi) \cup \{\neg\varphi\}$.

Παραδείγματα

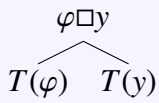
1. $\text{sub}(p_1 \to p_2) = \text{sub}(p_1) \cup \text{sub}(p_2) \cup \{p_1 \to p_2\}$
$= \{p_1\} \cup \{p_2\} \cup \{p_1 \to p_2\}$
$= \{p_1, p_2, p_1 \to p_2\}.$

2. $\text{sub}(\neg p_1 \vee p_2 \to p_3 \wedge p_4) = \text{sub}(\neg p_1 \vee p_2) \cup \text{sub}(p_3 \wedge p_4)) \cup \{\neg p_1 \vee p_2 \to p_3 \wedge p_4\}$
$= \text{sub}(\neg p_1) \cup \text{sub}(p_2) \cup \{\neg p_1 \vee p_2\} \cup \text{sub}(p_3) \cup \text{sub}(p_4)$
$\cup \{p_3 \wedge p_4\} \cup \{\neg p_1 \vee p_2 \to p_3 \wedge p_4\}$
$= \{p_1, \neg p_1, p_2, \neg p_1 \vee p_2, p_3, p_4, p_3 \wedge p_4, \neg p_1 \vee p_2 \to p_3 \wedge p_4\}.$

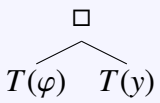
3. Ορισμός. Το **δένδρο ανάλυσης $T(\varphi)$** το οποίο δίνει μια σχηματική παράσταση της δομής της πρότασης φ, ορίζεται ως εξής:

i) Το $T(p_i)$ είναι το σημείο (κόμβος) $\cdot\ p_i$,

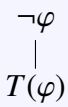
ii) Το $T(\varphi \square y)$ είναι το διάγραμμα



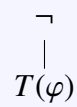
ή (απλούστερα)



iii) Το $T(\neg\varphi)$ είναι το διάγραμμα

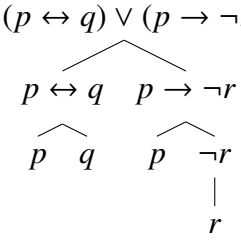


ή (απλούστερα)

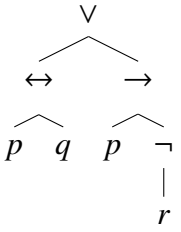


Παραδείγματα

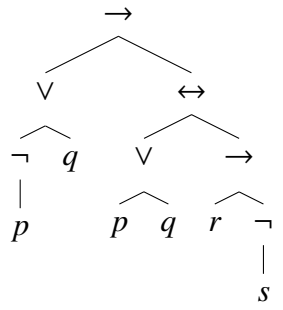
1. Το $T(\varphi)$ για τη $\varphi = (p \leftrightarrow q) \vee (p \to \neg r)$ είναι το:



ή, σε απλούστερη γραφή:



2. Το $T(\varphi)$ για τη $\varphi = \neg p \vee q \to (p \vee q \leftrightarrow (r \to \neg s))$ είναι το:



6.2.1 Λυμένες ασκήσεις

Άσκηση 6.1. *Να δειχθεί ότι η έκφραση:* $((p \wedge q) \rightarrow) \wedge r$ *δεν είναι πρόταση.*

Λύση. Η πρόταση έχει τη μορφή $\varphi \wedge r$, όπου $\varphi = (p \wedge q) \rightarrow$, και η φ δεν είναι άτομο, ούτε πρόταση, αφού δεν είναι της μορφής $\varphi_1 \square \varphi_2$ ή $\neg\varphi_1$. □

Άσκηση 6.2. *Να δοθούν επαγωγικοί ορισμοί των εννοιών* $\alpha(\varphi)$ *ο αριθμός των θέσεων της* φ *όπου εμφανίζεται άτομο και* $\beta(\varphi)$ *ο αριθμός των θέσεων όπου εμφανίζεται διμελής σύνδεσμος (που ορίστηκαν ήδη "άτυπα").*

Λύση. $\alpha(p) = 1$, $\alpha(\neg\varphi) = \alpha(\varphi)$ και $\alpha(\varphi_1 \square \varphi_2) = \alpha(\varphi_1) + \alpha(\varphi_2)$.
$\beta(p) = 0$, $\beta(\neg\varphi) = \beta(\varphi)$ και $\beta(\varphi_1 \square \varphi_2) = \beta(\varphi_1) + \beta(\varphi_2) + 1$. □

Άσκηση 6.3. *Να δειχθεί ότι κάθε πρόταση περιέχει άρτιο αριθμό παρενθέσεων.*

Λύση. Έστω πρόταση ϕ και έστω $\pi(\phi)$ το πλήθος παρενθέσεων που περιέχει. Αν $\phi = p$, όπου p άτομο, τότε $\pi(\phi) = 0$ (άρτιος). Αν $\phi = (\phi_1) \square (\phi_2)$ τότε $\pi(\phi) = \pi(\phi_1) + 2 + \pi(\phi_2) + 2$ (άρτιος ως άθροισμα άρτιων). Αν $\phi = \neg(\phi_1)$ τότε $\pi(\phi) = \pi(\phi_1) + 2$ (άρτιος). □

6.2.2 Ασκήσεις προς επίλυση

1) Να βρεθεί η τάξη των προτάσεων:

   α) $(p_1 \to \neg(p_2 \wedge (\neg p_3 \to p_1))) \vee (p_3 \to \neg(p_4 \vee p_4))$,

   β) $\neg p_1 \to (p_2 \vee (p_3 \wedge (p_4 \leftrightarrow p_5)))$.

   γ) $p_1 \vee (p_1 \vee p_1)$.

   δ) $p_1 \vee (p_1 \vee (p_1 \vee p_1))$.

2) Να κατασκευαστούν τα δένδρα ανάλυσης των προτάσεων της ᾽σκησης 1).

3) Έστω $r(\varphi)$ η τάξη της φ και $\boldsymbol{\gamma(\varphi)}$ ο αριθμός των θέσεων όπου εμφανίζεται σύνδεσμος στη φ. Να δειχθεί ότι $r(\varphi) \leq \gamma(\varphi)$.

4) Να δειχθεί ότι $|\,\mathrm{sub}(\varphi)| \leq 2\gamma(\varphi) + 1$.

5) Έστω $\boldsymbol{|T(\varphi)|}$ ο αριθμός των κόμβων του δένδρου $T(\varphi)$ και $|\,\mathrm{sub}(\varphi)|$ ο αριθμός των υποπροτάσεων της φ. Να δειχθεί ότι:

   i) $\alpha(\varphi) + \gamma(\varphi) = |T(\varphi)|$,

   ii) $|\,\mathrm{sub}(\varphi)| \leq |T(\varphi)|$,

   iii) $\alpha(\varphi) + \gamma(\varphi) \leq 2^{r(\varphi)+1} - 1$.

6) Να δοθούν επαγωγικοί ορισμοί των εννοιών $\gamma(\varphi)$ και $|T(\varphi)|$ (που ορίστηκαν ήδη "άτυπα").

7) Να ορισθούν επαγωγικά οι έννοιες:

   i) "Πλήθος θέσεων όπου εμφανίζεται $\leftrightarrow$ στην φ".

   ii) "Πλήθος θέσεων όπου εμφανίζεται $\leftrightarrow$ ή $\to$ στην φ".

8) Έστω T ένα δένδρο με ρίζα. Ορίζουμε ως ύψος $\boldsymbol{h(T)}$ τη μέγιστη από τις αποστάσεις ανάμεσα στη ρίζα και τα φύλλα του T. Να ορισθεί επαγωγικά το $h(T(\varphi))$ για κάθε πρόταση $\varphi \in P$ και να δειχθεί (επαγωγικά) ότι $h(T(\varphi)) = r(\varphi)$.

6.3 Τιμές αληθείας, εκτίμηση, λογικό συμπέρασμα

Κάθε πρόταση $\varphi \in P$ είναι Αληθής (1, Α, T) ή Ψευδής (0, Ψ, F). Η απονομή μιας τιμής αληθείας σε μια πρόταση λέγεται **εκτίμηση**. Δηλαδή, η εκτίμηση είναι μια απεικόνιση $v : P \to \{0,1\}$. Θα ορίσουμε την εκτίμηση επαγωγικά. Για το λόγο αυτό, χρειαζόμαστε τους κανόνες:

$$G_\square : \{0,1\} \times \{0,1\} \to \{0,1\} \qquad \text{και} \qquad G_\neg : \{0,1\} \to \{0,1\}.$$

Οι κανόνες αυτοί ορίζονται ως εξής:

$G_\wedge(0,0) = 0$	$G_\vee(0,0) = 0$	$G_\to(0,0) = 1$	$G_\leftrightarrow(0,0) = 1$
$G_\wedge(0,1) = 0$	$G_\vee(0,1) = 1$	$G_\to(0,1) = 1$	$G_\leftrightarrow(0,1) = 0$
$G_\wedge(1,0) = 0$	$G_\vee(1,0) = 1$	$G_\to(1,0) = 0$	$G_\leftrightarrow(1,0) = 0$
$G_\wedge(1,1) = 1$	$G_\vee(1,1) = 1$	$G_\to(1,1) = 1$	$G_\leftrightarrow(1,1) = 1$

και $G_\neg(0) = 1$, $G_\neg(1) = 0$.

Επίσης, γράφουμε ισοδύναμα:

$G_\wedge(\varphi, y)$

$\varphi \backslash y$	1	0
1	1	0
0	0	0

$G_\vee(\varphi, y)$

$\varphi \backslash y$	1	0
1	1	1
0	1	0

$G_\to(\varphi, y)$

$\varphi \backslash y$	1	0
1	1	0
0	1	1

$G_\leftrightarrow(\varphi, y)$

$\varphi \backslash y$	1	0
1	1	0
0	0	1

$G_\neg(\varphi)$

φ	$G_\neg(\varphi)$
1	0
0	1

ή, πιο συνηθισμένα:

φ	y	$\varphi \wedge y$
1	1	1
1	0	0
0	1	0
0	0	0

φ	y	$\varphi \vee y$
1	1	1
1	0	1
0	1	1
0	0	0

φ	y	$\varphi \to y$
1	1	1
1	0	0
0	1	1
0	0	1

φ	y	$\varphi \leftrightarrow y$
1	1	1
1	0	0
0	1	0
0	0	1

φ	$\neg\varphi$
1	0
0	1

Είμαστε τώρα έτοιμοι να δώσουμε τον ορισμό της εκτίμησης.

Ορισμός. *Κάθε απεικόνιση $v : P_0 \to \{0,1\}$ που επεκτείνεται στο P μέσω των κανόνων*

φ	y	$\varphi \wedge y$
1	*1*	*1*
1	*0*	*0*
0	*1*	*0*
0	*0*	*0*

φ	y	$\varphi \vee y$
1	*1*	*1*
1	*0*	*1*
0	*1*	*1*
0	*0*	*0*

φ	y	$\varphi \to y$
1	*1*	*1*
1	*0*	*0*
0	*1*	*1*
0	*0*	*1*

φ	y	$\varphi \leftrightarrow y$
1	*1*	*1*
1	*0*	*0*
0	*1*	*0*
0	*0*	*1*

φ	$\neg\varphi$
1	*0*
0	*1*

ονομάζεται ***εκτίμηση*** *(valuation)* [α].

[α] Δηλαδή, με βάση τους παραπάνω κανόνες για τους 5 συνδέσμους, μπορούμε να βρούμε την τιμή αλήθειας οποιασδήποτε πρότασης φ, αρκεί να έχουμε δώσει τιμή αλήθειας σε κάθε άτομο που περιέχεται στη φ.

Παράδειγμα

Έστω $\varphi = (p_1 \vee p_2) \vee (p_3 \to p_2)$.

Αν θεωρήσουμε $v(p_1) = 1$, $v(p_2) = 0$, $v(p_3) = 0$, τότε $v(p_1 \vee p_2) = 1$ και $v(p_3 \to p_2) = 1$, οπότε $v(\varphi) = 1$.

Αν θεωρήσουμε $\nu(p_1) = 1$, $\nu(p_2) = 0$, $\nu(p_3) = 1$, τότε $\nu(p_1 \vee p_2) = 1$ και $\nu(p_3 \to p_2) = 0$, οπότε $\nu(\varphi) = 1$, κ.ο.κ.

Για να καλύψουμε όλες τις περιπτώσεις, μπορούμε να δημιουργήσουμε **πίνακες αληθείας** με 2^n γραμμές, (όπου n είναι το πλήθος των (διαφορετικών) ατόμων της φ). Συχνά γράφουμε A, Ψ ή T, F αντί για 1, 0 αντίστοιχα.

Παράδειγμα 6.3.1. *Να γραφεί ο πίνακας αληθείας της πρότασης* $\varphi_1 = (p \to q) \vee \neg(p \leftrightarrow \neg q)$.

p	q	$p \to q$	$\neg q$	$p \leftrightarrow \neg q$	$\neg(p \leftrightarrow \neg q)$	φ_1
1	1	1	0	0	1	1
1	0	0	1	1	0	0
0	1	1	0	1	0	1
0	0	1	1	0	1	1

Παράδειγμα 6.3.2. *Να γραφεί ο πίνακας αληθείας της πρότασης* $\varphi_2 = (p \wedge q) \vee (r \to \neg p)$.

p	q	r	$p \wedge q$	$\neg p$	$r \to \neg p$	φ_2
A	A	A	A	Ψ	Ψ	A
A	A	Ψ	A	Ψ	A	A
A	Ψ	A	Ψ	Ψ	Ψ	Ψ
A	Ψ	Ψ	Ψ	Ψ	A	A
Ψ	A	A	Ψ	A	A	A
Ψ	A	Ψ	Ψ	A	A	A
Ψ	Ψ	A	Ψ	A	A	A
Ψ	Ψ	Ψ	Ψ	A	A	A

Παράδειγμα 6.3.3. *Να γραφεί ο πίνακας αληθείας της πρότασης* $\varphi_3 = \neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	φ_3
A	A	A	Ψ	Ψ	Ψ	Ψ	A
A	Ψ	Ψ	A	Ψ	A	A	A
Ψ	A	Ψ	A	A	Ψ	A	A
Ψ	Ψ	Ψ	A	A	A	A	A

Ορισμός. *Αν* $\nu(\varphi) = 1$, *λέμε ότι η* ν ***ικανοποιεί*** *ή* ***επαληθεύει τη*** $\boldsymbol{\varphi}$ *ή ότι η* ν ***είναι μοντέλο της*** φ *και γράφουμε* $\boldsymbol{\nu \models \varphi}$. *(Γράφουμε* $\boldsymbol{\nu \not\models \varphi}$ *όταν* $\nu(\varphi) = 0$.)

Αν τώρα $\Sigma \subseteq P$ *και* $\nu \models \varphi$, *για κάθε* $\varphi \in \Sigma$, *τότε λέμε ότι η* ν ***ικανοποιεί*** *ή* ***επαληθεύει το*** $\boldsymbol{\Sigma}$ *ή ότι η* ν ***είναι μοντέλο του*** $\boldsymbol{\Sigma}$ *και γράφουμε* $\boldsymbol{\nu \models \Sigma}$.

Το $\Sigma \subseteq P$ *λέγεται* ***ικανοποιήσιμο*** *όταν υπάρχει (τουλάχιστον μια) εκτίμηση* ν *τέτοια ώστε* $\nu \models \Sigma$, *(δηλαδή, αν έχει τουλάχιστον ένα μοντέλο). Αν το* Σ *δεν είναι ικανοποιήσιμο (δηλαδή όταν δεν υπάρχει εκτίμηση* ν *τέτοια ώστε* $\nu \models \Sigma$*) τότε ονομάζεται* ***μη ικανοποιήσιμο*** *ή* ***αντιφατικό***.

Παραδείγματα

1. Η εκτίμηση v_1 με $v_1(p) = 0$ και $v_1(q) = 1$ ικανοποιεί τη φ_1 του παραδείγματος 6.3.1.
2. Για τη v_2 με $v_2(p) = \Psi$ και $v_2(q) = v_2(r) = A$ έχουμε $v_2 \models \varphi_2$ για το παράδειγμα 6.3.2.
3. Για τη v_3 με $v_3(q) = \Psi$ και $v_3(p) = v_3(r) = A$ έχουμε $v_3 \not\models \varphi_2$ για το παράδειγμα 6.3.2.
4. Αν τώρα $\Sigma = \{\varphi_2, \varphi_3\} \subseteq P$, έχουμε ότι για τη v_2 ισχύει ότι $v_2 \models \Sigma$, δηλαδή η v_2 είναι ένα μοντέλο του Σ (και άρα το Σ αυτό είναι ικανοποιήσιμο). Αντίθετα, για την εκτίμηση v_3 δεν ισχύει ότι $v_3 \models \Sigma$, αφού η v_3 δεν ικανοποιεί την φ_2.

Παρατήρηση. Αν το Σ είναι ικανοποιήσιμο, τότε κάθε υποσύνολό του Σ' είναι ικανοποιήσιμο. Αντίθετα, αν το Σ είναι μη ικανοποιήσιμο, τότε κάθε υπερσύνολο του Σ'' είναι μη ικανοποιήσιμο.

Ορισμός. *Μια πρόταση φ λέγεται* ***ταυτολογία*** *αν $v \models \varphi$ για κάθε v και τότε γράφουμε* $\models \varphi$. *Η φ λέγεται* ***αντίφαση*** *ή* ***αντιλογία*** *αν $v \not\models \varphi$ για κάθε v.*

Παραδείγματα

1. Η φ_3 του προηγούμενου παραδείγματος 6.3.3 είναι μια ταυτολογία (ταυτότητα De Morgan).
2. Η $\varphi = p \wedge q \leftrightarrow \neg p \vee \neg q$ είναι αντίφαση, όπως φαίνεται και από τον πίνακα αληθείας της:

p	q	$p \wedge q$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	φ
1	1	1	0	0	0	0
1	0	0	0	1	1	0
0	1	0	1	0	1	0
0	0	0	1	1	1	0

Περισσότερα παραδείγματα ταυτολογιών (έλεγχος με πίνακες αληθείας - Άσκηση):

$$\varphi \rightarrow \neg\neg\varphi, \qquad \varphi \wedge y \rightarrow \varphi, \qquad \varphi \rightarrow \varphi \vee y, \qquad \varphi \rightarrow \varphi, \qquad \varphi \vee \neg\varphi \qquad \text{κ.λπ.}$$

Ορισμός. *Έστω $\varphi \in P$, $\Sigma \subseteq P$. Η φ λέγεται* ***λογικό συμπέρασμα του*** Σ, *αν κάθε μοντέλο του Σ είναι και μοντέλο της φ, (δηλαδή για κάθε εκτίμηση v, αν $v \models \Sigma$ τότε $v \models \varphi$). Γράφουμε τότε* $\Sigma \models \varphi$. *(Αν $\Sigma = \{y\}$, γράφουμε* $y \models \varphi$ *αντί $\{y\} \models \varphi$.)*

Παρατήρηση. Από τον ορισμό προκύπτει ότι **η φ δεν είναι λογικό συμπέρασμα του** Σ ανν υπάρχει μοντέλο του Σ το οποίο δεν είναι μοντέλο της φ. Επομένως, στην περίπτωση όπου το Σ είναι μη ικανοποιήσιμο, έπεται ότι $\Sigma \models \varphi$ για κάθε $\varphi \in P$.

Παραδείγματα

$\varphi \models \varphi$, $\varphi \wedge y \models \varphi$, $\varphi \models y \vee \varphi$, $\{\varphi, \varphi \rightarrow y\} \models y$ [1], $\{y \rightarrow \varphi, \neg\varphi\} \models \neg y$ [2],
$\{p_1, p_2, p_1 \vee p_3\} \models (p_1 \wedge p_2) \wedge (p_3 \vee \neg p_3)$ [3].

[1] Το (μοναδικό) μοντέλο v του $\{\varphi, \varphi \rightarrow y\}$ (με $v(\varphi) = v(y) = 1$) είναι και μοντέλο του y (αφού $v(y) = 1$).
[2] Ομοίως για $v(y) = v(\varphi) = 0$.
[3] Τα μοναδικά μοντέλα του $\{p_1, p_2, p_1 \vee p_3\}$ (με $\begin{Bmatrix} v(p_1) = v(p_2) = 1, v(p_3) = 0 \\ \text{ή } v(p_1) = v(p_2) = v(p_3) = 1 \end{Bmatrix}$) είναι και μοντέλα της $(p_1 \wedge p_2) \wedge (p_3 \vee \neg p_3)$.

Πρόταση 6.3. *$\varphi \models y$ αν και μόνο αν $\models \varphi \to y$.*
(Δηλαδή η y είναι λογικό συμπέρασμα της φ, αν και μόνο αν η $\varphi \to y$ είναι ταυτολογία.)

Απόδειξη. Αρχικά θα αποδείξουμε το ευθύ. Διακρίνουμε 2 περιπτώσεις:

1. Αν $\nu(\varphi) = 0$, τότε $\nu(\varphi \to y) = 1$.
2. Αν $\nu(\varphi) = 1$, τότε, αφού $\varphi \models y$, έχουμε ότι και $\nu(y) = 1$, οπότε πάλι $\nu(\varphi \to y) = 1$.

᾽ρα πράγματι $\models \varphi \to y$.

Στη συνέχεια θα αποδείξουμε το αντίστροφο. Αφού $\models \varphi \to y$, έχουμε ότι $\nu(\varphi \to y) = 1$. Αν λοιπόν $\nu(\varphi) = 1$, τότε πρέπει και $\nu(y) = 1$. ᾽ρα, πράγματι, $\varphi \models y$. □

Ορισμός. *Οι φ, y λέγονται **(λογικά) ισοδύναμες**, αν και μόνο αν $\varphi \models y$ και $y \models \varphi$ (δηλαδή οι φ και y έχουν τα ίδια μοντέλα). Γράφουμε τότε $\boldsymbol{\varphi \rightleftarrows y}$.*

Πρόταση 6.4. *$\varphi \rightleftarrows y$, αν και μόνο αν $\models \varphi \leftrightarrow y$.*

Πρόταση 6.5 (**Αντικατάσταση**). *Αν σ υποπρόταση της φ και σ' τυχούσα πρόταση, συμβολίζουμε με $\boldsymbol{\varphi[\sigma/\sigma']}$ την έκφραση που προκύπτει αν αντικαταστήσουμε τη σ με τη σ' στη φ. Τότε:*

i) Η $\varphi[\sigma/\sigma']$ είναι πρόταση, και

ii) Αν $\sigma \rightleftarrows \sigma'$ τότε $\varphi \rightleftarrows \varphi[\sigma/\sigma']$.

Βασικές Ισοδυναμίες

$$\left\{\begin{array}{c}(\varphi \to y) \rightleftarrows (\neg\varphi \vee y)\\ (\varphi \leftrightarrow y) \rightleftarrows (\varphi \to y) \wedge (y \to \varphi)\end{array}\right\}$$
(Άρα οι σύνδεσμοι $\to, \leftrightarrow$ δεν είναι απαραίτητοι.)

$$\left\{\begin{array}{c}\neg(\varphi \wedge y) \rightleftarrows \neg\varphi \vee \neg y\\ \neg(\varphi \vee y) \rightleftarrows \neg\varphi \wedge \neg y\\ \neg(\neg\varphi) \rightleftarrows \varphi\end{array}\right\}$$
Κανόνες του De Morgan.

$$\left\{\begin{array}{c}\varphi \wedge (y \wedge \sigma) \rightleftarrows (\varphi \wedge y) \wedge \sigma\\ \varphi \vee (y \vee \sigma) \rightleftarrows (\varphi \vee y) \vee \sigma\end{array}\right\}$$
Προσεταιριστικότητα των $\wedge, \vee$. (Μπορούμε λοιπόν να παραλείπουμε τις παρενθέσεις σ΄ αυτές τις περιπτώσεις[4].)

$$\left\{\begin{array}{c}\varphi \wedge y \rightleftarrows y \wedge \varphi\\ \varphi \vee y \rightleftarrows y \vee \varphi\end{array}\right\}$$
Αντιμεταθετικότητα των $\wedge, \vee$.

$$\left\{\begin{array}{c}\varphi \vee (y \wedge \sigma) \rightleftarrows (\varphi \vee y) \wedge (\varphi \vee \sigma)\\ \varphi \wedge (y \vee \sigma) \rightleftarrows (\varphi \wedge y) \vee (\varphi \wedge \sigma)\end{array}\right\}$$
Επιμεριστικότητα των $\wedge, \vee$ ως προς τους $\vee, \wedge$ αντίστοιχα.

$$\left\{\begin{array}{l}\text{Αν } \varphi \models y, \text{ τότε } \varphi \wedge y \rightleftarrows \varphi\\ \text{Αν } \varphi \models y, \text{ τότε } \varphi \vee y \rightleftarrows y\end{array}\right\}$$
Κανόνες απορρόφησης.

Οι αποδείξεις των προηγούμενων ιδιοτήτων γίνονται εύκολα με πίνακες αληθείας (ʹσκηση). Για παράδειγμα, για την $(\varphi \to y) \nvDash (\neg\varphi \vee y)$, δηλαδή $\models (\varphi \to y) \leftrightarrow (\neg\varphi \vee y)$, έχουμε:

φ	y	$\varphi \to y$	$\neg\varphi$	$\neg\varphi \vee y$	$(\varphi \to y) \leftrightarrow (\neg\varphi \vee y)$
1	1	1	0	1	1
1	0	0	0	0	1
0	1	1	1	1	1
0	0	1	1	1	1

Παρατήρηση. Χρησιμοποιώντας τους κανόνες De Morgan (για τις προτάσεις $\neg\varphi$ και $\neg y$) παίρνουμε ότι $\neg(\neg\varphi \wedge \neg y) \nvDash \neg(\neg\varphi) \vee \neg(\neg y)$, δηλαδή $\varphi \vee y \nvDash \neg(\neg\varphi \wedge \neg y)$, και όμοια $\varphi \wedge y \nvDash \neg(\neg\varphi \vee \neg y)$. Άρα, και ο ένας από τους συνδέσμους $\wedge, \vee$ μπορεί να θεωρηθεί ότι δεν είναι απαραίτητος.

Ορισμός. *Το σύνολο $\Sigma \subseteq P$ λέγεται* ***πεπερασμένα ικανοποιήσιμο*** *αν κάθε πεπερασμένο υποσύνολό του είναι ικανοποιήσιμο.*

Το Σ λέγεται ***μεγιστικό πεπερασμένα ικανοποιήσιμο*** *αν είναι πεπερασμένα ικανοποιήσιμο, και κάθε $\Sigma' \supset \Sigma$ δεν είναι πεπερασμένα ικανοποιήσιμο.*

Πρόταση 6.6 (Θεώρημα Συμπάγειας (**Compactness Thoeorem**)). *Το σύνολο $\Sigma \subseteq P$ είναι ικανοποιήσιμο αν και μόνο αν είναι πεπερασμένα ικανοποιήσιμο.*

Πόρισμα 6.7. *Αν $\Sigma \models \varphi$, τότε υπάρχει πεπερασμένο $A \subseteq \Sigma$, με $A \models \varphi$.*

Παρατήρηση. Από το Θεώρημα της Συμπάγειας επίσης προκύπτει ότι αν ένα σύνολο είναι μη ικανοποιήσιμο, τότε περιέχει ένα πεπερασμένο υποσύνολο το οποίο είναι μη ικανοποιήσιμο.

[4] Λόγω της προσεταιριστικότητας των $\wedge, \vee$, θα γράφουμε γενικότερα:

$$\bigwedge_{i=1}^{n} \varphi_i = \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n \qquad \text{και} \qquad \bigvee_{i=1}^{n} \varphi_i = \varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_n.$$

6.3.1 Λυμένες ασκήσεις

Άσκηση 6.4. *Έστω η πρόταση*

$$\varphi = (p_1 \vee p_2) \vee (p_3 \to p_1).$$

i) Να βρεθεί η τιμή αλήθειας της πρότασης φ όταν $v(p_1) = 1$, $v(p_2) = 0$ και $v(p_3) = 0$.

ii) Να εξετασθεί αν υπάρχει εκτίμηση v για την οποία η πρόταση φ είναι ψευδής.

Λύση.

i) $v(p_1 \vee p_2) = 1$, διότι $v(p_1) = 1$ και $v(p_2) = 0$.
$v(p_3 \to p_2) = 1$, διότι $v(p_3) = v(p_2) = 0$.
Άρα, $v(\varphi) = 1$, διότι $v(p_1 \vee p_2) = 1$ και $v(p_3 \to p_2) = 1$.

ii) Η φ είναι ψευδής αν και μόνο αν οι προτάσεις $p_1 \vee p_2$ και $p_3 \to p_2$ είναι ψευδείς.
$v(p_1 \vee p_2) = 0 \Leftrightarrow v(p_1) = v(p_2) = 0$.
$v(p_3 \to p_2) = 0 \Leftrightarrow v(p_3) = 1$ και $v(p_2) = 0$.
Άρα, η φ είναι ψευδής αν και μόνο αν $v(p_1) = v(p_2) = 0$ και $v(p_3) = 1$. □

Άσκηση 6.5 (Τιμές αλήθειας). *Δοθέντος ότι η πρόταση $p \to q$ είναι ψευδής, να βρεθεί η τιμή αλήθειας των προτάσεων $(p \to q) \to r$, $p \vee (q \to r)$ και $q \wedge (p \vee r)$.*

Λύση. Επειδή $v(p \to q) = 0$ ισχύει ότι $v(p) = 1$ και $v(q) = 0$.
Άρα,
$v((p \to q) \to r) = 1$ (αφού $v(p \to q) = 0$).
$v(p \vee (q \to r)) = 1$ (αφού $v(p) = 1$).
$v(q \wedge (p \vee r)) = 0$ (αφού $v(q) = 0$). □

Άσκηση 6.6 (Ψευδείς προτάσεις). *Να βρεθούν εκτιμήσεις για τις οποίες οι παρακάτω προτάσεις είναι ψευδείς:*

i) $\varphi_1 = (x \vee y \vee z) \to ((x \vee y) \wedge (x \vee z))$.

ii) $\varphi_2 = ((p \to (q \wedge r)) \to (\neg q \to \neg p)) \to \neg q$.

Λύση.

i) Για να είναι η πρόταση φ_1 ψευδής πρέπει $v((x \vee y \vee z)) = 1$ και $v(((x \vee y) \wedge (x \vee z)) = 0$.
Αν $v(x) = 1$, τότε $v((x \vee y \vee z)) = v(((x \vee y) \wedge (x \vee z))) = 1$. Άρα, $v(x) = 0$.
Επομένως, πρέπει ακριβώς ένα από τα y και z να είναι ψευδές (και το άλλο αληθές).
Άρα, έχουμε δύο εκτιμήσεις για τις οποίες $v(\varphi_1) = 0$:

- $v(x) = v(y) = 0$ και $v(z) = 1$.

- $\nu(x) = \nu(z) = 0$ και $\nu(y) = 1$.

ιι) Για να είναι η πρόταση φ_2 ψευδής πρέπει $\nu((p \to (q \wedge r)) \to (\neg q \to \neg p)) = 1$ και $\nu(\neg q) = 0$.

Άρα, $\nu(q) = 1$.

Επομένως, $\nu(\neg q \to \neg p) = 1$ (αφού $\nu(\neg q) = 0$).

οπότε και $\nu((p \to (q \wedge r)) \to (\neg q \to \neg p)) = 1$ (αφού $\nu(\neg q \to \neg p) = 1$).

Συνεπώς, έχουμε τέσσερεις εκτιμήσεις για τις οποίες $\nu(\varphi_2) = 0$:

- $\nu(q) = \nu(p) = \nu(r) = 1$
- $\nu(q) = \nu(p) = 1$, $\nu(r) = 0$
- $\nu(q) = \nu(r) = 1$, $\nu(p) = 0$
- $\nu(q) = 1$, $\nu(p) = \nu(r) = 0$. □

Άσκηση 6.7. *Να εξετασθεί αν η πρόταση*

$$\varphi = ((p \to q) \to (q \to r)) \to (p \to r)$$

είναι ταυτολογία ή όχι.

Λύση. Θα χρησιμοποιήσουμε την μέθοδο του πίνακα αληθείας. Η πρόταση αυτή περιέχει 3 διαφορετικά άτομα: Τα p, q, r. Άρα, ο πίνακας αληθείας της θα έχει $2^3 = 8$ γραμμές.

p	q	r	$p \to q$	$q \to r$	$(p \to q) \to (q \to r)$	$p \to r$	φ
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	0	0
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

Από τον πίνακα αληθείας προκύπτει ότι η φ δεν είναι ταυτολογία, διότι υπάρχει εκτίμηση ν για την οποία $\nu(\varphi) = 0$: Η εκτίμηση ν με $\nu(p) = 1$ και $\nu(q) = \nu(r) = 0$. □

Άσκηση 6.8. *Δίδεται η πρόταση*

$$\varphi = (p \to q) \to \neg(r \leftrightarrow (p \wedge \neg q)).$$

(i) Να βρεθούν όλα τα μοντέλα της πρότασης φ.

(ii) Να εξετασθεί αν η πρόταση φ είναι ταυτολογία ή αντιλογία.

Λύση.

(i)

p	q	r	$p \to q$	$p \wedge \neg q$	$r \leftrightarrow (p \wedge \neg q)$	$\neg(r \leftrightarrow (p \wedge \neg q))$	φ
1	1	1	1	0	0	1	1
1	1	0	1	0	1	0	0
1	0	1	0	1	1	0	1
1	0	0	0	1	0	1	1
0	1	1	1	0	0	1	1
0	1	0	1	0	1	0	0
0	0	1	1	0	0	1	1
0	0	0	1	0	1	0	0

Άρα, τα μοντέλα της πρότασης φ είναι οι επόμενες πέντε εκτιμήσεις:

1. $v(p) = v(q) = v(r) = 1$,
2. $v(p) = v(r) = 1$, $v(q) = 0$,
3. $v(p) = 1$, $v(q) = v(r) = 0$,
4. $v(p) = 0$, $v(q) = v(r) = 1$,
5. $v(p) = v(q) = v(r) = 0$

(ii) Η φ δεν είναι ούτε ταυτολογία, ούτε αντιλογία. □

Άσκηση 6.9. *Να εξετασθεί αν η πρόταση q είναι λογικό συμπέρασμα του συνόλου Σ, όπου $\Sigma = \{p, p \to q\}$.*

Λύση. Για να απαντήσουμε στο ερώτημα θα βρούμε όλα τα μοντέλα του Σ και θα ελέγξουμε αν επαληθεύουν την πρόταση q.

Έστω εκτίμηση v που ικανοποιεί το Σ. Πρέπει

$$v(p) = 1 \text{ και } v(p \to q) = 1,$$

επομένως,

$$v(p) = 1 \text{ και } v(q) = 1,$$

δηλαδή

$$v \models \Sigma \text{ αν και μόνο αν } v(p) = v(q) = 1,$$

οπότε

$$v \models q.$$

Άρα, η q είναι λογικό συμπέρασμα του Σ. □

Άσκηση 6.10 (Λογικά συμπεράσματα). *Δίδονται οι προτάσεις $\varphi_1 = p \wedge q$ και $\varphi_2 = p \vee q$. Να εξετασθεί αν η πρόταση φ_2 είναι λογικό συμπέρασμα της πρότασης φ_1 και το αντίστροφο.*

Λύση. Η φ_1 έχει μοναδικό μοντέλο την εκτίμηση v με $v(p) = v(q) = 1$. Η εκτίμηση αυτή επαληθεύει την φ_2, οπότε η φ_2 είναι λογικό συμπέρασμα της φ_1.

Το αντίστροφο δεν ισχύει διότι η εκτίμηση v με $v(p) = 1$ και $v(q) = 0$ είναι μοντέλο της φ_2 (αφού $v(\varphi_2) = 1$) όμως δεν είναι μοντέλο της φ_1 (αφού $v(\varphi_1) = 0$).

Παρατήρηση: Μπορούσαμε να δώσουμε την απάντηση ελέγχοντας αν οι προτάσεις $(p \wedge q) \to (p \vee q)$ και $(p \vee q) \to (p \wedge q)$ είναι ταυτολογίες ή όχι, αντίστοιχα. □

Άσκηση 6.11. *Να βρεθούν, αν υπάρχουν, όλα τα μοντέλα του συνόλου Σ_i, όπου*

i) $\Sigma_1 = \{p_1 \to p_2, p_1 \wedge (p_1 \to p_2), p_2 \vee (p_1 \wedge p_2)\}$.

ii) $\Sigma_2 = \{p_1 \vee p_2, p_1 \wedge \neg p_3, p_2 \to (p_1 \vee p_3)\}$.

iii) $\Sigma_3 = \{p_1 \wedge \neg p_2, p_2 \vee p_3, p_3 \wedge p_4, \neg p_4 \vee \neg p_5, \neg p_5 \vee p_6\}$.

Στη συνέχεια, να εξετασθεί αν κάποια από τις προτάσεις $p_1 \to p_6$ και $p_1 \to p_3$ είναι λογικό συμπέρασμα του συνόλου Σ_3.

Λύση.

i) Στις προτάσεις του Σ_1 εμφανίζονται 2 διαφορετικά άτομα: τα p_1, p_2.

Ο πίνακας αληθείας των προτάσεων του Σ_1 είναι ο εξής:

p_1	p_2	$p_1 \to p_2$	$p_1 \wedge (p_1 \to p_2)$	$p_2 \vee (p_1 \wedge p_2)$
1	1	1	1	1
1	0	0	0	0
0	1	1	0	1
0	0	1	0	0

Από τον πίνακα αληθείας των προτάσεων έπεται ότι το Σ_1 έχει ακριβώς ένα μοντέλο: την εκτίμηση v με $v(p_1) = v(p_2) = 1$.

ii) Ο πίνακας αληθείας των προτάσεων του Σ_2 είναι ο εξής:

p_1	p_2	p_3	$p_1 \vee p_2$	$p_1 \wedge \neg p_3$	$p_2 \to (p_1 \vee p_3)$
1	1	1	1	0	1
1	1	0	1	1	1
1	0	1	1	0	1
1	0	0	1	1	1
0	1	1	1	0	1
0	1	0	1	0	0
0	0	1	0	0	1
0	0	0	0	0	1

Άρα, το Σ_2 έχει δύο μοντέλα:

1ο μοντέλο: $v(p_1) = v(p_2) = 1$ και $v(p_3) = 0$.

2ο μοντέλο: $v(p_1) = 1$ και $v(p_2) = v(p_3) = 0$.

iii) Επειδή στις προτάσεις του Σ_3 εμφανίζονται 6 διαφορετικά άτομα (p_1, p_2, p_3, p_4, p_5, p_6) η μέθοδος του πίνακα αληθείας απαιτεί $2^6 = 64$ γραμμές.

Γι' αυτό θα χρησιμοποιήσουμε έναν άλλο τρόπο για να βρούμε τα μοντέλα του Σ_3.

Έστω v ένα μοντέλο του Σ_3, τότε $v(\varphi) = 1$ για κάθε $\varphi \in \Sigma_3$.

Για να μειώσουμε τον αριθμό των περιπτώσεων που πρέπει να εξετάσουμε, αρχίζουμε από τις συζευκτικές προτάσεις.

$v(p_1 \wedge \neg p_2) = 1 \Leftrightarrow v(p_1) = 1$ και $v(\neg p_2) = 1 \Leftrightarrow v(p_1) = 1$ και $v(p_2) = 0$.

$v(p_3 \wedge p_4) = 1 \Leftrightarrow v(p_3) = 1$ και $v(p_4) = 1$.

$v(p_2 \vee p_3) = 1$, το οποίο ισχύει αφού $v(p_3) = 1$.

$v(\neg p_4 \vee \neg p_5) = 1 \Leftrightarrow v(\neg p_5) = 1$ αφού $v(p_4) = 1$. Άρα, $v(p_5) = 0$.

$v(\neg p_5 \vee p_6) = 1$, το οποίο ισχύει αφού $v(p_5) = 0$. Για το p_6 υπάρχουν 2 επιλογές $v(p_6) = 1$ ή $v(p_6) = 0$.

Άρα, τελικά, για το Σ_3 υπάρχουν 2 ακριβώς μοντέλα:

1ο μοντέλο: $v(p_1) = v(p_3) = v(p_4) = v(p_6) = 1$ και $v(p_2) = v(p_5) = 0$.

2ο μοντέλο: $v(p_1) = v(p_3) = v(p_4) = 1$ και $v(p_2) = v(p_5) = v(p_6) = 0$.

Η πρόταση $p_1 \to p_6$ δεν είναι λογικό συμπέρασμα του συνόλου Σ_3 διότι υπάρχει μοντέλο του Σ_3, το οποίο δεν είναι μοντέλο της πρότασης $p_1 \to p_6$. (Το 2ο μοντέλο του Σ_3.)

Η πρόταση $p_1 \to p_3$ είναι λογικό συμπέρασμα του Σ_3, διότι κάθε μοντέλο του Σ_3 είναι και μοντέλο της πρότασης $p_1 \to p_3$. □

Άσκηση 6.12 (Μη ικανοποιήσιμο σύνολο). *Έστω*

$$\Sigma = \{\neg(q \to (p \vee r)), (q \to p) \wedge q\}.$$

i) Να βρεθούν όλα τα μοντέλα του συνόλου Σ.

ii) Να εξετασθεί αν η πρόταση $p \to r$ *είναι λογικό συμπέρασμα του* Σ.

Λύση.

i) Για κάθε μοντέλο v του Σ πρέπει να ισχύει

$v(\neg(q \to (p \vee r))) = v((q \to p) \wedge q) = 1$.

Επομένως,

$v(\neg(q \to (p \vee r))) = 1 \Leftrightarrow v(q \to (p \vee r)) = 0 \Leftrightarrow v(q) = 1$ και $v(p \vee r) = 0$.

Άρα, πρέπει $v(q) = 1$ και $v(p) = v(r) = 0$.

Για την εκτίμηση αυτή έχουμε $v((q \to p) \wedge q) = 0$.

Άρα, το Σ είναι μη ικανοποιήσιμο, δηλαδή δεν έχει κανένα μοντέλο.

ιι) Επειδή το Σ είναι μη ικανοποιήσιμο, έπεται ότι η πρόταση $p \to r$ είναι λογικό συμπέρασμα του Σ. □

Άσκηση 6.13.
Να εξετασθεί αν κάποιο από τα παρακάτω ξεύγη προτάσεων είναι λογικά ισοδύναμα:

(i) $\neg(p \leftrightarrow q)$, $\neg p \leftrightarrow \neg q$.

(ii) $p \vee (q \leftrightarrow r)$, $(p \vee q) \leftrightarrow (p \vee r)$.

(iii) $p \wedge (q \leftrightarrow r)$, $(p \wedge q) \leftrightarrow (p \wedge r)$.

Λύση.

(i)

p	q	$p \leftrightarrow q$	$\neg(p \leftrightarrow q)$	$\neg p$	$\neg q$	$\neg p \leftrightarrow \neg q$
1	1	1	0	0	0	1
1	0	0	1	0	1	0
0	1	0	1	1	0	0
0	0	1	0	1	1	1

Άρα, οι προτάσεις $\neg(p \leftrightarrow q)$ και $\neg p \leftrightarrow \neg q$ **δεν** είναι λογικά ισοδύναμες. Στην πραγματικότητα η πρόταση $\neg p \leftrightarrow \neg q$ είναι λογικά ισοδύναμη με την $p \leftrightarrow q$.

(ii)

p	q	r	$q \leftrightarrow r$	$p \vee (q \leftrightarrow r)$	$p \vee q$	$p \vee r$	$(p \vee q) \leftrightarrow (p \vee r)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	1	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	1	1	0	0	1

Άρα, οι προτάσεις $p \vee (q \leftrightarrow r)$, $(p \vee q) \leftrightarrow (p \vee r)$ είναι λογικά ισοδύναμες.

(iii)

p	q	r	$q \leftrightarrow r$	$p \wedge (q \leftrightarrow r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \leftrightarrow (p \wedge r)$
1	1	1	1	1	1	1	1
1	1	0	0	0	1	0	0
1	0	1	0	0	0	1	0
1	0	0	1	1	0	0	1
0	1	1	1	0	0	0	1
0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	1
0	0	0	1	0	0	0	1

Άρα, οι προτάσεις $p \wedge (q \leftrightarrow r)$, $(p \wedge q) \leftrightarrow (p \wedge r)$ **δεν** είναι λογικά ισοδύναμες. □

Άσκηση 6.14 (Ιδιότητες λογικού συμπεράσματος).

α) Να δειχθεί ότι αν $\Sigma \models \varphi$ ή/και $\Sigma \models \psi$, τότε ισχύει ότι $\Sigma \models \varphi \vee \psi$.

> *Έστω ότι η $\varphi \vee \psi$ δεν είναι λογικό συμπέρασμα του Σ. Τότε υπάρχει ένα μοντέλο ν του Σ το οποίο δεν επαληθεύει την πρόταση $\varphi \vee \psi$, δηλαδή $\nu(\varphi \vee \psi) = 0 \Rightarrow \nu(\varphi) = \nu(\psi) = 0$.*
>
> *Άρα, ούτε η φ είναι λογικό συμπέρασμα του Σ, ούτε η ψ είναι λογικό συμπέρασμα του Σ, το οποίο είναι άτοπο.*
>
> *Άρα, η $\varphi \vee \psi$ είναι λογικό συμπέρασμα του Σ.*

β) Να δειχθεί ότι δεν ισχύει ότι $\Sigma \models \varphi \vee \psi \Rightarrow \Sigma \models \varphi$ *ή/και* $\Sigma \models \psi$.

Θα δώσουμε ένα αντιπαράδειγμα που δείχνει ότι δεν ισχύει αυτή η συνεπαγωγή.

Θα βρούμε ένα σύνολο προτάσεων Σ *και δύο προτάσεις* φ, ψ *που έχουν τις εξής ιδιότητες:*

Κάθε μοντέλο του Σ *να επαληθεύει την* $\varphi \vee \psi$.

Υπάρχει ένα μοντέλο του Σ *που δεν επαληθεύει την* φ.

Υπάρχει ένα (άλλο) του Σ *που δεν επαληθεύει την* ψ.

p	q	Σ	φ	ψ
1	1	1	1	0
1	0	1	0	1
0	1	0	-	-
0	0	0	-	-

Αν επιλέξουμε $\Sigma = \{p \vee q, p \vee \neg q\}$, $\varphi = p \wedge q$ *και* $\psi = \neg(p \to q)$

τότε ισχύει ότι $\Sigma \models \varphi \vee \psi$, *ενώ δεν ισχύει καμία από τις προτάσεις* $\Sigma \models \varphi$ *και* $\Sigma \models \psi$.

Άσκηση 6.15. *Να εξετασθεί ποιες από τις επόμενες προτάσεις είναι αληθείς ή ψευδείς. (Να αιτιολογηθούν οι απαντήσεις.)*

(i) Το σύνολο P *είναι ικανοποιήσιμο.*

(ii) Το σύνολο P_0 *είναι ικανοποιήσιμο.*

(iii) Το σύνολο P'_0 *που περιέχει τις αρνήσεις των ατόμων δεν είναι ικανοποιήσιμο.*

(iv) Αν Σ *είναι ικανοποιήσιμο, τότε περιέχει μόνο ταυτολογίες.*

(v) Αν Σ_1, Σ_2 *είναι ικανοποιήσιμα, τότε το σύνολο* $\Sigma_1 \cup \Sigma_2$ *είναι ικανοποιήσιμο.*

(vi) Αν Σ_1, Σ_2 *είναι ικανοποιήσιμα, τότε το σύνολο* $\Sigma_1 \cup \Sigma_2$ *δεν είναι ικανοποιήσιμο.*

(vii) Αν Σ *είναι ικανοποιήσιμο, τότε το σύνολο* Σ' *που περιέχει τις αρνήσεις όλων των προτάσεων του* Σ *είναι επίσης ικανοποιήσιμο.*

(viii) Αν Σ *είναι ικανοποιήσιμο και* $\Sigma \models \varphi$, *τότε το σύνολο* $\Sigma \cup \{\varphi\}$ *είναι ικανοποιήσιμο.*

(ix) Αν $\Sigma \models \varphi$, *τότε το σύνολο* $\Sigma \cup \{\varphi\}$ *είναι ικανοποιήσιμο.*

(x) Αν $\Sigma \models (\varphi \vee \psi)$, *τότε* $\Sigma \models \varphi$ *ή* $\Sigma \models \psi$.

(xi) Αν $\Sigma \models (\varphi \wedge \psi)$, *τότε* $\Sigma \models \varphi$ *και* $\Sigma \models \psi$.

Λύση.

(i) Ψευδής. Το P περιέχει και αντιλογίες.

(ii) Αληθής. Η εκτίμηση ν με $\nu(p) = 1$ για κάθε $p \in P_0$ είναι μοντέλο του P_0.

(iii) Ψευδής. Η εκτίμηση ν με $\nu(p) = 0$ για κάθε $p \in P_0$ είναι μοντέλο του P'_0.

(iv) Ψευδής. Το $\Sigma = \{p\}$ είναι ικανοποιήσιμο, αλλά η πρόταση p δεν είναι ταυτολογία.

(v) Ψευδής. Για παράδειγμα, αν $\Sigma_1 = \{p\}$, $\Sigma_2 = \{\neg p\}$, τότε Σ_1, Σ_2 ικανοποιήσιμα, αλλά $\Sigma_1 \cup \Sigma_2$ μη ικανοποιήσιμο.

(vi) Ψευδής. Για παράδειγμα, αν $\Sigma_1 = \{p\}$, $\Sigma_2 = \{q\}$, τότε Σ_1, Σ_2 ικανοποιήσιμα και $\Sigma_1 \cup \Sigma_2 = \{p, q\}$ είναι επίσης ικανοποιήσιμο.

(vii) Ψευδής. Για παράδειγμα, αν $\Sigma = \{p \vee \neg p\}$, τότε Σ είναι ικανοποιήσιμο, αλλά $\Sigma' = \{\neg(p \vee \neg p)\}$ είναι μη ικανοποιήσιμο.

(viii) Αληθής. Αφού Σ είναι ικανοποιήσιμο υπάρχει εκτίμηση ν ώστε $\nu \models \Sigma$. Επίσης, αφού φ είναι λογικό συμπέρασμα του Σ για κάθε εκτίμηση ν με $\nu \models \Sigma$ ισχύει ότι $\nu \models \varphi$.

Άρα $\nu \models \Sigma \cup \{\varphi\}$. Άρα, το σύνολο $\Sigma \cup \{\phi\}$ είναι ικανοποιήσιμο.

(ix) Ψευδής. Αν το Σ είναι μη ικανοποιήσιμο, τότε $\Sigma \models \varphi$ για κάθε $\varphi \in P$. Όμως, προφανώς, το $\Sigma \cup \{\varphi\}$ είναι μη ικανοποιήσιμο.

(x) Ψευδής. Για παράδειγμα, αν $\Sigma = \{p \vee q\}$, $\varphi = p$, $\psi = q$, τότε υπάρχουν τρεις εκτιμήσεις ν που ικανοποιούν το Σ:

1. $\nu(p) = \nu(q) = 1$,
2. $\nu(p) = 1$, $\nu(q) = 0$,
3. $\nu(p) = 0$, $\nu(q) = 1$.

Προφανώς, $\Sigma \models p \vee q$. Όμως, $\Sigma \not\models p$, αφού για την εκτίμηση 3. έπεται ότι $\nu \models \Sigma$ ενώ $\nu \not\models p$, επίσης $\Sigma \not\models q$, αφού για την εκτίμηση 2. έπεται ότι $\nu \models \Sigma$, ενώ $\nu \not\models q$.

(xi) Αληθής. Έστω $\Sigma \models (\varphi \wedge \psi)$.

Αν Σ αντιφατικό, τότε $\Sigma \models \varphi$ και $\Sigma \models \psi$.

Αν Σ ικανοποιήσιμο, τότε για κάθε μοντέλο ν του Σ ισχύει ότι $\nu(\varphi \wedge \psi) = 1$, δηλαδή $\nu(\varphi) = 1$ και $\nu(\psi) = 1$, δηλαδή $\Sigma \models \varphi$ και $\Sigma \models \psi$. □

6.3.2 Ασκήσεις προς επίλυση

1) Να ελεγχθεί με πίνακες αληθείας ποιές από τις παρακάτω προτάσεις είναι ταυτολογίες:

   i) $\varphi \to ((\psi \to \sigma) \to ((\varphi \to \psi) \to (\varphi \to \sigma)))$.

   ii) $(\varphi \to \neg\varphi) \leftrightarrow \neg\varphi$.

   iii) $(\varphi \to (\psi \to \sigma)) \leftrightarrow (\varphi \wedge \psi \to \sigma)$.

   iv) $\neg\varphi \to (\varphi \to \psi)$.

   v) $(\varphi \to \psi) \to ((\omega \vee \varphi) \to (\omega \vee \psi))$.

   vi) $((\varphi \to \psi) \to \varphi) \to \varphi$.

2) Δοθέντος ότι οι προτάσεις φ και $\varphi \to \psi$ είναι ταυτολογίες, να αποδειχθεί ότι και η πρόταση ψ είναι επίσης ταυτολογία.

3) Να δειχθεί ότι η πρόταση φ είναι ικανοποιήσιμη αν και μόνο αν η πρόταση $\neg\varphi$ δεν είναι ταυτολογία

4) Να βρεθούν εκτιμήσεις για τις οποίες οι παρακάτω προτάσεις είναι ψευδείς:

   i) $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \vee (u \wedge v) \vee (u \wedge w) \vee (v \wedge w) \vee (\neg x \wedge \neg u)$.

   ii) $((x \vee y) \wedge (y \vee z) \wedge (z \vee x)) \to (x \wedge y \wedge z)$.

   iii) $(x \vee y) \to ((\neg x \wedge y) \vee (x \wedge \neg y))$.

5) Έστω $\Sigma = \{\neg(q \to (p \vee r)), (p \to q) \wedge q\}$.

   i) Να βρεθούν όλα τα μοντέλα του συνόλου Σ.

   ii) Να εξετασθεί αν η πρόταση $p \to r$ είναι λογικό συμπέρασμα του Σ.

6) Χρησιμοποιώντας την Πρόταση της Αντικατάστασης και τις βασικές ισοδυναμίες να απλοποιηθούν όσο είναι δυνατό οι προτάσεις:

   α) $(p_1 \wedge ((p_1 \wedge p_2) \vee (p_1 \wedge \neg p_2))) \vee \neg(p_3 \vee \neg p_1)$.

   β) $((\varphi \vee \sigma) \wedge (\sigma \to \varphi)) \vee ((\psi \wedge \omega) \vee \neg(\psi \to \omega))$.

   γ) $(\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.

7) Να δειχθεί ότι για κάθε εκτίμηση ν ισχύουν τα παρακάτω:

   α) $\nu(\varphi \wedge \psi) = \nu(\varphi) \cdot \nu(\psi)$.

   β) $\nu(\varphi \vee \psi) = \nu(\varphi) + \nu(\psi) - \nu(\varphi) \cdot \nu(\psi)$.

   γ) $\nu(\neg\varphi) = 1 - \nu(\varphi)$.

   δ) $\nu(\varphi \to \psi) = 1 - \nu(\varphi) + \nu(\varphi) \cdot \nu(\psi)$.

   ε) $\nu(\varphi \leftrightarrow \psi) = 1 - |\nu(\varphi) - \nu(\psi)|$.

8) Ποιές από τις παρακάτω ισοδυναμίες ισχύουν;

   α) $\Sigma \models \varphi \vee \psi \Leftrightarrow \Sigma \models \varphi$ ή $\Sigma \models \psi$.

   β) $\Sigma \models \varphi \wedge \psi \Leftrightarrow \Sigma \models \varphi$ και $\Sigma \models \psi$.

γ) $\Sigma \models \varphi \to \psi \Leftrightarrow \Sigma \cup \{\varphi\} \models \psi$.

9) Έστω Σ ένα ικανοποιήσιμο σύνολο προτάσεων και $\varphi \in P$. Να δειχθεί ότι ένα τουλάχιστον από τα σύνολα $\Sigma \cup \{\varphi\}$, $\Sigma \cup \{\neg\varphi\}$ είναι επίσης ικανοποιήσιμο.

10) Έστω $\Sigma_1 = \{\varphi_1, \varphi_2, \varphi_3\}$ και $\Sigma_2 = \{\psi_1, \psi_2\}$ δύο ικανοποιήσιμα σύνολα προτάσεων. Αν το σύνολο $\Sigma_1 \cup \Sigma_2$ δεν είναι ικανοποιήσιμο, να βρεθεί πρόταση φ τέτοια ώστε $\Sigma_1 \models \varphi$ και $\Sigma_2 \models \neg\varphi$.

11) Οι A, B, C είναι ύποπτοι για φόνο. Ο A λέει: "Δεν τον σκότωσα εγώ. Το θύμα ήταν παλιός γνώριμος του B αλλά ο C τον μισούσε". Ο B λέει: "Δεν τον σκότωσα εγώ. Ούτε καν τον ήξερα. Εξ άλλου έλειπα από την πόλη αυτή την εβδομάδα". Ο C λέει: "Δεν τον σκότωσα εγώ. Είδα τους A και B εκείνη την ημέρα μαζί με το θύμα. Κάποιος από αυτούς είναι ο δράστης". Υποθέτοντας ότι οι δύο αθώοι λένε την αλήθεια ενώ ο ένοχος λέει ψέμματα, ποιός είναι ο ένοχος; (Να συγκριθούν οι ισχυρισμοί ανά δύο και να βρεθεί ποιός ψεύδεται.)

12) Να δειχθεί ότι τα παρακάτω είναι ισοδύναμα:

α) $\{\varphi_1, \varphi_2, \ldots, \varphi_n\} \models \varphi$.

β) $\models \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n \to \varphi$.

γ) $\models \varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \varphi)\cdots))$.

13) Έστω φ^* η πρόταση που προκύπτει από τη φ αντικαθιστώντας κάθε άτομο p της φ με την άρνησή του $\neg p$. Να δοθεί ο επαγωγικός ορισμός της φ^*.

14) Έστω μια πρόταση φ η οποία δεν περιέχει άλλους συνδέσμους εκτός από $\leftrightarrow$. Να δειχθεί ότι η φ είναι ταυτολογία αν και μόνο αν κάθε κάθε άτομο p έχει άρτιο αριθμό εμφανίσεων στην φ.

15) Έστω μια πρόταση φ η οποία δεν περιέχει άλλους συνδέσμους εκτός από $\leftrightarrow$ και $\neg$. Να δειχθεί ότι η φ είναι ταυτολογία αν και μόνο αν ο αριθμός των εμφανίσεων του συνδέσμου $\neg$ στην φ είναι άρτιος και κάθε άτομο p έχει άρτιο αριθμό εμφανίσεων στην φ.

16) Να απλοποιηθούν οι προτάσεις:

α) $(\varphi \to \psi) \wedge \varphi$.

β) $(\varphi \to \psi) \vee \neg\varphi$.

γ) $(\varphi \to \psi) \to \varphi$.

δ) $\varphi \to (\varphi \wedge \psi)$.

ε) $((\varphi \to \psi) \to \sigma) \vee ((\sigma \to \varphi) \to \psi)$.

17) Να δειχθεί ότι οι παρακάτω προτάσεις είναι ικανοποιήσιμες:

α) $\neg(p \to \neg p)$.

β) $((p \to q) \to (q \to p))$.

γ) $((q \to (p \wedge r)) \wedge \neg((p \vee r) \to q))$.

18) Να εξετασθεί ποιά από τα παρακάτω σύνολα προτάσεων είναι ικανοποιήσιμα:

α) Το $\{p_1, p_1 \to p_2, \neg p_2\}$.

β) Το $\{p_n \to p_{n+1} : n \in \mathbb{N}\}$.

γ) Το $\{p \wedge q, r \to \neg q, r \vee \neg p, p \vee q \vee r\}$.

δ) Το $\{p \to q, q \to r, r \to s, s \to \neg p, \neg p \to t, t \to w, w \to p\}$.

ε) Το $\{p \wedge r, \neg p \vee q, q \to s, s \to w, \neg w \to (p \vee r), p \vee s\}$.

19) Για τα σύνολα προτάσεων $\Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \Sigma_5, \Sigma_6, \Sigma_7, \Sigma_8$ ισχύουν οι παρακάτω ιδιότητες:

Κάθε εκτίμηση ν ικανοποιεί το σύνολο Σ_1.

Υπάρχει εκτίμηση ν που ικανοποιεί κάθε πρόταση του Σ_2.

Υπάρχει εκτίμηση ν για την οποία κάθε πρόταση του Σ_3 είναι ψευδής.

Δεν υπάρχει εκτίμηση ν που ικανοποιεί κάθε πρόταση του Σ_4.

Για κάθε πρόταση φ στο Σ_5 υπάρχει εκτίμηση ν που την ικανοποιεί.

Για κάθε πρόταση φ στο Σ_6 υπάρχει εκτίμηση ν που δεν την ικανοποιεί.

Για κάθε εκτίμηση ν υπάρχει πρόταση του Σ_7 που ικανοποιείται από την ν.

Για κάθε εκτίμηση ν υπάρχει πρόταση του Σ_8 που δεν ικανοποιείται από την ν.

Να εξετασθεί ποιες από τις παρακάτω προτάσεις που αναφέρονται σε κάθε ένα από τα σύνολα $\Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \Sigma_5, \Sigma_6, \Sigma_7, \Sigma_8$ είναι αληθείς, ή ψευδείς, ή δεν γνωρίζουμε αρκετές πληροφορίες για να μπορούμε να αποφανθούμε για την τιμή αληθείας τους.

i) Το σύνολο είναι ικανοποιήσιμο.

ii) Το σύνολο είναι μη ικανοποιήσιμο.

iii) Το σύνολο περιέχει τουλάχιστον μια ταυτολογία.

iv) Το σύνολο δεν περιέχει ταυτολογίες.

v) Το σύνολο περιέχει μόνο ταυτολογίες.

vi) Το σύνολο περιέχει τουλάχιστον μια αντιλογία.

vii) Το σύνολο δεν περιέχει αντιλογίες.

viii) Το σύνολο περιέχει μόνο αντιλογίες.

6.4 Προβλήματα ικανοποιησιμότητας

Δίδονται τα σύνολα

$$\Sigma_1 = \{p_1 \vee p_2 \vee p_3, p_1 \vee \neg p_2 \vee \neg p_3, \neg p_1 \vee p_2 \vee \neg p_3\}$$
$$\Sigma_2 = \{p_1 \vee p_2 \vee p_3, p_1 \vee \neg p_2, p_2 \vee \neg p_3, p_3 \vee \neg p_1, \neg p_1 \vee \neg p_2 \vee \neg p_3\}$$

Είναι κάποιο από τα σύνολα Σ_1 και Σ_2 ικανοποιήσιμο, δηλαδή υπάρχουν εκτιμήσεις ν_1, ν_2 ώστε $\nu_1 \models \Sigma_1$ ή $\nu_2 \models \Sigma_2$;

Εύκολα, μπορούμε να ελέγξουμε ότι η εκτίμηση ν_1 με $\nu_1(p_1) = 1$, $\nu_1(p_2) = \nu_1(p_3) = 0$ ικανοποιεί το σύνολο Σ_1.

Αντίθετα, καμιά εκτίμηση δεν ικανοποιεί το σύνολο Σ_2, διότι από τις προτάσεις $p_1 \vee \neg p_2$, $p_2 \vee \neg p_3$, $p_3 \vee \neg p_1$ έπεται ότι για κάθε εκτίμηση ν_2 που ικανοποιεί το Σ_2 ισχύει ότι

$$\nu_2(p_1) = \nu_2(p_2) = \nu_2(p_3),$$

επομένως, σε κάθε περίπτωση έχουμε αντίστοιχα ότι

$$\nu_2(p_1 \vee p_2 \vee p_3) = 0 \qquad \text{ή} \qquad \nu_2(\neg p_1 \vee \neg p_2 \vee \neg p_3) = 0.$$

Στην γενική του μορφή, το πρόβλημα της ικανοποιησιμότητας ορίζεται ως εξής:

Πρόβλημα Ικανοποιησιμότητας (πρόβλημα SAT) Δίδεται ένα σύνολο προτάσεων Σ και ζητείται να δοθεί μια εκτίμηση ν που ικανοποιεί το Σ, ή η απάντηση ότι δεν υπάρχει τέτοια εκτίμηση.

Το πρόβλημα της ικανοποιησιμότητας είναι ένα από τα σημαντικότερα προβλήματα της Λογικής, με πολλές εφαρμογές στην Πληροφορική.

Η προφανής μέθοδος λύσης του είναι η *εξαντλητική εξέταση* όλων των δυνατών εκτιμήσεων, π.χ. με την βοήθεια των πινάκων αληθείας. Όμως, αν στο Σ περιέχονται n διαφορετικά άτομα, τότε ο συνολικός αριθμός των δυνατών εκτιμήσεων ισούται με 2^n (διότι για κάθε άτομο έχουμε ακριβώς δύο επιλογές). Ακόμα και ένας υπολογιστής που εξετάζει 10^{20} περιπτώσεις το δευτερόλεπτο, για σύνολα που περιέχουν 100 άτομα θα έπρεπε να εξετάσει 2^{100} περιπτώσεις, το οποίο θα απαιτούσε περίπου 4 αιώνες!

Φυσικά, αντί να δοκιμάσουμε όλες τις περιπτώσεις, είναι καλύτερο πρώτα να μελετήσουμε τις προτάσεις του Σ, ελπίζοντας ότι θα μπορέσουμε να βρούμε κανόνες που πρέπει να ικανοποιούν όλες οι πιθανές εκτιμήσεις που ικανοποιούν το Σ, όπως στο παράδειγμα με το σύνολο Σ_2.

Δυστυχώς, στην γενική του μορφή το πρόβλημα της ικανοποιησιμότητας δεν έχει αντιμετωπισθεί με κάποιο αποδοτικό τρόπο. Μάλιστα, ανήκει σε μια κατηγορία "δύσκολων" προβλημάτων της Πληροφορικής, τα οποία χαρακτηρίζονται με τον όρο **NP-complete** προβλήματα.

Το πρόβλημα της ικανοποιησιμότητας είναι σημαντικό διότι:

1. Ο έλεγχος σχετικά με τις βασικές έννοιες της ταυτολογίας, του λογικού συμπεράσματος και της λογικής ισοδυναμίας μπορούν να αναχθούν σε προβλήματα ικανοποιησιμότητας. Συγκεκριμένα:

   - Για να δείξουμε ότι μια πρόταση φ είναι ταυτολογία, αρκεί να δείξουμε ότι η πρόταση $\neg\varphi$ είναι μη ικανοποιήσιμη.
   - Για να δείξουμε ότι οι προτάσεις φ και ψ είναι λογικά ισοδύναμες, αρκεί να δείξουμε ότι η πρόταση $\varphi \leftrightarrow \psi$ είναι ταυτολογία. Άρα, ισοδύναμα, αρκεί να δείξουμε ότι η πρόταση $\neg(\varphi \leftrightarrow \psi)$ είναι μη ικανοποιήσιμη.

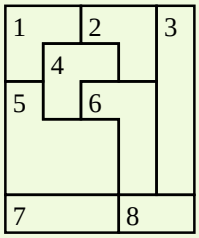
- Για να δείξουμε ότι η πρόταση φ είναι λογικό συμπέρασμα του Σ, αρκεί να δείξουμε ότι το σύνολο $\Sigma \cup \{\neg\varphi\}$ είναι μη ικανοποιήσιμο.

2. Πολλά αλγοριθμικά προβλήματα μπορούν να μοντελοποιηθούν ως προβλήματα ικανοποιησιμότητας. Επομένως, αν βρεθούν γρήγοροι αλγόριθμοι για την επίλυση του προβλήματος ικανοποιησιμότητας, με την βοήθεια αυτών θα λυθούν αποδοτικά και όλα αυτά τα αλγοριθμικά προβλήματα. Παρακάτω δίδονται μερικά παραδείγματα τέτοιων μοντελοποιήσεων.

Παραδείγματα μοντελοποίησης ως προβλήματα ικανοποιησιμότητας.

Παράδειγμα 6.4.1 (Πρόβλημα χρωματισμού).

Σε κάθε μια από τις 8 περιοχές του διπλανού σχήματος να τοποθετηθεί ένας από τους αριθμούς 1, 2, 3 έτσι ώστε οι γειτονικές περιοχές να έχουν διαφορετικούς αριθμούς. (Δύο περιοχές θεωρούνται γειτονικές αν το κοινό τους σύνορο περιέχει άπειρα σημεία)



Λύση. Για κάθε περιοχή i, $i \in [8]$ θεωρούμε τα άτομα:
p_{i1}: Η περιοχή i έχει τον αριθμό 1.
p_{i2}: Η περιοχή i έχει τον αριθμό 2.
p_{i3}: Η περιοχή i έχει τον αριθμό 3.
Συνολικά, για τις 8 περιοχές, χρειαζόμαστε $3 \cdot 8 = 24$ άτομα.
Οι περιορισμοί του προβλήματος μπορούν να μοντελοποιηθούν από τις παρακάτω προτάσεις:

1. Σε κάθε περιοχή πρέπει να τοποθετηθεί ένας τουλάχιστον αριθμός. Για κάθε περιοχή i, $i \in [8]$, πρέπει να ισχύει η πρόταση: $p_{i1} \vee p_{i2} \vee p_{i3}$.

   - $p_{11} \vee p_{12} \vee p_{13}$
   - $p_{21} \vee p_{22} \vee p_{23}$
   - $p_{31} \vee p_{32} \vee p_{33}$
   - $p_{41} \vee p_{42} \vee p_{43}$
   - $p_{51} \vee p_{52} \vee p_{53}$
   - $p_{61} \vee p_{62} \vee p_{63}$
   - $p_{71} \vee p_{72} \vee p_{73}$
   - $p_{81} \vee p_{82} \vee p_{83}$

2. (Προαιρετικά) Σε κάθε περιοχή πρέπει να τοποθετηθεί το πολύ ένας αριθμός. Για κάθε περιοχή i, $i \in [8]$, πρέπει να ισχύουν οι προτάσεις: $\neg p_{i1} \vee \neg p_{i2}, \neg p_{i1} \vee \neg p_{i3}, \neg p_{i2} \vee \neg p_{i3}$.

   - $\neg p_{11} \vee \neg p_{12}, \neg p_{11} \vee \neg p_{13}, \neg p_{12} \vee \neg p_{13}$
   - $\neg p_{21} \vee \neg p_{22}, \neg p_{21} \vee \neg p_{23}, \neg p_{22} \vee \neg p_{23}$
   - $\neg p_{31} \vee \neg p_{32}, \neg p_{31} \vee \neg p_{33}, \neg p_{32} \vee \neg p_{33}$
   - $\neg p_{41} \vee \neg p_{42}, \neg p_{41} \vee \neg p_{43}, \neg p_{42} \vee \neg p_{43}$
   - $\neg p_{51} \vee \neg p_{52}, \neg p_{51} \vee \neg p_{53}, \neg p_{52} \vee \neg p_{53}$
   - $\neg p_{61} \vee \neg p_{62}, \neg p_{61} \vee \neg p_{63}, \neg p_{62} \vee \neg p_{63}$
   - $\neg p_{71} \vee \neg p_{72}, \neg p_{71} \vee \neg p_{73}, \neg p_{72} \vee \neg p_{73}$
   - $\neg p_{81} \vee \neg p_{82}, \neg p_{81} \vee \neg p_{83}, \neg p_{82} \vee \neg p_{83}$

3. Αν οι περιοχές i, j είναι γειτονικές δεν επιτρέπεται να έχουν τον ίδιο αριθμό, οπότε πρέπει να ισχύουν οι προτάσεις: $\neg p_{i1} \vee \neg p_{j1}$, $\neg p_{i2} \vee \neg p_{j2}$, $\neg p_{i3} \vee \neg p_{j3}$.

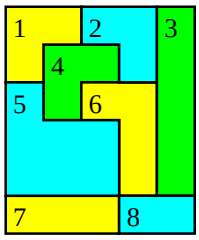
- $\neg p_{11} \vee \neg p_{21}$, $\neg p_{12} \vee \neg p_{22}$, $\neg p_{13} \vee \neg p_{23}$
- $\neg p_{11} \vee \neg p_{41}$, $\neg p_{12} \vee \neg p_{42}$, $\neg p_{13} \vee \neg p_{43}$
- $\neg p_{11} \vee \neg p_{51}$, $\neg p_{12} \vee \neg p_{52}$, $\neg p_{13} \vee \neg p_{53}$
- $\neg p_{21} \vee \neg p_{31}$, $\neg p_{22} \vee \neg p_{32}$, $\neg p_{23} \vee \neg p_{33}$
- $\neg p_{21} \vee \neg p_{41}$, $\neg p_{22} \vee \neg p_{42}$, $\neg p_{23} \vee \neg p_{43}$
- $\neg p_{21} \vee \neg p_{61}$, $\neg p_{22} \vee \neg p_{62}$, $\neg p_{23} \vee \neg p_{63}$
- $\neg p_{31} \vee \neg p_{61}$, $\neg p_{32} \vee \neg p_{62}$, $\neg p_{33} \vee \neg p_{63}$
- $\neg p_{31} \vee \neg p_{81}$, $\neg p_{32} \vee \neg p_{82}$, $\neg p_{33} \vee \neg p_{83}$
- $\neg p_{41} \vee \neg p_{51}$, $\neg p_{42} \vee \neg p_{52}$, $\neg p_{43} \vee \neg p_{53}$
- $\neg p_{41} \vee \neg p_{61}$, $\neg p_{42} \vee \neg p_{62}$, $\neg p_{43} \vee \neg p_{63}$
- $\neg p_{51} \vee \neg p_{61}$, $\neg p_{52} \vee \neg p_{62}$, $\neg p_{53} \vee \neg p_{63}$
- $\neg p_{51} \vee \neg p_{71}$, $\neg p_{52} \vee \neg p_{72}$, $\neg p_{53} \vee \neg p_{73}$
- $\neg p_{61} \vee \neg p_{81}$, $\neg p_{62} \vee \neg p_{82}$, $\neg p_{63} \vee \neg p_{83}$
- $\neg p_{71} \vee \neg p_{81}$, $\neg p_{72} \vee \neg p_{82}$, $\neg p_{73} \vee \neg p_{83}$

Το πρόβλημα έχει λύση αν και μόνο αν το σύνολο Σ που αποτελείται από τις προηγούμενες $8 + 24 + 42 = 74$ προτάσεις (οι οποίες συνολικά περιέχουν 24 διαφορετικά άτομα) είναι ικανοποιήσιμο. Τα μοντέλα του Σ αντιστοιχούν στις λύσεις του προβλήματος τοποθέτησης.

Ένα τέτοιο μοντέλο του Σ είναι η εκτίμηση ν για την οποία όλα τα άτομα, εκτός από τα επόμενα 8, είναι ψευδή:

$$p_{11}, p_{22}, p_{33}, p_{43}, p_{52}, p_{61}, p_{71}, p_{82}$$

Το μοντέλο αυτό αντιστοιχεί στην διπλανή λύση όπου
οι περιοχές που περιέχουν τον αριθμό 1 είναι κίτρινες
οι περιοχές που περιέχουν τον αριθμό 2 είναι γαλάζιες
οι περιοχές που περιέχουν τον αριθμό 3 είναι πράσινες.



□

Παράδειγμα 6.4.2 (Πρόβλημα κλίκας).

Σε ένα κοινωνικό δίκτυο συμμετέχουν (μεταξύ πολλών άλλων) 8 συγκεκριμένοι χρήστες. Ο καθένας έχει μια λίστα από φίλους στην οποία περιέχονται ορισμένοι από αυτούς τους χρήστες. Συγκεκριμένα, οι λίστες φίλων των 8 χρηστών εμφανίζονται στον διπλανό πίνακα.
Να βρεθεί, αν υπάρχει, μια ομάδα που αποτελείται από τουλάχιστον 3 χρήστες οι οποίοι ανά δύο είναι φίλοι.

Χρήστης	*Λίστα φίλων*
1	2, 7, 8
2	1, 3, 4, 8
3	2, 4
4	2, 3, 5
5	4, 7, 8
6	8
7	1, 5
8	1, 2, 5, 6

Απόδειξη. Για κάθε χρήστη i, $i \in [8]$ θεωρούμε τα άτομα:
p_i: Ο χρήστης i συμμετέχει στην ομάδα.
Συνολικά, για τους 8 χρήστες, χρειαζόμαστε 8 άτομα.
Οι περιορισμοί του προβλήματος μπορούν να μοντελοποιηθούν από τις παρακάτω προτάσεις:

1. Πρέπει να επιλέξουμε τουλάχιστον 3 χρήστες. Ισοδύναμα, από κάθε (δυνατή) εξάδα χρηστών επιλέγουμε τουλάχιστον 1 χρήστη. Πράγματι, αν υπάρχει εξάδα από την οποία δεν επιλέγουμε κανένα χρήστη, τότε έχουμε επιλέξει το πολύ 2 χρήστες στην ομάδα. Αντίστροφα, αν επιλέξουμε τουλάχιστον 3 χρήστες, τότε σε κάθε εξάδα χρηστών περιέχεται τουλάχιστον 1 από αυτούς.

   Υπάρχουν $\binom{8}{6} = 28$ τέτοιες προτάσεις που πρέπει να ισχύουν:

- $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6$
- $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_7$
- $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_8$
- $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_6 \vee p_7$
- $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_6 \vee p_8$
- $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_7 \vee p_8$
- $p_1 \vee p_2 \vee p_3 \vee p_5 \vee p_6 \vee p_7$
- $p_1 \vee p_2 \vee p_3 \vee p_5 \vee p_6 \vee p_8$
- $p_1 \vee p_2 \vee p_3 \vee p_5 \vee p_7 \vee p_8$
- $p_1 \vee p_2 \vee p_3 \vee p_6 \vee p_7 \vee p_8$
- $p_1 \vee p_2 \vee p_4 \vee p_5 \vee p_6 \vee p_7$
- $p_1 \vee p_2 \vee p_4 \vee p_5 \vee p_6 \vee p_8$
- $p_1 \vee p_2 \vee p_4 \vee p_5 \vee p_7 \vee p_8$
- $p_1 \vee p_2 \vee p_4 \vee p_6 \vee p_7 \vee p_8$
- $p_1 \vee p_2 \vee p_5 \vee p_6 \vee p_7 \vee p_8$
- $p_1 \vee p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_7$
- $p_1 \vee p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_8$
- $p_1 \vee p_3 \vee p_4 \vee p_5 \vee p_7 \vee p_8$
- $p_1 \vee p_3 \vee p_4 \vee p_6 \vee p_7 \vee p_8$
- $p_1 \vee p_3 \vee p_5 \vee p_6 \vee p_7 \vee p_8$
- $p_1 \vee p_4 \vee p_5 \vee p_6 \vee p_7 \vee p_8$
- $p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_7$
- $p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_8$
- $p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_7 \vee p_8$
- $p_2 \vee p_3 \vee p_4 \vee p_6 \vee p_7 \vee p_8$
- $p_2 \vee p_3 \vee p_5 \vee p_6 \vee p_7 \vee p_8$
- $p_2 \vee p_4 \vee p_5 \vee p_6 \vee p_7 \vee p_8$
- $p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_7 \vee p_8$

2. Αν δύο χρήστες δεν είναι φίλοι, τότε δεν μπορούν να επιλεγούν και οι δύο στην ομάδα. Συγκεκριμένα, αν οι χρήστες i, j δεν είναι φίλοι πρέπει να ισχύει η πρόταση $\neg p_i \vee \neg p_j$.

- (1): $\neg p_1 \vee \neg p_3$, $\neg p_1 \vee \neg p_4$, $\neg p_1 \vee \neg p_5$, $\neg p_1 \vee \neg p_6$
- (2): $\neg p_2 \vee \neg p_5$, $\neg p_2 \vee \neg p_6$, $\neg p_2 \vee \neg p_7$
- (3): $\neg p_3 \vee \neg p_5$, $\neg p_3 \vee \neg p_6$, $\neg p_3 \vee \neg p_8$
- (4): $\neg p_4 \vee \neg p_6$, $\neg p_4 \vee \neg p_7$, $\neg p_4 \vee \neg p_8$
- (5): $\neg p_5 \vee \neg p_6$
- (6): $\neg p_6 \vee \neg p_7$
- (7): $\neg p_7 \vee \neg p_8$

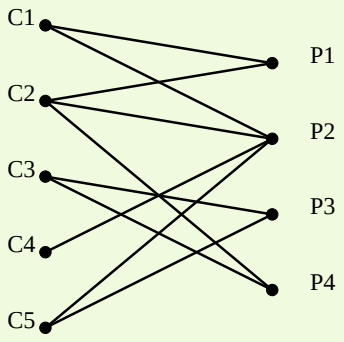
Το πρόβλημα έχει λύση αν και μόνο αν το σύνολο Σ που αποτελείται από τις προηγούμενες $28 + 16 = 44$ προτάσεις (οι οποίες συνολικά περιέχουν 8 διαφορετικά άτομα) είναι ικανοποιήσιμο. Τα μοντέλα του Σ αντιστοιχούν στις λύσεις του προβλήματος επιλογής της ομάδας. Ένα τέτοιο μοντέλο του Σ είναι η εκτίμηση ν για την οποία

$$\nu(p_1) = \nu(p_2) = \nu(p_8) = 1, \qquad \nu(p_3) = \nu(p_4) = \nu(p_5) = \nu(p_6) = \nu(p_7) = 0.$$

Το μοντέλο αυτό αντιστοιχεί στην ομάδα που αποτελείται από τα άτομα $\{1, 2, 8\}$, τα οποία ανά δύο είναι φίλοι. □

Παράδειγμα 6.4.3 (Πρόβλημα αντιστοίχισης).

Σε ένα πρόγραμμα Πρακτικής Άσκησης είναι διαθέσιμες 4 θέσεις P_1, P_2, P_3, P_4 για τις οποίες υπάρχουν 5 υποψήφιοι C_1, C_2, C_3, C_4, C_5. Κάθε υποψήφιος έχει δηλώσει τις θέσεις για τις οποίες ενδιαφέρεται να αποσχοληθεί. Στο διπλανό σχήμα δίνονται οι επιλογές κάθε υποψήφιου. (Οι γραμμές δείχνουν τις θέσεις που προτιμά κάθε υποψήφιος.) Να βρεθεί ένας τρόπος ώστε να καλυφθούν όλες οι θέσεις σύμφωνα με τις προτιμήσεις των υποψηφίων. (Σε κάθε θέση μπορεί να απασχοληθεί το πολύ ένας υποψήφιος).



Λύση. Για κάθε θέση i, $i \in [4]$ και για κάθε υποψήφιο j, $j \in [5]$ και θεωρούμε τα άτομα:

p_{ij}: Ο υποψήφιος j θα απασχοληθεί στην θέση i.

Γενικά σε ένα τέτοιο πρόβλημα χρειαζόμαστε το πολύ $4 \cdot 5 = 20$ άτομα. Μπορούμε όμως να μειώσουμε τον αριθμό των ατόμων με βάση τις προτιμήσεις των υποψηφίων. Στο παρόν πρόβλημα χρειαζόμαστε $2 + 3 + 2 + 1 + 2 = 10$ άτομα.

Οι περιορισμοί του προβλήματος μπορούν να μοντελοποιηθούν από τις παρακάτω προτάσεις:

1. Σε κάθε θέση πρέπει να απασχοληθεί τουλάχιστον ένας υποψήφιος, (ο οποίος ενδιαφέρεται γι' αυτή). Συγκεκριμένα, αν για την θέση i ενδιαφέρονται οι υποψήφιοι a, b, ..., z τότε πρέπει πρέπει να ισχύει η πρόταση $p_{ia} \vee p_{ib} \vee \cdots \vee p_{iz}$.

   - (Θέση $P1$): $p_{11} \vee p_{12}$
   - (Θέση $P2$): $p_{21} \vee p_{22} \vee p_{24} \vee p_{25}$
   - (Θέση $P3$): $p_{33} \vee p_{35}$
   - (Θέση $P4$): $p_{42} \vee p_{43}$

2. Σε κάθε θέση πρέπει να απασχοληθεί το πολύ ένας υποψήφιος, (ο οποίος ενδιαφέρεται γι' αυτή). Συγκεκριμένα, αν για την θέση i ενδιαφέρονται περισσότεροι από ένας υποψήφιοι (και έστω A_i το σύνολο των υποψήφιων που ενδιαφέρονται για την θέση i) τότε πρέπει πρέπει να ισχύουν οι προτάσεις $\neg p_{ix} \vee \neg p_{iy}$ για κάθε $x, y \in A_i$ με $x < y$.

   - (Θέση $P1$): $\neg p_{11} \vee \neg p_{12}$
   - (Θέση $P2$): $\neg p_{21} \vee \neg p_{22}$, $\neg p_{21} \vee \neg p_{24}$, $\neg p_{21} \vee p_{25}$, $\neg p_{22} \vee \neg p_{24}$, $\neg p_{22} \vee \neg p_{25}$, $\neg p_{24} \vee \neg p_{25}$
   - (Θέση $P3$): $\neg p_{33} \vee \neg p_{35}$
   - (Θέση $P4$): $\neg p_{42} \vee \neg p_{43}$

3. Κάθε υποψήφιος μπορεί να απασχοληθεί σε μια το πολύ θέση, (από αυτές που τον ενδιαφέρουν). Συγκεκριμένα, αν ο υποψήφιος j ενδιαφέρεται για περισσότερες από μια θέσεις (και έστω B_j το σύνολο των θέσεων που ενδιαφέρουν τον υποψήφιο j) τότε πρέπει πρέπει να ισχύουν οι προτάσεις $\neg p_{xj} \vee \neg p_{yj}$ για κάθε $x, y \in B_j$ με $x < y$.

   - (Υποψήφιος C_1): $\neg p_{11} \vee \neg p_{21}$
   - (Υποψήφιος C_2): $\neg p_{12} \vee \neg p_{22}$, $\neg p_{12} \vee \neg p_{42}$, $\neg p_{22} \vee p_{42}$
   - (Υποψήφιος C_3): $\neg p_{33} \vee \neg p_{43}$
   - (Υποψήφιος C_4):
   - (Υποψήφιος C_5): $\neg p_{25} \vee \neg p_{35}$

Το πρόβλημα έχει λύση αν και μόνο αν το σύνολο Σ που αποτελείται από τις προηγούμενες $4+9+6 = 19$ προτάσεις (οι οποίες συνολικά περιέχουν 10 διαφορετικά άτομα) είναι ικανοποιήσιμο. Τα μοντέλα του Σ αντιστοιχούν στις λύσεις του προβλήματος αντιστοίχισης.

Ένα τέτοιο μοντέλο του Σ είναι η εκτίμηση v για την οποία:

$$v(p_{11}) = v(p_{24}) = v(p_{35}) = v(p_{43}) = 1$$

και τα υπόλοιπα 6 άτομα είναι ψευδή. Το μοντέλο αυτό αντιστοιχεί στην αντιστοίχιση $C_1 - P_1$, $C_4 - P_2$, $C_5 - P_3$ και $C_3 - P_4$. □

Παράδειγμα 6.4.4 (Πρόβλημα κάλυψης).
Σε ένα τεστ πιστοποίησης εξετάζεται η γνώση πάνω σε 9 ενότητες A, B, C, D, E, F, G, H, I. Οι ερωτήσεις του τεστ επιλέγονται από μια βάση ερωτήσεων. Κάθε ερώτηση καλύπτει ορισμένες από τις ενότητες και απαιτεί κατά μέσο όρο 10 λεπτά για να απαντηθεί. Στον διπλανό πίνακα φαίνονται οι ενότητες που εξετάζει κάθε ερώτηση της βάσης:
Να βρεθεί αν υπάρχει τρόπος να κατασκευασθεί ένα τεστ, που να διαρκεί κατά μέσο όρο 30 λεπτά και οι ερωτήσεις του να εξετάζουν και τις 9 ενότητες.

Ερώτηση	*Ενότητα*
1	*A, B, G*
2	*A, B, C, E*
3	*C, D, H*
4	*A, E, G, I*
5	*D, F, H*
6	*D, E, G*
7	*A, C, I*

Απόδειξη. Για κάθε ερώτηση i, $i \in [7]$ θεωρούμε τα άτομα:
p_i: Η ερώτηση i επιλέγεται για το τεστ.
Συνολικά, για τις 7 ερωτήσεις, χρειαζόμαστε 7 άτομα.
Οι περιορισμοί του προβλήματος μπορούν να μοντελοποιηθούν από τις παρακάτω προτάσεις:

1. Πρέπει να επιλέξουμε τουλάχιστον 3 ερωτήσεις. Ισοδύναμα, από κάθε (δυνατή) πεντάδα ερωτήσεων επιλέγουμε τουλάχιστον 1 ερώτηση. Πράγματι, αν υπάρχει πεντάδα από την οποία δεν επιλέγουμε καμία ερώτηση, τότε έχουμε επιλέξει το πολύ 2 ερωτήσεις για το τεστ. Αντίστροφα, αν επιλέξουμε τουλάχιστον 3 ερωτήσεις, τότε σε κάθε πεντάδα ερωτήσεων περιέχεται τουλάχιστον 1 από αυτές.

   Υπάρχουν $\binom{7}{5} = 21$ τέτοιες προτάσεις που πρέπει να ισχύουν:

   - $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5$
   - $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_6$
   - $p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_7$
   - $p_1 \vee p_2 \vee p_3 \vee p_5 \vee p_6$
   - $p_1 \vee p_2 \vee p_3 \vee p_5 \vee p_7$
   - $p_1 \vee p_2 \vee p_3 \vee p_6 \vee p_7$
   - $p_1 \vee p_2 \vee p_4 \vee p_5 \vee p_6$
   - $p_1 \vee p_2 \vee p_4 \vee p_5 \vee p_7$
   - $p_1 \vee p_2 \vee p_4 \vee p_6 \vee p_7$
   - $p_1 \vee p_2 \vee p_5 \vee p_6 \vee p_7$
   - $p_1 \vee p_3 \vee p_4 \vee p_5 \vee p_6$
   - $p_1 \vee p_3 \vee p_4 \vee p_5 \vee p_7$
   - $p_1 \vee p_3 \vee p_4 \vee p_6 \vee p_7$
   - $p_1 \vee p_3 \vee p_5 \vee p_6 \vee p_7$
   - $p_1 \vee p_4 \vee p_5 \vee p_6 \vee p_7$
   - $p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6$
   - $p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_7$
   - $p_2 \vee p_3 \vee p_4 \vee p_6 \vee p_7$
   - $p_2 \vee p_3 \vee p_5 \vee p_6 \vee p_7$
   - $p_2 \vee p_4 \vee p_5 \vee p_6 \vee p_7$
   - $p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_7$

2. Προκειμένου ο χρόνος απαντήσεων να είναι περίπου ίσος με 30 λεπτά δεν επιτρέπεται να επιλεγούν πάνω από 3 ερωτήσεις. Ισοδύναμα, σε κάθε τετράδα ερωτήσεων δεν μπορούν να επιλεγούν όλες οι ερωτήσεις της. Συγκεκριμένα, αν η τετράδα περιέχει τις ερωτήσεις i, j, k, r τότε πρέπει να ισχύει η πρόταση $\neg p_i \vee \neg p_j \vee \neg p_k \vee \neg p_r$.

   Υπάρχουν $\binom{7}{4} = 35$ τέτοιες προτάσεις που πρέπει να ισχύουν:

   - $\neg p_1 \vee \neg p_2 \vee \neg p_3 \vee \neg p_4$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_3 \vee \neg p_5$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_3 \vee \neg p_6$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_3 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_4 \vee \neg p_5$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_4 \vee \neg p_6$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_4 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_5 \vee \neg p_6$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_5 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_2 \vee \neg p_6 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_3 \vee \neg p_4 \vee \neg p_5$
   - $\neg p_1 \vee \neg p_3 \vee \neg p_4 \vee \neg p_6$
   - $\neg p_1 \vee \neg p_3 \vee \neg p_4 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_3 \vee \neg p_5 \vee \neg p_6$
   - $\neg p_1 \vee \neg p_3 \vee \neg p_5 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_3 \vee \neg p_6 \vee \neg p_7$
   - $\neg p_1 \vee \neg p_4 \vee \neg p_5 \vee \neg p_6$
   - $\neg p_1 \vee \neg p_4 \vee \neg p_5 \vee \neg p_7$

- $\neg p_1 \vee \neg p_4 \vee \neg p_6 \vee \neg p_7$
- $\neg p_1 \vee \neg p_5 \vee \neg p_6 \vee \neg p_7$
- $\neg p_2 \vee \neg p_3 \vee \neg p_4 \vee \neg p_5$
- $\neg p_2 \vee \neg p_3 \vee \neg p_4 \vee \neg p_6$
- $\neg p_2 \vee \neg p_3 \vee \neg p_4 \vee \neg p_7$
- $\neg p_2 \vee \neg p_3 \vee \neg p_5 \vee \neg p_6$
- $\neg p_2 \vee \neg p_3 \vee \neg p_5 \vee \neg p_7$
- $\neg p_2 \vee \neg p_3 \vee \neg p_6 \vee \neg p_7$
- $\neg p_2 \vee \neg p_4 \vee \neg p_5 \vee \neg p_6$
- $\neg p_2 \vee \neg p_4 \vee \neg p_5 \vee \neg p_7$
- $\neg p_2 \vee \neg p_4 \vee \neg p_6 \vee \neg p_7$
- $\neg p_2 \vee \neg p_5 \vee \neg p_6 \vee \neg p_7$
- $\neg p_3 \vee \neg p_4 \vee \neg p_5 \vee \neg p_6$
- $\neg p_3 \vee \neg p_4 \vee \neg p_5 \vee \neg p_7$
- $\neg p_3 \vee \neg p_4 \vee \neg p_6 \vee \neg p_7$
- $\neg p_3 \vee \neg p_5 \vee \neg p_6 \vee \neg p_7$
- $\neg p_4 \vee \neg p_5 \vee \neg p_6 \vee \neg p_7$

3. Κάθε μία από τις 9 ενότητες πρέπει να εξετάζεται από τουλάχιστον μια ερώτηση. Συγκεκριμένα, αν η ενότητα U εξετάζεται από τις ερωτήσεις x, y, …, z πρέπει να ισχύει η πρόταση $p_x \vee p_y \vee \cdots \vee p_z$.

- (Ενότητα A): $p_1 \vee p_2 \vee p_4 \vee p_7$
- (Ενότητα B): $p_1 \vee p_2$
- (Ενότητα C): $p_2 \vee p_3 \vee p_7$
- (Ενότητα D): $p_3 \vee p_5 \vee p_6$
- (Ενότητα E): $p_2 \vee p_4 \vee p_6$
- (Ενότητα F): p_5
- (Ενότητα G): $p_1 \vee p_4 \vee p_6$
- (Ενότητα H): $p_3 \vee p_5$
- (Ενότητα I): $p_4 \vee p_7$

Το πρόβλημα έχει λύση αν και μόνο αν το σύνολο Σ που αποτελείται από τις προηγούμενες $21+35+9 = 65$ προτάσεις (οι οποίες συνολικά περιέχουν 7 διαφορετικά άτομα) είναι ικανοποιήσιμο. Τα μοντέλα του Σ αντιστοιχούν στις λύσεις του προβλήματος κατασκευής του τεστ. Ένα τέτοιο μοντέλο του Σ (και μάλιστα μοναδικό) είναι η εκτίμηση ν για την οποία

$$\nu(p_2) = \nu(p_4) = \nu(p_5) = 1, \qquad \nu(p_1) = \nu(p_3) = \nu(p_6) = \nu(p_7) = 0.$$

Το μοντέλο αυτό αντιστοιχεί στο τεστ που αποτελείται από τις 3 ερωτήσεις $\{2, 4, 5\}$, οι οποίες καλύπτουν και τις 9 ενότητες. □

Παρατήρηση. Στις επόμενες ενότητες θα δούμε δύο μεθόδους που μπορούν να χρησιμοποιηθούν και για την επίλυση του προβλήματος της ικανοποιησιμότητας: τα **δένδρα αληθείας** και την **αρχή της απόφασης**.

6.4.1 Ασκήσεις προς επίλυση

1) Σε μια διαδικασία επιλογής μεταξύ τριών αντικειμένων α, β, γ είναι απαραίτητη η ικανοποίηση των παρακάτω περιορισμών:

   i) Δεν μπορούν να επιλεχθούν και τα τρία.
   ii) Αν επιλεχθεί το γ, τότε θα επιλεχθεί και το α.
   iii) Αν δεν επιλεχθεί το β, τότε δεν θα επιλεχθεί και το α.
   iv) Αν δεν επιλεχθεί το γ, τότε δεν θα επιλεχθεί και το α.
   v) Πρέπει να επιλεγεί τουλάχιστον ένα.

   Να μοντελοποιηθεί το πρόβλημα επιλογής ως πρόβλημα ικανοποιησιμότητας.

2) Σε κάποια δίκη κλήθηκαν 4 μάρτυρες. Από τις καταθέσεις τους προέκυψαν τα ακόλουθα συμπεράσματα.

i) Αν η μαρτυρία του M_1 είναι αληθής τότε και η μαρτυρία του M_2 είναι αληθής.

ii) Η μαρτυρία του M_3 είναι αληθής, αν και μόνο αν η μαρτυρία του M_4 είναι αληθής.

iii) Οι μαρτυρίες των M_2 και M_4 ουδέποτε συναληθεύουν.

iv) Η μαρτυρία του M_3 είναι αληθής.

Να μοντελοποιηθεί ως πρόβλημα ικανοποιησιμότητας ο έλεγχος συνέπειας των συμπερασμάτων που προέκυψαν.

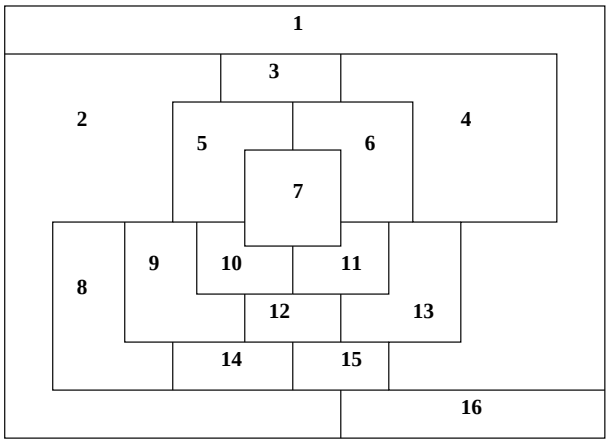
3) Κάποιος συλλέκτης επιθυμεί να συγκεντρώσει μια συλλογή γραμματοσήμων $S = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_n\}$. Τα γραμματόσημα πωλούνται σε ομάδες X_1, X_2, ..., X_k, κάθε μια εκ των οποίων περιέχει ορισμένα από τα γραμματόσημα της συλλογής και οι ομάδες μπορούν να έχουν επικαλύψεις.

Συγκεκριμένα, ο συλλέκτης επιθυμεί να συγκεντρώσει 10 γραμματόσημα Γ_1, Γ_2, ..., Γ_{10} τα οποία πωλούνται ως μέρος των διπλανών 6 ομάδων:

Ομάδα	Γραμματόσημα
X_1	Γ_1, Γ_2, Γ_5, Γ_7, Γ_8, Γ_{10}
X_2	Γ_2, Γ_3, Γ_6, Γ_8, Γ_9, Γ_{10}
X_3	Γ_1, Γ_3, Γ_4, Γ_7, Γ_9, Γ_{10}
X_4	Γ_2, Γ_5, Γ_6, Γ_7, Γ_8, Γ_9
X_5	Γ_3, Γ_6, Γ_7, Γ_8, Γ_9, Γ_{10}
X_6	Γ_1, Γ_3, Γ_4, Γ_5, Γ_7, Γ_9

Να μοντελοποιηθεί ως πρόβλημα ικανοποιησιμότητας το πρόβλημα της ύπαρξης και εύρεσης δύο ομάδων που να περιέχουν όλα τα γραμματόσημα της συλλογής.

4) Ζητείται να χρωματισθούν οι παρακάτω 16 περιοχές με 4 χρώματα έτσι ώστε δύο γειτονικές περιοχές να έχουν διαφορετικό χρώμα:



Να μοντελοποιηθεί ως πρόβλημα ικανοποιησιμότητας το πρόβλημα ύπαρξης και εύρεσης ενός τέτοιου χρωματισμού. (Δύο περιοχές θεωρούνται γειτονικές αν το κοινό τους σύνορο περιέχει άπειρα σημεία.)

(Απάντηση: Βλέπε εδώ.)

6.4.2 Κανονικές μορφές - Επάρκεια συνδέσμων

Στην γενική περίπτωση του προβλήματος της ικανοποιησιμότητας, η μορφή των προτάσεων του Σ μπορεί να είναι ιδιαίτερα περίπλοκη. Για παράδειγμα, μπορεί να περιέχει μια πρόταση όπως η ϕ: $(((p_1 \leftrightarrow \neg p_2) \rightarrow (\neg p_3 \leftrightarrow p_1)) \vee (p_2 \rightarrow \neg p_3) \vee (\neg p_1 \wedge p_3)) \rightarrow ((\neg p_2 \wedge (p_1 \rightarrow p_4)) \vee (\neg p_4 \leftrightarrow \neg p_2))$, κ.ο.κ. Πολλοί αλγόριθμοι για το πρόβλημα ικανοποιησιμότητας απαιτούν οι προτάσεις που εξετάζουν να έχουν συγκεκριμένη μορφή.

Για το λόγο αυτό έχει μελετηθεί το πρόβλημα της εύρεσης προτάσεων ψ που είναι λογικά ισοδύναμες με μια δοθείσα πρόταση ϕ αλλά έχουν μια συγκεκριμένη "απλούστερη" ή "τυποποιημένη" μορφή, η οποία ονομάζεται **κανονική μορφή**.

Υπάρχουν δύο κανονικές μορφές: η **κανονική διαζευκτική μορφή** και η **κανονική συζευκτική μορφή**.

Πρόταση 6.8. *Έστω φ μια πρόταση η οποία, δεν είναι αντιλογία και, περιέχει τις προτασιακές μεταβλητές $p_1, p_2, \ldots, p_n$. Ισχύει ότι:*

$$\varphi \rightleftarrows \bigvee_{v \in [\varphi]} \left(\bigwedge_{i=1}^{n} p_i^v\right),$$

όπου

$$[\varphi] = \{\textit{εκτίμηση } v : v(\varphi) = 1\} \textit{ και } p_i^v = \begin{cases} p_i, & \textit{αν } v(p_i) = 1 \\ \neg p_i, & \textit{αν } v(p_i) = 0. \end{cases}$$

Απόδειξη. Αρκεί να δείξουμε ότι οι δύο προτάσεις έχουν τα ίδια μοντέλα.

Επειδή η φ δεν είναι αντιλογία τα μοντέλα της φ είναι οι εκτιμήσεις του συνόλου $[\varphi]$.

Η πρόταση $\bigvee_{v \in [\varphi]}(\bigwedge_{i=1}^{n} p_i^v)$ είναι αληθής αν και μόνο αν τουλάχιστον μια από τις προτάσεις $\bigwedge_{i=1}^{n} p_i^v$ είναι αληθής. Όμως, η πρόταση $\bigwedge_{i=1}^{n} p_i^v$ είναι αληθής μόνο όταν $v(p_i^v) = 1$ για κάθε $i \in [n]$ δηλαδή μόνο όταν $v \in [\varphi]$ □

Πρακτικά, αυτό σημαίνει ότι οποιαδήποτε πρόταση φ μπορεί να γραφτεί ως διαζεύξεις συζεύξεων ακολουθώντας την εξής διαδικασία:

- Στον πίνακα αληθείας της φ κοιτάζουμε μόνο τις γραμμές με $v(\varphi) = 1$. Για κάθε τέτοια γραμμή δημιουργούμε μια σύζευξη από n μεταβλητές (p_i, αν στην i-οστή θέση της γραμμής έχουμε 1 και $\neg p_i$ αν έχουμε 0).
- Συνδέουμε τις συζεύξεις αυτές με διαζεύξεις.

Η γραφή που προκύπτει από τη διαδικασία αυτή ονομάζεται **(πλήρης) κανονική διαζευκτική μορφή** (**(full) disjunctive normal form**). Γενικότερα, αν μια πρόταση έχει γραφεί ως διαζεύξεις συζεύξεων, ονομάζεται **κανονική διαζευκτική μορφή** (**disjunctive normal form** - DNF)

Παραδείγματα

1) Η πρόταση

$$(\neg\phi \wedge \neg y) \vee (\phi \wedge y) \vee (y \wedge \neg\sigma)$$

είναι γραμμένη σε DNF (αλλά δεν είναι πλήρης).

2) Η πρόταση $\neg(\varphi \wedge y)$ έχει πίνακα αληθείας

φ	y	$\varphi \wedge y$	$\neg(\varphi \wedge y)$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	1

Για να τη γράψουμε λοιπόν σε πλήρη κανονική διαζευκτική μορφή ασχολούμαστε μόνο με τις τρεις τελευταίες γραμμές του πίνακα. Από τη $2^{η}$ γραμμή παίρνουμε: $\varphi \wedge \neg y$, από την $3^{η}$: $\neg\varphi \wedge y$ και από την $4^{η}$: $\neg\varphi\neg \wedge y$.

Άρα τελικά

$$\neg(\varphi \wedge y) \nexists (\varphi \wedge \neg y) \vee (\neg\varphi \wedge y) \vee (\neg\varphi \wedge \neg y).$$

3) Η πρόταση $\varphi(p_1, p_2, p_3)$ με πίνακα:

p_1	p_2	p_3	$\varphi(p_1, p_2, p_3)$	
1	1	1	**1**	$\longrightarrow \quad p_1 \wedge p_2 \wedge p_3$
1	1	0	0	
1	0	1	0	
1	0	0	**1**	$\longrightarrow \quad p_1 \wedge \neg p_2 \wedge \neg p_3$
0	1	1	**1**	$\longrightarrow \quad \neg p_1 \wedge p_2 \wedge p_3$
0	1	0	0	
0	0	1	0	
0	0	0	**1**	$\longrightarrow \quad \neg p_1 \wedge \neg p_2 \wedge \neg p_3$

γράφεται σε DNF: $(p_1 \wedge p_2 \wedge p_3) \vee (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (\neg p_1 \wedge p_2 \wedge p_3) \vee (\neg p_1 \wedge \neg p_2 \wedge \neg p_3)$.

Παρατήρηση. Τα άτομα, οι αρνήσεις ατόμων, προτάσεις που χρησιμοποιούν μόνο διαζεύξεις ατόμων (ή αρνήσεων ατόμων) και προτάσεις που χρησιμοποιούν μόνο συζεύξεις ατόμων (ή αρνήσεων ατόμων), μπορούν τετριμμένα να θεωρηθούν ότι είναι σε DNF.

Για παράδειγμα, η πρόταση $p_1 \vee \neg p_2 \vee p_3 \vee p_4$ μπορεί να θεωρηθεί ως διάζευξη συζεύξεων (DNF) αφού είναι προφανώς ισοδύναμη με την $(p_1 \wedge p_1) \vee (\neg p_2 \wedge \neg p_2) \vee (p_3 \wedge p_3) \vee (p_4 \wedge p_4)$.

Ομοίως, η πρόταση $p_1 \wedge p_2 \wedge \neg p_3$ μπορεί να θεωρηθεί ως διάζευξη συζεύξεων (DNF) αφού είναι προφανώς ισοδύναμη με την $(p_1 \wedge p_2 \wedge \neg p_3) \vee (p_1 \wedge p_2 \wedge \neg p_3)$.

Αντίστοιχα με την κανονική διαζευκτική μορφή, μπορούμε επίσης να γράφουμε οποιαδήποτε πρόταση φ (η οποία δεν είναι ταυτολογία) ως συζεύξεις διαζεύξεων:

- Κοιτάζουμε στον πίνακα αληθείας της φ μόνο τις γραμμές με $\nu(\varphi) = 0$. Για κάθε τέτοια γραμμή δημιουργούμε μια διάζευξη από n μεταβλητές ($\neg p_i$ αν στη i-οστή θέση της γραμμής έχουμε 1 και p_i αν έχουμε 0).
- Συνδέουμε τις διαζεύξεις αυτές με συζεύξεις.

Η γραφή που προκύπτει από αυτή την διαδικασία ονομάζεται **(πλήρης) κανονική συζευκτική μορφή** (**(full) conjuctive normal form - CNF**). Γενικότερα, αν μια πρόταση έχει γραφεί ως συζεύξεις διαζεύξεων, ονομάζεται **κανονική συζευκτική μορφή** (**conjuctive normal form - CNF**).

Έτσι, το προηγούμενο Παράδειγμα 2), δίνει

$$\neg(\varphi \wedge y) \nexists \neg\varphi \vee \neg y$$

και το Παράδειγμα 3) δίνει για την φ τη μορφή

$$(\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_1 \vee p_2 \vee \neg p_3) \wedge (p_1 \vee \neg p_2 \vee p_3) \wedge (p_1 \vee p_2 \vee \neg p_3).$$

Παρατήρηση. Αντίστοιχα με την DNF, προφανώς ισχύει επίσης ότι τα άτομα, οι αρνήσεις ατόμων, προτάσεις που χρησιμοποιούν μόνο διαζεύξεις ατόμων (ή αρνήσεων ατόμων) και προτάσεις που χρησιμοποιούν μόνο συζεύξεις ατόμων (ή αρνήσεων ατόμων), μπορούν τετριμμένα να θεωρηθούν ότι είναι σε CNF.

Αν μας είναι αρκετό να μετατρέψουμε μια πρόταση σε κανονική μορφή (χωρίς να είναι υποχρεωτικά πλήρης), μπορούμε πολλές φορές να το κάνουμε απλούστερα και γρηγορότερα, χρησιμοποιώντας τις ιδιότητες των συνδέσμων (επιμεριστικότητα των $\vee$, $\wedge$, κανόνες De Morgan κ.λπ).

Έτσι, για παράδειγμα, η πρόταση $p_4 \wedge (p_4 \to p_1)$, η οποία γράφεται με χρήση πινάκων αληθείας σε πλήρη CNF ως

$$(\neg p_1 \vee p_4) \wedge (\neg p_4 \vee p_1) \wedge (p_1 \vee p_4),$$

μπορεί να γραφεί πολύ απλούστερα στην ισοδύναμή της (τετριμμένη, μη πλήρη) CNF ως $p_4 \wedge p_1$, αφού

$$p_4 \wedge (p_4 \to p_1) \overset{(1)}{\equiv} p_4 \wedge (\neg p_4 \vee p_1) \overset{(2)}{\equiv} (p_4 \wedge \neg p_4) \vee (p_4 \wedge p_1) \overset{(3)}{\equiv} p_4 \wedge p_1$$

(1): Βλέπε τις βασικές (λογικές) ισοδυναμίες (σελ. 294)

(2): Επιμεριστικότητα

(3): Αφού η $p_4 \wedge \neg p_4$ είναι ψευδής. Γενικά ισχύει προφανώς ότι αν η ψ είναι ψευδής τότε $\psi \vee \phi \equiv \phi$.

Παρατήρηση. Στο πρόβλημα της ικανοποιησιμότητας συνήθως χρησιμοποιείται η δεύτερη κανονική μορφή, δηλαδή η κανονική συζευκτική μορφή (CNF).

Επάρκεια συνδέσμων. Στο σημείο αυτό μπορούμε να κάνουμε μια ενδιαφέρουσα παρατήρηση:

Από τις προηγούμενες δύο κανονικές μορφές είναι φανερό ότι κάθε πρόταση ϕ είναι λογικά ισοδύναμη με μια πρόταση που περιέχει μόνο τους συνδέσμους $\neg$ και $\vee$, ή μόνο τους συνδέσμους $\neg$ και $\wedge$.

Πράγματι, όπως εύκολα μπορούμε να επαληθεύσουμε ισχύουν οι ισοδυναμίες:

$$\begin{array}{ll}
(\varphi \to y) \equiv (\neg\varphi \vee y) & \\
(\varphi \leftrightarrow y) \equiv (\varphi \to y) \wedge (y \to \varphi) & (\text{άρα } (\varphi \leftrightarrow y) \equiv (\neg\varphi \vee y) \wedge (\neg y \vee \varphi)) \\
\neg(\varphi \wedge y) \equiv \neg\varphi \vee \neg y & (\text{άρα } \varphi \wedge y \equiv \neg(\neg\varphi \vee \neg y)) \\
\neg(\varphi \vee y) \equiv \neg\varphi \wedge \neg y & (\text{άρα } \varphi \vee y \equiv \neg(\neg\varphi \wedge \neg y))
\end{array}$$

Άρα, κάθε πρόταση φ που εκφράζεται από τα άτομα και τους λογικούς συνδέσμους $\neg$, $\vee$, $\wedge$, $\to$, $\leftrightarrow$ (δηλαδή κάθε πρόταση του P) μπορεί να εκφραστεί χρησιμοποιώντας μόνο δύο από τους τρεις πρώτους.

Στην πραγματικότητα ισχύει κάτι ακόμα πιο ισχυρό.

Μέχρι τώρα ορίσαμε στην γλώσσα P του προτασιακού λογισμού το μονομελή σύνδεσμο $\neg$ και τους διμελείς συνδέσμους $\wedge, \vee, \to, \leftrightarrow$.

Ο μονομελής σύνδεσμος $\neg$ είναι στην ουσία μια απεικόνιση $F : P \mapsto P$ (με $F(\varphi) = \neg\varphi$) και συνοδεύεται από τον πίνακα αληθείας:

φ	$F(\varphi)$
1	0
0	1

Ισοδύναμα, ο μονομελής σύνδεσμος $\neg$ ορίζεται στην ουσία από τη συνάρτηση $G_\neg : \{0,1\} \mapsto \{0,1\}$ με

φ	$G_\neg(\varphi)$
1	0
0	1

Ομοίως ο διμελής σύνδεσμος $\wedge$ είναι μια απεικόνιση $F : P^2 \mapsto P$ (με $F(\varphi, y) = \varphi \wedge y$) και συνοδεύεται από τον πίνακα αληθείας

φ	y	$F(\varphi, y)$
1	1	1
1	0	0
0	1	0
0	0	0

Αντίστοιχα έχουν ορισθεί και οι διμελείς σύνδεσμοι $\vee, \rightarrow, \leftrightarrow$.

Τα παραπάνω γενικεύονται προφανώς για n-μελείς συνδέσμους ως εξής:

Ορισμός. *Κάθε απεικόνιση $F : P^n \mapsto P$ που συνοδεύεται από έναν πίνακα αληθείας για τις τιμές της $F(\varphi_1, \varphi_2, \ldots, \varphi_n)$ (ή μια συνάρτηση $G_F : \{0,1\}^n \mapsto \{0,1\}$) ονομάζεται* ***n-μελής σύνδεσμος*** *στο P.*

Παράδειγμα

Η συνάρτηση $G_F : \{0,1\}^3 \mapsto \{0,1\}$ με:

φ_1	φ_2	φ_3	$G_F(\varphi_1, \varphi_2, \varphi_3)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

είναι ένας τριμελής σύνδεσμος.

Αποδεικνύεται το παρακάτω γενικό αποτέλεσμα.

Θεώρημα 6.9. *Το σύνολο $\{\wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$ (άρα και τα σύνολα $\{\wedge, \vee, \neg\}$, $\{\wedge, \neg\}$, $\{\vee, \neg\}$) είναι* ***επαρκές****. Δηλαδή, οποιοσδήποτε n-μελής σύνδεσμος F είναι ισοδύναμος (και άρα μπορεί να αντικατασταθεί) με μια πρόταση φ η οποία χρησιμοποιεί μόνο τους συνδέσμους $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$ (ή όπως είδαμε ήδη μόνο τους $\neg$, $\wedge$, $\vee$ ή μόνο τους $\neg$, $\wedge$ ή μόνο τους $\neg$, $\vee$).*

Άρα οι σύνδεσμοι $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$ (ή και μόνο οι $\neg$, $\wedge$, $\vee$ ή μόνο οι $\neg$, $\wedge$ ή μόνο οι $\neg$, $\vee$) επαρκούν για να εκφρασθεί μέσω αυτών οποιοσδήποτε άλλος σύνδεσμος.

Ορισμός. *Έστω $\varphi \in P$ και η φ δεν περιέχει τους συνδέσμους $\rightarrow, \leftrightarrow$. Η πρόταση φ^d που προκύπτει από τη φ αν εναλλάξουμε τους συνδέσμους $\wedge, \vee$ της λέγεται **δυϊκή** της φ.*

Πρόταση 6.10 (Θεώρημα Δυϊκότητας). $\varphi \dashv\vdash y \Leftrightarrow \varphi^d \dashv\vdash y^d$.

Έτσι, για παράδειγμα, αφού όπως ήδη είδαμε ισχύει ότι (προηγούμενο Παράδειγμα 1): $\neg(\varphi \wedge y) \dashv\vdash (\varphi \wedge \neg y) \vee (\neg\varphi \wedge y) \vee (\neg\varphi \wedge \neg y)$, (η DNF της $\neg(\varphi \wedge y)$), τότε ισχύει και ότι: $\neg(\varphi \vee y) \dashv\vdash (\varphi \vee \neg y) \wedge (\neg\varphi \vee y) \wedge (\neg\varphi \vee \neg y)$, (η CNF της $\neg(\varphi \vee y)$).

Πρόταση 6.11. *Το σύνολο $\{\wedge, \rightarrow\}$ είναι μη επαρκές.*

Απόδειξη. Θα δείξουμε ότι ο σύνδεσμος $\neg$ για παράδειγμα δεν μπορεί να αναχθεί στους $\wedge, \rightarrow$. Δηλαδή θα δείξουμε ότι αν p είναι ένα άτομο, τότε η $\neg p$ δεν μπορεί να είναι ισοδύναμη με κάποια πρόταση σ που περιέχει την p και μόνο τους συνδέσμους $\wedge, \rightarrow$.

Έστω λοιπόν ότι η $\neg p$ είναι ισοδύναμη με μια τέτοια σ, δηλαδή $\sigma \dashv\vdash \neg p$, δηλαδή $v(p) = 1 \Leftrightarrow v(\sigma) = 0$. Θα φτάσουμε σε άτοπο. Αρκεί να δείξουμε ότι $v(p) = 1 \Rightarrow v(\sigma) = 1$. Θα χρησιμοποιήσουμε επαγωγή.

Αν η σ είναι άτομο, τότε η σ είναι η p (αφού υποθέσαμε ότι η σ περιέχει την p). Τότε όμως, προφανώς, $v(p) = 1 \Rightarrow v(\sigma) = 1$.

Έστω τώρα ότι ισχύει για τις φ και y. Δηλαδή $v(p) = 1 \Rightarrow (v(\varphi) = 1$ και $v(y) = 1)$. Τότε όμως αν $\sigma = \varphi \wedge y$ έχουμε ότι $v(\sigma) = v(\varphi \wedge y) = 1$, καθώς επίσης και αν $\sigma = \varphi \rightarrow y$ τότε έχουμε ότι $v(\sigma) = v(\varphi \rightarrow y) = 1$. Άρα η επαγωγή ολοκληρώθηκε (αφού ασχολούμαστε μόνο με το σύνολο $\{\wedge, \rightarrow\}$). □

6.4.3 Λυμένες ασκήσεις

Άσκηση 6.16. *Να γραφεί η πρόταση*

$$\varphi = (p \to q) \to \neg(r \leftrightarrow (p \wedge \neg q))$$

σε (πλήρη) κανονική διαζευκτική μορφή και σε (πλήρη) κανονική συζευκτική μορφή.

p	q	r	$p \to q$	$p \wedge \neg q$	$r \leftrightarrow (p \wedge \neg q)$	$\neg(r \leftrightarrow (p \wedge \neg q))$	φ
1	1	1	1	0	0	1	1
1	1	0	1	0	1	0	0
1	0	1	0	1	1	0	1
1	0	0	0	1	0	1	1
0	1	1	1	0	0	1	1
0	1	0	1	0	1	0	0
0	0	1	1	0	0	1	1
0	0	0	1	0	1	0	0

Λύση. Από τον πίνακα αληθείας της φ προκύπτει ότι η φ είναι λογικά ισοδύναμη με την πρόταση

$$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r).$$

Επίσης, η φ είναι λογικά ισοδύναμη με την πρόταση

$$(\neg p \vee \neg q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee r).$$ □

Άσκηση 6.17. *Να γραφούν σε κανονική διαζευκτική και κανονική συζευκτική μορφή οι παρακάτω προτάσεις:*

1. $\phi \to \psi$

   ⊨ $\neg\phi \vee \psi$ *(Είναι σε μορφή CNF και DNF.)*

2. $((\phi \to \psi) \to \phi) \to \psi$

   ⊨ $\neg\phi \vee \psi$

3. $(\neg\phi \vee (\phi \to \zeta)) \wedge (\neg\zeta \vee (\phi \to \psi))$

   ⊨ $(\neg\phi \vee \zeta) \wedge (\neg\zeta \vee \neg\phi \vee \psi)$ *(CNF)*
   ⊨ $(\neg\phi \wedge \neg\zeta) \vee (\zeta \wedge \neg\phi) \vee (\zeta \wedge \psi)$ *(Μετά από πράξεις.) (DNF)*

4. $(\neg\phi) \vee (\phi \wedge \psi)$

$\nVdash \neg\phi \vee \psi$ *(Μετά από πράξεις.)*

5. $(\neg\phi) \to (\psi \wedge (\zeta \vee \psi))$

$\nVdash \phi \vee \psi$ *(Μετά από πράξεις.)*

Άσκηση 6.18. *Να βρεθεί μια πρόταση φ που περιέχει τα άτομα p, q, r και είναι αληθής μόνο όταν ακριβώς δύο από τα p, q, r είναι αληθή.*

Λύση. Ο πίνακας αληθείας της πρότασης φ είναι ο εξής:

p	q	r	φ
1	1	1	0
1	0	1	1
1	1	0	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Άρα, μια τέτοια πρόταση φ είναι η πρόταση

$$(p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r),$$

η οποία προκύπτει γράφοντας την φ σε (πλήρη) κανονική διαζευκτική μορφή. □

Άσκηση 6.19. *Να αποδειχθεί ότι ο σύνδεσμος $|$ (που ονομάζεται **σύνδεσμος του Sheffer**) με πίνακα αληθείας*

φ	y	$\varphi \mid y$
1	*1*	*0*
1	*0*	*1*
0	*1*	*1*
0	*0*	*1*

είναι επαρκής για να εκφράσει οποιοδήποτε λογικό σύνδεσμο.

Λύση. Αφού το σύνολο $\{\neg, \vee, \wedge\}$ είναι επαρκές, αρκεί να εκφραστούν οι τρεις αυτοί σύνδεσμοι συναρτήσει του $|$. Χρησιμοποιώντας την ισοδυναμία $p|q \nVdash \neg(p \wedge q)$, έχουμε ότι

$$\begin{aligned} \neg p &\nVdash \neg(p \wedge p) \nVdash p|p \\ p \vee q &\nVdash \neg(\neg p \wedge \neg q) \nVdash (\neg p)|(\neg q) \nVdash (p|p)|(q|q) \\ p \wedge q &\nVdash \neg\neg(p \wedge q) \nVdash \neg(p|q) \nVdash (p|q)|(p|q) \end{aligned}$$

Άρα το μονοσύνολο $\{|\}$ είναι επαρκές. □

6.4.4 Ασκήσεις προς επίλυση

1) Πόσοι n-μελείς σύνδεσμοι υπάρχουν για κάθε n; Βρείτε αναλυτικά όλους τους μονομελείς συνδέσμους.

2) i) Να δοθεί αναδρομικός ορισμός της δυϊκότητας.
   ii) Να δειχθεί ότι $(\varphi^d)^d \models\!\models \varphi$.

3) Να δειχθεί ότι ο σύνδεσμος $\vee$ μπορεί να εκφραστεί μόνο με τη βοήθεια του συνδέσμου $\to$.

4) Να δειχθεί ότι το σύνολο $\{\neg, \to\}$ είναι επαρκές.

5) Έστω η διμελής πράξη "$\downarrow$", όπου $G_\downarrow(0,0) = 1$ και $G_\downarrow(1,1) = G_\downarrow(1,0) = G_\downarrow(0,1) = 0$. Βρείτε τον πίνακα αληθείας του συνδέσμου και δείξτε ότι το $\{\downarrow\}$ είναι επαρκές.

6) Μετατρέψτε τις παρακάτω προτάσεις σε DNF και CNF:

$$\neg(p_1 \to p_2) \vee (\neg p_1 \wedge p_3), \qquad p_1 \to ((p_2 \wedge \neg p_1) \vee p_3).$$

7) Να βρεθεί μια πρόταση φ που περιέχει τα άτομα p, q, r και είναι αληθής όταν ακριβώς ένα από τα p, q, r είναι αληθές.

8) Να βρεθεί μια πρόταση φ ώστε η πρόταση ψ να είναι ταυτολογία, όταν

   i) $\psi = ((\varphi \wedge q) \to \neg p) \to ((p \to \neg q) \to \varphi)$
   ii) $\psi = ((r \to (\neg q \wedge p)) \to \varphi) \to (\varphi \wedge (p \to q) \wedge r)$.

9) Να βρεθεί μια πρόταση φ που περιέχει τα άτομα p, q, r τέτοια ώστε

   i) $p \wedge \varphi \models\!\models p \wedge q$ και $p \vee \varphi \models\!\models p \vee r$.
   ii) $(r \to \varphi) \models\!\models (r \to (p \wedge q))$ και $(\varphi \to r) \models\!\models (\neg(p \vee q) \to r)$.
   iii) $(r \to \varphi) \models\!\models (q \to (\neg p \vee r))$ και $((r \to q) \to p) \models\!\models (\neg p \to \neg\varphi$.

10) Δεδομένου ότι γνωρίζουμε την πλήρη κανονική διαζευτική μορφή της πρότασης φ, να βρεθεί η πλήρης κανονική διαζευτική και συζευκτική μορφή της πρότασης $\neg\varphi$.

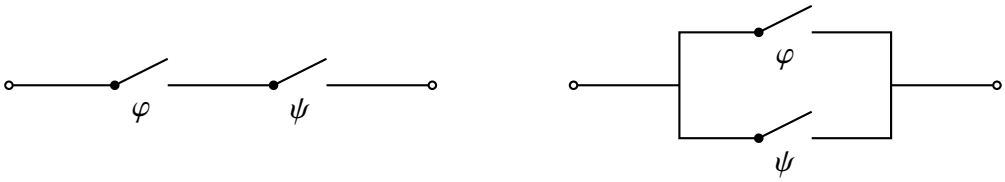
11) Δεδομένου ότι γνωρίζουμε τις πλήρεις κανονικές διαζευκτικές μορφές των προτάσεων φ και ψ, να βρεθεί πώς μπορούμε να βρούμε τις πλήρεις κανονικές διαζευτικές και συζευκτικές μορφές των προτάσεων

   i) $\varphi \vee \psi$
   ii) $\varphi \wedge \psi$.
   iii) $\varphi \to \psi$.

12) Βρείτε το σύνδεσμο $F(\varphi_1, \varphi_2, \varphi_3)$ για τον οποίο:

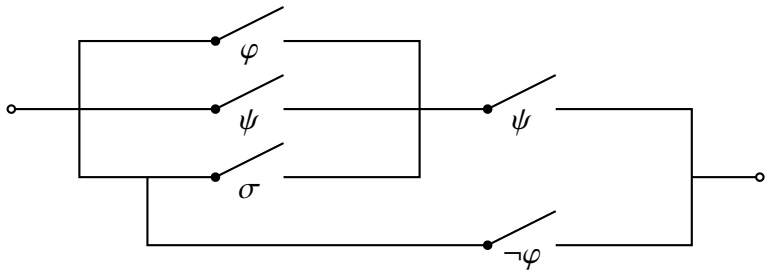
   α) $v(F) = 1 \Leftrightarrow v(\varphi_1) + v(\varphi_2) + v(\varphi_3) = 2$,
   β) $v(F) = 1 \Leftrightarrow v(\varphi_1) + v(\varphi_2) + v(\varphi_3) \geq 2$.

13) Μια πρόταση $\varphi(p_1, \ldots, p_n)$ μοιάζει με ένα ηλεκτρικό κύκλωμα όπου τα p_i είναι διακόπτες. Κάθε διακόπτης έχει δύο δυνατές καταστάσεις, να είναι κλειστός ή ανοιχτός (αλήθεια - ψεύδος), πράγμα που συνεπάγεται δύο καταστάσεις και για το κύκλωμα: περνάει ή δεν περνάει ρεύμα. Τα p_i, $\neg p_i$ αντιστοιχούν στον ίδιο διακόπτη που νοείται ανοιχτός (κλειστός) σαν p_i και κλειστός (ανοιχτός) σαν $\neg p_i$. Έτσι, οι προτάσεις $\varphi \wedge \psi$ και $\varphi \vee \psi$ παριστούν τα στοιχειώδη κυκλώματα αντίστοιχα:

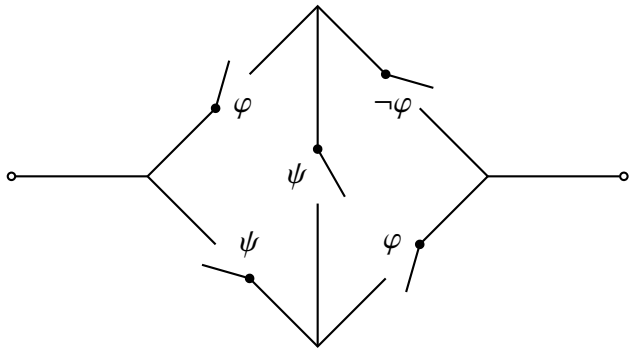


α) Ποιές προτάσεις αντιστοιχούν στα κυκλώματα:

i)



ii)



β) Κατασκευάστε τα κυκλώματα των προτάσεων

$$(\varphi \vee \psi) \wedge \sigma, \qquad (\varphi \vee \sigma) \wedge (\psi \vee \sigma), \qquad (\varphi \to \psi) \wedge (\psi \to \varphi).$$

γ) Κατασκευάστε κύκλωμα με τρεις διακόπτες τέτοιο ώστε να έχει ρεύμα αν και μόνο αν δύο τουλάχιστον από τους διακόπτες είναι κλειστοί.

6.4.5 Το πρόβλημα CNF-SAT

Σε προηγούμενη ενότητα ορίσθηκε το γενικό πρόβλημα ικανοποιησιμότητας:

Το πρόβλημα της ικανοποιησιμότητας: Δοθέντος ενός συνόλου Σ λογικών προτάσεων, να ευρεθεί εκτίμηση που να το ικανοποιεί, ή η απάντηση ότι δεν υπάρχει τέτοια εκτίμηση.

Δεδομένου ότι κάθε πρόταση του Σ μπορεί να γραφεί ισοδύναμα σε CNF μορφή, το παραπάνω πρόβλημα είναι ισοδύναμο με

Το πρόβλημα CNF-SAT: Δοθείσης μιας λογικής πρότασης φ σε CNF μορφή, να ευρεθεί εκτίμηση που να την ικανοποιεί, ή η απάντηση ότι δεν υπάρχει τέτοια εκτίμηση.

Παρατήρηση. Αν και στο πρόβλημα CNF-SAT ασχολούμαστε μόνο με μια πρόταση, αυτό δεν μειώνει την γενικότητα ή τη δυσκολία του. Αυτό ισχύει διότι αν ένα σύνολο Σ αποτελείται από περισσότερες από μία προτάσεις $\phi_1, \phi_2, \ldots, \phi_m$, τότε γράφοντας κάθε μία από αυτές σε κανονική συζευκτική μορφή $\phi'_1, \phi'_2, \ldots, \phi'_m$, προκύπτει ότι το Σ είναι ικανοποιησιμο αν και μόνο αν η CNF πρόταση $\phi'_1 \wedge \phi'_2 \wedge \cdots \wedge \phi'_m$ είναι ικανοποιήσιμη.

Το πρόβλημα 3-CNF-SAT ή 3-SAT Το πρόβλημα 3-CNF-SAT είναι μια ειδική περίπτωση του προβλήματος CNF-SAT, όπου κάθε παρένθεση της πρότασης ϕ περιέχει ακριβώς 3 όρους. Στην περίπτωση αυτή, λέμε ότι η ϕ είναι σε μορφή 3-CNF.

Παράδειγμα 6.4.5. *Η πρόταση*

$$(p_1 \vee p_2 \vee p_3) \wedge (p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_1 \vee p_2 \vee p_4)$$

είναι σε μορφή 3-CNF.

Αν και το 3-CNF-SAT αποτελεί ειδική περίπτωση του CNF-SAT, τελικά είναι **ισοδύναμο** με το γενικό πρόβλημα CNF-SAT, όπως προκύπτει από την **αναγωγή** που ακολουθεί.

Από το CNF-SAT στο 3-CNF-SAT. Έστω ϕ μια πρόταση εκφρασμένη σε CNF ως $\phi_1 \wedge \cdots \wedge \phi_m$, όπου κάθε ϕ_i είναι διάζευξη από άτομα ή/και αρνήσεις ατόμων. Μπορούμε για κάθε ϕ_i να κατασκευάσουμε μια λογικά ισοδύναμη διάζευξη με ακριβώς 3 όρους ως εξής:

- Αν η ϕ_i περιέχει έναν ακριβώς όρο, έστω τον p_1, τότε είναι λογικά ισοδύναμη με την πρόταση ϕ'_i:
$$(p_1 \vee y_1 \vee y_2) \wedge (p_1 \vee \neg y_1 \vee y_2) \wedge (p_1 \vee y_1 \vee \neg y_2) \wedge (p_1 \vee \neg y_1 \vee \neg y_2)$$
όπου y_1, y_2 νέα άτομα.
- Αν η ϕ_i περιέχει 2 όρους, έστω $\phi_i : p_1 \vee p_2$, τότε είναι λογικά ισοδύναμη με την πρόταση ϕ'_i:
$$(p_1 \vee p_2 \vee y_1) \wedge (p_1 \vee p_2 \vee \neg y_1)$$
όπου y_1 νέο άτομο.
- Αν η ϕ_i περιέχει 3 ακριβώς άτομα, τότε δεν κάνουμε καμία αλλαγή

- Αν η ϕ_i περιέχει 4 ή περισσότερους όρους, έστω $\phi_i : p_1 \vee p_2 \vee \cdots \vee p_k$, $k > 3$ τότε την αντικαθιστούμε με την πρόταση ϕ_i':

$$\begin{aligned}&(p_1 \vee p_2 \vee y_1)\\ \wedge&(\neg y_1 \vee p_3 \vee y_2) \wedge (\neg y_2 \vee p_4 \vee y_3) \wedge \cdots \wedge (\neg y_{k-4} \vee p_{k-2} \vee y_{k-3})\\ \wedge&(\neg y_{k-3} \vee p_{k-1} \vee p_k)\end{aligned}$$

όπου $y_1, \ldots, y_{k-3}$ νέα άτομα.

Εύκολα προκύπτει ότι υπάρχει εκτίμηση που ικανοποιεί την ϕ_i' αν και μόνο αν ο περιορισμός αυτής της εκτίμησης στα $p_1, \ldots, p_k$ ικανοποιεί την ϕ_i.

Παράδειγμα 6.4.6. *Να γραφεί η πρόταση*

$$\varphi = (p_1 \vee p_2 \vee \neg p_3 \vee \neg p_4 \vee p_5) \wedge (p_1 \vee \neg p_2)$$

σε μορφή 3-CNF.

Λύση. Η φ είναι λογικά ισοδύναμη με την πρόταση

$$(p_1 \vee p_2 \vee y_1) \vee (\neg y_1 \vee \neg p_3 \vee y_2) \vee (\neg y_2 \vee \neg p_4 \vee p_5) \vee (p_1 \vee \neg p_2 \vee y_4) \vee (p_1 \vee \neg p_2 \vee \neg y_4) \qquad \square$$

Με βάση αυτή την ισοδυναμία, η οποία ανάγει το πρόβλημα CNF-SAT στο πρόβλημα 3-CNF-SAT προκύπτει το συμπέρασμα ότι:

Τα προβλήματα CNF-SAT και 3-CNF-SAT είναι ισοδύναμα από πλευράς δυσκολίας επίλυσης.

Επομένως αν βρεθεί ένας αλγόριθμος που δίνει "αποδοτική" λύση στο πρόβλημα 3-CNF-SAT, αυτός θα δώσει "αποδοτική" λύση και στο πρόβλημα CNF-SAT και άρα και στο γενικό πρόβλημα της ικανοποιησιμότητας (πρόβλημα SAT).

Παρατήρηση. Ενώ το πρόβλημα 3-CNF-SAT είναι δύσκολο, το πρόβλημα 2-CNF-SAT, όπου κάθε διάζευξη περιέχει ακριβώς δύο όρους, είναι εύκολο.

6.4.6 Λυμένες ασκήσεις

Άσκηση 6.20. *Να μετασχηματισθούν σε μορφή 3-CNF-SAT οι τύποι:*

i) $\phi \to \psi$

$\phi \to \psi \amalg \neg\phi \vee \psi \amalg (\neg\phi \vee \psi \vee y_1) \wedge (\neg\phi \vee \psi \vee \neg y_1)$

ii) $((\phi \to \psi) \to \phi) \to \psi$

Από τον πίνακα αληθείας προκύπτει ότι $((\phi \to \psi) \to \phi) \to \psi \amalg \phi \to \psi$*, οπότε η λύση είναι ίδια με την προηγούμενη.*

iii) $(\neg\phi \vee (\phi \to \zeta)) \wedge (\neg\zeta \vee (\phi \to \psi))$

$\amalg (\neg\phi \vee \zeta \vee y) \wedge (\neg\phi \vee \zeta \vee \neg y) \wedge (\neg\zeta \vee \neg\phi \vee \psi)$

iv) $(\neg\phi) \vee (\phi \wedge \psi)$

$\amalg (\neg\phi \vee \phi) \wedge (\neg\phi \vee \psi) \amalg \neg\phi \vee \psi \amalg (\neg\phi \vee \psi \vee y_1) \wedge (\neg\phi \vee \psi \vee \neg y_1)$

v) $(\neg\phi) \to (\psi \wedge (\zeta \vee \psi))$

$\amalg \phi \vee ((\psi \wedge \zeta) \vee \psi) \amalg \phi \vee \psi \amalg (\phi \vee \psi \vee y_1) \wedge (\phi \vee \psi \vee \neg y_1)$

Άσκηση 6.21. *Να μετασχηματισθεί το πρόβλημα ικανοποιησιμότητας του συνόλου:*

$$\Sigma = \{\neg p_1 \vee \neg p_2 \vee \neg p_5, \neg p_2, p_2 \to p_1, (p_3 \wedge p_2) \to p_4, \neg p_4 \vee \neg p_5, (p_4 \vee p_1) \to p_2\}$$

σε μορφή CNF-SAT και στη συνέχεια σε μορφή 3-CNF-SAT.

Λύση.

$$\begin{aligned}
\Sigma \amalg\ & (\neg p_1 \vee \neg p_2 \vee \neg p_5) \wedge (\neg p_2) \wedge (\neg p_2 \vee p_1) \wedge (\neg p_3 \vee \neg p_2 \vee p_4) \\
& \wedge (\neg p_4 \vee \neg p_5) \wedge (\neg p_4 \vee p_2) \wedge (\neg p_1 \vee p_2) \\
\amalg\ & (\neg p_1 \vee \neg p_2 \vee \neg p_5) \wedge (\neg p_2 \vee y_1 \vee y_2) \wedge (\neg p_2 \vee y_1 \vee \neg y_2) \\
& \wedge (\neg p_2 \vee \neg y_1 \vee y_2) \wedge (\neg p_2 \vee \neg y_1 \vee \neg y_2) \\
& \wedge (\neg p_2 \vee p_1 \vee y_1) \wedge (\neg p_2 \vee p_1 \vee \neg y_1) \wedge (\neg p_3 \vee \neg p_2 \vee p_4) \\
& \wedge (\neg p_4 \vee \neg p_5 \vee y_1) \wedge (\neg p_4 \vee \neg p_5 \vee \neg y_1) \\
& \wedge (\neg p_4 \vee p_2 \vee y_1) \wedge (\neg p_4 \vee p_2 \vee \neg y_1) \\
& \wedge (\neg p_1 \vee p_2 \vee y_1) \wedge (\neg p_1 \vee p_2 \vee \neg y_1)
\end{aligned}$$

□

6.4.7 Ικανοποιησιμότητα τύπων Horn

Το πρόβλημα της ικανοποιησιμότητας δεν είναι δύσκολο σε όλες τις περιπτώσεις προτάσεων (π.χ. 2-CNF-SAT). Άλλη μια τέτοια εύκολη περίπτωση έχουμε όταν το σύνολο προτάσεων Σ περιέχει μόνο προτάσεις που ανήκουν σε μια κατηγορία που ονομάζονται *τύποι Horn*. Χάριν απλότητας, θα περιοριστούμε σε τρεις μορφές των τύπων Horn.

Τύποι Horn. Μια πρόταση ονομάζεται **τύπος Horn** αν γράφεται σε μία από τις τρεις μορφές:

α) p_k

β) $(p_1 \wedge p_2 \wedge p_3 \wedge \cdots \wedge p_k) \rightarrow p_{k+1}$

γ) $\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_k$

όπου $p_1, p_2, \ldots, p_k, p_{k+1}$ είναι άτομα.

Στις μορφές β, γ, ανήκουν και προτάσεις της μορφής: $p_k \rightarrow p_{k+1}$, $\neg p_k$.

Για παράδειγμα, οι προτάσεις $(p_1 \wedge p_2) \rightarrow p_1$, p_1, $\neg p_2 \vee \neg p_3$, $p_3 \rightarrow p_1$, $\neg p_2$ είναι τύποι Horn.

Το πρόβλημα της ικανοποιησιμότητας στην περίπτωση των τύπων Horn μπορεί να λυθεί ακολουθώντας τον παρακάτω αλγόριθμο.

Είσοδος: Ένα σύνολο τύπων Horn
Έξοδος: Μια εκτίμηση που το ικανοποιεί, αν υπάρχει.

Βήμα 1: Θέσε ψευδείς τις εκτιμήσεις όλων των ατόμων, εκτός αυτών που περιέχονται **ως** προτάσεις στο Σ.

Βήμα 2: Όσο υπάρχει συνεπαγωγή η οποία δεν ικανοποιείται, θέσε την εκτίμηση του άτομου στο δεξιό της μέλος ως αληθή, και επανάλαβε μέχρις ότου όλες οι συνεπαγωγές ικανοποιούνται.

Βήμα 3: Έλεγξε μόνο τους τύπους οι οποίοι περιέχουν μόνο αρνήσεις ατόμων. Αν όλοι αυτοί οι τύποι είναι αληθείς, τότε επίστρεψε την εκτίμηση που βρέθηκε.
Αλλιώς, επίστρεψε ότι το σύνολο δεν ικανοποιείται.

Παράδειγμα 6.4.7. *Έστω Σ το σύνολο που αποτελείται από τους εξής τύπους Horn.*

$$\Sigma = \{(p_1 \wedge p_2 \wedge p_3) \rightarrow p_1, p_1 \rightarrow p_2, (p_1 \wedge p_3) \rightarrow p_4, (p_1 \wedge p_2) \rightarrow p_4, p_1, p_4, \neg p_3 \vee \neg p_1 \vee \neg p_2\}.$$

Να εξετασθεί αν το σύνολο Σ είναι ικανοποιήσιμο.

Λύση. Το Σ περιέχει 4 άτομα: p_1, p_2, p_3, p_4.

Βήμα 1: Αρχικά θέτουμε όλα τα άτομα ψευδή εκτός από τα p_1, p_4, οπότε έχουμε

$$v(p_2) = v(p_3) = 0, \quad v(p_1) = v(p_4) = 1$$

Βήμα 2: Η συνεπαγωγή $p_1 \rightarrow p_2$ είναι ψευδής, άρα θέτουμε p_2 αληθές, οπότε έχουμε

$$v(p_3) = 0, \quad v(p_1) = v(p_2) = v(p_4) = 1$$

Τώρα, όλες οι συνεπαγωγές είναι αληθείς.

Βήμα 3: Η πρόταση $\neg p_3 \vee \neg p_1 \vee \neg p_2$ είναι αληθής, αφού επαληθεύται από την εκτίμηση ν. Άρα, η εκτίμηση ν που βρήκαμε ικανοποιεί το Σ. □

Παρατηρήσεις.

1) Παρατηρήστε ότι στο Βήμα 2

   - αν η εκτίμηση ενός ατόμου γίνει αληθή, ποτέ δεν θα αλλάξει σε ψευδής
   - μπορεί η εκτίμηση μιας συνεπαγωγής να αλλάξει (μια φορά) από αληθής σε ψευδής
   - αν η εκτίμηση μιας συνεπαγωγής αλλάξει από ψευδής σε αληθής, ποτέ δεν πρόκειται να αλλάξει ξανά, οπότε μπορούμε να την αγνοήσουμε στους μελλοντικούς ελέγχους

2) Οι τύποι Horn βρίσκονται στην καρδιά της γλώσσα προγραμματισμού Prolog. Στην γλώσσα αυτή τα προγράμματα αποτελούνται από λογικές εκφράσεις που δηλώνουν τις επιθυμητές ιδιότητες της εξόδου του προγράμματος. Η βασική λειτουργία των μεταγλωτιστών της Prolog είναι ο προηγούμενος αλγόριθμος.

6.4.8 Ασκήσεις προς επίλυση

Να εξετασθεί αν τα επόμενα σύνολα τύπων Horn είναι ικανοποιήσιμα.

i) $\{(p_1 \wedge p_3 \wedge p_5) \to p_4, \neg p_1 \vee \neg p_4 \vee \neg p_2, p_3 \to p_1, \neg p_5 \vee \neg p_1 \vee \neg p_2, p_3, (p_1 \wedge p_3) \to p_5\}$
Απάντηση. Ικανοποιήσιμο, με $\nu(p_1) = \nu(p_3) = \nu(p_4) = \nu(p_5) = 1$ και $\nu(p_2) = 0$.

ii) $\{p_6, \neg p_3 \vee \neg p_4 \vee \neg p_2, (p_6 \wedge p_3) \to p_1, \neg p_1 \vee \neg p_5 \vee \neg p_3, (p_1 \wedge p_6) \to p_4, p_6 \to p_3\}$
Απάντηση. Ικανοποιήσιμο, με $\nu(p_1) = \nu(p_3) = \nu(p_4) = \nu(p_6) = 1$ και $\nu(p_2) = \nu(p_5) = 0$.

iii) $\{\neg p_1 \vee \neg p_2 \vee \neg p_5, \neg p_2, p_2 \to p_1, (p_3 \wedge p_2 \wedge p_5) \to p_4, \neg p_4 \vee \neg p_5, (p_4 \wedge p_1) \to p_2, p_1\}$.
Απάντηση. Ικανοποιήσιμο, με $\nu(p_1) = 1$ και $\nu(p_2) = \nu(p_3) = \nu(p_4) = \nu(p_5) = 0$.

6.5 Αξιωματικοποίηση του προτασιακού λογισμού - Πληρότητα

Μέχρι τώρα, ελέγχαμε αν $\varphi \models y$ με πίνακες αληθείας. Στα μαθηματικά όμως συνήθως δεν δουλεύουμε έτσι. Θέλουμε αποδείξεις (προτάσεων, θεωρημάτων) από άλλες (βασικές) προτάσεις (αξιώματα) με τη βοήθεια συγκεκριμένων κανόνων παραγωγής. Η μέθοδος αυτή (συντακτική μέθοδος) συνίσταται στην ύπαρξη:

1. Μιας γλώσσας,
2. Κανόνων σχηματισμού των προτάσεων της γλώσσας,
3. Αξιωμάτων (πεπερασμένων σε πλήθος, ή και άπειρων αλλά "αναγνωρίσιμων"),
4. Κανόνων παραγωγής που να οδηγούν μηχανικά από ορισμένες προτάσεις σε άλλες, με μοναδικό κριτήριο τη μορφή (σύνταξη).

Παίρνουμε λοιπόν:

1. Τη γλώσσα L του Π.Λ. που αποτελείται από $\begin{cases} \text{τα άτομα } p_i, i \in \mathbb{N}^*, \\ \text{τους συνδέσμους } {}^{5}\neg, \to, \\ \text{τις παρενθέσεις.} \end{cases}$
2. Τους κανόνες σχηματισμού: $\begin{cases} \text{Τα } p_i \text{ είναι προτάσεις.} \\ \text{Αν } \varphi, y: \text{ προτάσεις, τότε } \neg\varphi, \varphi \to y: \text{ προτάσεις.} \\ \text{Δεν υπάρχουν άλλες προτάσεις.} \end{cases}$
3. Αξιώματα: κάποιες προτάσεις που είναι πάντα αληθείς (δηλαδή κάποιες ταυτολογίες). Διαλέγουμε όσο γίνεται πιο λίγες, κατάλληλες όμως, και αρκετές για να μπορούμε όσο γίνεται πιο εύκολα να συμπεραίνουμε τις υπόλοιπες προτάσεις. Διαλέγουμε τα αξιώματα (αξιωματικά σχήματα με προτασιακές μεταβλητές τις φ, y, σ):

Π_1:	$\varphi \to (y \to \varphi)$.
Π_2:	$(\varphi \to (y \to \sigma)) \to ((\varphi \to y) \to (\varphi \to \sigma))$.
Π_3:	$(\neg\varphi \to \neg y) \to ((\neg\varphi \to y) \to \varphi)$.

4. (Μοναδικός) κανόνας παραγωγής (**Modus Ponens - M.P., ή Κανόνας της Απόσπασης**):

$$\{\varphi, \varphi \to y\} \models y,$$

δηλαδή, από τις φ, $\varphi \to y$ παράγεται η y.

Παρατήρηση. Παρά του ότι δεν είναι απαραίτητοι, θα χρησιμοποιούμε και τους συνδέσμους $\wedge, \vee, \leftrightarrow$, για λόγους συντομίας. Δηλαδή θα γράφουμε

$\varphi \wedge y$ αντί για $\neg(\varphi \to \neg y)$,
$\varphi \vee y$ αντί για $\neg\varphi \to y$,
$\varphi \leftrightarrow y$ αντί για $(\varphi \to y) \wedge (y \to \varphi)$ (δηλαδή, αντί για $\neg((\varphi \to y) \to \neg(y \to \varphi))$).

[5] Υπενθυμίζεται ότι το σύνολο $\{\neg, \to\}$ είναι επαρκές (Άσκηση 4 στην προηγούμενη παράγραφο).

Ορισμός. *Έστω* $\Sigma \subseteq P$ *και* $\varphi \in P$. ***Απόδειξη της*** φ ***από το*** Σ *λέγεται μια πεπερασμένη ακολουθία προτάσεων* $\varphi_1, \varphi_2, \ldots, \varphi_n$, *τέτοια ώστε* $\varphi_n = \varphi$ *και κάθε* φ_i *είναι*

i) *αξίωμα, ή*

ii) *πρόταση του* Σ, *ή*

iii) *παράγεται με το M.P. από δύο προηγούμενες προτάσεις της ακολουθίας (δηλαδή, υπάρχουν* $j, k < i$ *με* $\varphi_j = (\varphi_k \to \varphi_i)$).

Λέμε ότι η φ **παράγεται** ή **αποδεικνύεται** από το Σ, ή είναι **λογική συνέπεια** του Σ και γράφουμε $\boldsymbol{\Sigma \vdash \varphi}$, αν υπάρχει μια απόδειξη της φ από το Σ.

Αν $\Sigma = \{y\}$, τότε γράφουμε $\boldsymbol{y \vdash \varphi}$.

Αν $\Sigma = \emptyset$ (δηλαδή αν η φ παράγεται μόνο από τα αξιώματα) τότε λέμε ότι η φ είναι **θεώρημα** και γράφουμε $\boldsymbol{\vdash \varphi}$.

Πρόταση 6.12.

i) Αν $T \vdash \varphi$ *και* $T \subseteq \Sigma$, *τότε* $\Sigma \vdash \varphi$. *Αν* $\vdash \varphi$, *τότε* $\Sigma \vdash \varphi$.

ii) Αν $\Sigma \vdash \varphi$, *τότε υπάρχει πεπερασμένο* $\Sigma_0 \subseteq \Sigma$ *με* $\Sigma_0 \vdash \varphi$.

iii) Αν $\Sigma \vdash \varphi$ *και* $\Sigma \vdash \varphi \to y$, *τότε* $\Sigma \vdash y$.

Απόδειξη.

i) Προφανώς τα στοιχεία $\varphi_1, \varphi_2, \ldots, \varphi_n = \varphi$ της απόδειξης της φ τα οποία ανήκουν στο T θα ανήκουν και στο $\Sigma \supseteq T$ και άρα $\Sigma \vdash \varphi$. Αν $T = \emptyset$, έχουμε $\vdash \varphi \Rightarrow \Sigma \vdash \varphi$.

ii) Αρκεί να πάρουμε $\Sigma_0 = \Sigma \cap \{\varphi_1, \varphi_2, \ldots, \varphi_n\} \subseteq \Sigma$, όπου $\varphi_1, \varphi_2, \ldots, \varphi_n$ είναι απόδειξη της φ από το Σ.

iii) Αν $\varphi_1, \varphi_2, \ldots, \varphi_n$ είναι απόδειξη της φ και $y_1, y_2, \ldots, y_m$ είναι απόδειξη της $\varphi \to y$, τότε η ακολουθία $\varphi_1, \varphi_2, \ldots, \varphi_n = \varphi, y_1, y_2, \ldots, y_m = (\varphi \to y), y$ είναι απόδειξη της y. □

Λήμμα 6.13.

α) $\vdash \varphi \to \varphi$.

β) $\{\varphi \to y, y \to \sigma\} \vdash \varphi \to \sigma$.

Απόδειξη.

α) 1. $(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$, (από Π_2, με $y = \varphi \to \varphi$ και $\sigma = \varphi$)

2. $\varphi \to ((\varphi \to \varphi) \to \varphi)$, (από Π_1, με $y = \varphi \to \varphi$)

3. $(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$, (από 1, 2 και Μ.Ρ.)

4. $\varphi \to (\varphi \to \varphi)$, (από Π_1 με $y = \varphi$)

5. $\varphi \to \varphi$, (από 3, 4 και Μ.Ρ.)

β) 1. $\varphi \to y$, (από υπόθεση)

2. $y \to \sigma$, (από υπόθεση)

3. $(y \to \sigma) \to (\varphi \to (y \to \sigma))$, (από Π_1, με $\varphi = y \to \sigma$ και $y = \varphi$)

4. $\varphi \to (y \to \sigma)$, (από 3, 2 και Μ.Ρ.) □

5. $(\varphi \to (y \to \sigma)) \to ((\varphi \to y) \to (\varphi \to \sigma))$, ($\Pi_2$)

6. $(\varphi \to y) \to (\varphi \to \sigma)$, (από 5, 4 και Μ.Ρ.)

7. $\varphi \to \sigma$, (από 6, 1 και Μ.Ρ.)

Πρόταση 6.14 (Θεώρημα Παραγωγής (**Deduction Theorem**)).
Αν $\Sigma \subseteq P$ *και* $\varphi, y \in P$, *τότε*

$$\Sigma \cup \{\varphi\} \vdash y \Leftrightarrow \Sigma \vdash \varphi \to y.$$

Επίσης (για $\Sigma = \emptyset$*),* $\varphi \vdash y \Leftrightarrow \vdash \varphi \to y$.

Λήμμα 6.15.

α) $\vdash \varphi \to \neg\neg\varphi$,
β) $\vdash (\varphi \to y) \to (\neg y \to \neg\varphi)$,
γ) $\vdash (\neg\varphi \to \neg y) \to (y \to \varphi)$,
δ) $\vdash \varphi \wedge y \to y \wedge \varphi$,
ε) $\vdash \varphi \wedge y \to y$,
στ) $\vdash \varphi \wedge y \to \varphi$,
ζ) $\vdash \varphi \to (y \to \varphi \wedge y)$,
η) $\vdash \varphi \to (\neg\varphi \to y)$.

Ορισμός. *Ένα σύνολο* Σ *λέγεται* ***συνεπές*** *αν δεν υπάρχει πρόταση* φ *με* $\Sigma \vdash \varphi \wedge \neg\varphi$. *Αλλιώς, το σύνολο λέγεται* ***ασυνεπές***.

Πρόταση 6.16. *Αν το* Σ *είναι ασυνεπές, τότε* $\Sigma \vdash y$, *για κάθε*[6] $y \in P$.

Απόδειξη. Έστω $\Sigma \vdash \varphi \wedge \neg\varphi$. Τότε, βάσει του προηγούμενου Λήμματος, έχουμε:

1.	$\Sigma \vdash \varphi \to (\neg\varphi \to y)$	(από π)
2.	$\Sigma \vdash \varphi$	(από στ, και *iii* της τελευταίας Πρότασης)
3.	$\Sigma \vdash \neg\varphi \to y$	(από 1, 2 και Μ.Ρ.)
4.	$\Sigma \vdash \neg\varphi$	(από ε, και *iii* της τελευταίας Πρότασης)
5.	$\Sigma \vdash y$	(από 3, 4 και Μ.Ρ.)

□

Για να αποδείξουμε τώρα ότι το σύνολο των αξιωμάτων μας $\{\Pi_1, \Pi_2, \Pi_3\}$ είναι συνεπές, χρειαζόμαστε πρώτα το ακόλουθο θεώρημα.

Πρόταση 6.17 (Θεώρημα Ορθότητας (**Soundness Theorem**)).
Αν $\Sigma \vdash \varphi$, *τότε* $\Sigma \models \varphi$, *(δηλαδή, αν υπάρχει μια απόδειξη της* φ *από το* Σ, *τότε η* φ *είναι λογικό συμπέρασμα του* Σ*).*
Επίσης (για $\Sigma = \emptyset$*), αν* $\vdash \varphi$, *τότε* $\models \varphi$, *(δηλαδή, αν η* φ *είναι θεώρημα, τότε είναι ταυτολογία).*

Απόδειξη. Έστω $\varphi_1, \varphi_2, \ldots, \varphi_n$ μια απόδειξη της φ από το Σ. Θα δείξουμε με επαγωγή ότι $\Sigma \models \varphi_i$, για κάθε $i = 1, 2, \ldots, n$ (άρα και $\Sigma \models \varphi_n$, δηλαδή $\Sigma \models \varphi$, αφού $\varphi_n = \varphi$).

Η φ_1 είναι αξίωμα (οπότε είναι ταυτολογία, οπότε $\Sigma \models \varphi_1$), ή $\varphi_1 \in \Sigma$ (οπότε $\Sigma \models \varphi_1$).

Έστω $\Sigma \models \varphi_m$, για κάθε $m < i$. Θα δείξουμε ότι $\Sigma \models \varphi_i$. Αν η φ_i είναι αξίωμα ή $\varphi_i \in \Sigma$, τότε πράγματι $\Sigma \models \varphi_i$ (όπως για τη φ_1). Διαφορετικά, υπάρχουν $j, k < i$ με $\varphi_j = (\varphi_k \to \varphi_i)$. Αλλά (από την υπόθεση της επαγωγής) έχουμε ότι $\Sigma \models \varphi_k$ και $\Sigma \models \varphi_k \to \varphi_i$, οπότε για κάθε μοντέλο ν του Σ έχουμε ότι $\nu(\varphi_k) = 1$ και $\nu(\varphi_k \to \varphi_i) = 1$, και συνεπώς $\nu(\varphi_i) = 1$, δηλαδή $\Sigma \models \varphi_i$. □

Πόρισμα 6.18. *Το σύνολο* $\{\Pi_1, \Pi_2, \Pi_3\}$ *είναι συνεπές.*

Απόδειξη. Αν όχι, τότε από το σύνολο $\{\Pi_1, \Pi_2, \Pi_3\}$ των αξιωμάτων θα μπορούσαμε να συμπεράνουμε τη $\varphi \wedge \neg\varphi$. Δηλαδή, η $\varphi \wedge \neg\varphi$ θα ήταν ένα θεώρημα, δηλαδή $\vdash \varphi \wedge \neg\varphi$, δηλαδή $\models \varphi \wedge \neg\varphi$ το οποίο είναι αντίφαση. □

Πρόταση 6.19. *Αν* $\Sigma \subseteq P$ *και* $\varphi \in P$, *τότε*

$$\Sigma \nvdash \varphi \Leftrightarrow \Sigma \cup \{\neg\varphi\}\text{: συνεπές.}$$

Το Θεώρημα της Ορθότητας δηλώνει ότι αν μπορούμε να αποδείξουμε μια πρόταση, αυτή μπορεί να θεωρηθεί ως ένα λογικό συμπέρασμα. Ισχύει όμως και το αντίστροφο (όπως θα δούμε παρακάτω, στο Θεώρημα Πληρότητας και το Πόρισμά του). Δηλαδή, αν έχουμε ένα λογικό συμπέρασμα, τότε μπορούμε να το αποδείξουμε. Δηλαδή, τα σύμβολα $\models$ και $\vdash$ είναι ισοδύναμα, και το τυπικό σύστημα του Προτασιακού Λογισμού λέγεται **πλήρες**.

Δίδεται τώρα το Θεώρημα Πληρότητας, διατυπωμένο με δύο ισοδύναμες μορφές.

[6] Δηλαδή, από ένα ασυνεπές σύνολο μπορούμε να αποδείξουμε τα πάντα!

Πρόταση 6.20 (Θεώρημα Πληρότητας (**Completeness Theorem**)).
Αν ένα σύνολο προτάσεων Σ είναι συνεπές, τότε είναι ικανοποιήσιμο.

Η διατύπωση αυτή συνδέει τη (σημασιολογική) έννοια του μοντέλου με τη (συντακτική) έννοια της συνέπειας.

Η δεύτερη εκδοχή του Θεωρήματος της Πληρότητας (που εμφανίζεται σαν συνέπεια - πόρισμα της πρώτης) έχει, όπως ήδη αναφέρθηκε, τη μορφή του αντίστροφου του Θεωρήματος της Ορθότητας:

Πόρισμα 6.21. *Αν* $\Sigma \models \varphi$ *τότε* $\Sigma \vdash \varphi$, *(δηλαδή, για κάθε λογικό συμπέρασμα του* Σ, *υπάρχει μια απόδειξή του από το* Σ*).*
Επίσης, (για $\Sigma = \emptyset$*): Αν* $\models \varphi$ *τότε* $\vdash \varphi$, *(δηλαδή, κάθε ταυτολογία είναι ένα θεώρημα).*

Απόδειξη. Έστω $\Sigma \nvdash \varphi$. Τότε (από προηγούμενη πρόταση) το $\Sigma \cup \{\neg\varphi\}$ είναι συνεπές. Άρα (από το Θεώρημα Πληρότητας) το $\Sigma \cup \{\neg\varphi\}$ είναι ικανοποιήσιμο. Δηλαδή, υπάρχει ν τέτοια ώστε $\nu \models \Sigma$ και $\nu \models \neg\varphi$. Αλλά τότε $\Sigma \not\models \varphi$ (αφού, αν $\Sigma \models \varphi$ θα παίρναμε $\nu \models \varphi$ το οποίο είναι άτοπο). □

Παρατήρηση. Λόγω του Θεωρήματος Πληρότητας, θεμελιώνονται οι παρακάτω ισοδυναμίες:

Σημασιολογική έννοια	Συντακτική έννοια
φ: ταυτολογία, $\models \varphi$	φ: θεώρημα, $\vdash \varphi$
φ: λογικό συμπέρασμα του Σ, $\Sigma \models \varphi$	φ: αποδεικνύεται από το Σ, $\Sigma \vdash \varphi$
Σ: ικανοποιήσιμο	Σ: συνεπές

Ορισμός. *Το* $\Sigma \subseteq P$ *λέγεται* ***πλήρες***[7] *αν για κάθε* $\varphi \in P$, *έχουμε* $\Sigma \vdash \varphi$ *ή* $\Sigma \vdash \neg\varphi$.

Πρόταση 6.22. *Κάθε συνεπές σύνολο προτάσεων μπορεί να επεκταθεί σε ένα πλήρες συνεπές σύνολο.*

Όπως ήδη είπαμε, μπορούμε με διάφορους τρόπους να "αξιωματικοποιήσουμε" τον Π.Λ. (δηλαδή να αλλάξουμε τους συνδέσμους που χρησιμοποιούμε, ή τα αξιώματα, ή τους κανόνες παραγωγής).

Έτσι, για παράδειγμα, στο **σύστημα Hilbert - Ackermann** χρησιμοποιούνται οι σύνδεσμοι $\vee$, $\neg$ και τα αξιώματα

1) $\varphi \vee \varphi \to \varphi$,
2) $\varphi \to \varphi \vee y$,
3) $\varphi \vee y \to y \vee \varphi$,
4) $(\varphi \to \sigma) \to (y \vee \varphi \to y \vee \sigma)$,

ενώ στο **σύστημα Rosser** χρησιμοποιούνται οι σύνδεσμοι $\wedge$, $\neg$ και τα αξιώματα

1) $\varphi \to \varphi \wedge \varphi$,
2) $\varphi \wedge y \to \varphi$,
3) $(\varphi \to y) \to (\neg(y \wedge \sigma) \to (\neg(\sigma \wedge y))$.

[7] Η έννοια της πληρότητας ενός υποσυνόλου του P που δίνεται στον ορισμό αυτό, και της πληρότητας ενός τυπικού συστήματος που δόθηκε νωρίτερα είναι διαφορετικές.

6.5.1 Ανεξαρτησία των αξιωμάτων

Έστω $\varphi \in \Sigma \subseteq P$ και $\Sigma' = \Sigma \setminus \{\varphi\}$. Αν το $\Sigma' \nvdash \varphi$ τότε λέμε ότι **η φ είναι ανεξάρτητη από το Σ'**.

Το σύνολο Σ λέγεται **ανεξάρτητο** αν καμία πρότασή του δεν παράγεται από τις υπόλοιπες, δηλαδή:

$$\Sigma \setminus \{\varphi\} \nvdash \varphi, \qquad \text{για κάθε } \varphi \in \Sigma.$$

Ο έλεγχος της ανεξαρτησίας συνήθως γίνεται με τη χρήση μοντέλων. Αν δηλαδή $\Sigma = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$, πρέπει $\Sigma \setminus \{\varphi_i\} \nvdash \varphi_i$, για κάθε $i = 1, 2, \ldots, n$. Λόγω της πληρότητας, αυτό είναι ισοδύναμο με: $\Sigma \setminus \{\varphi_i\} \not\models \varphi_i$, δηλαδή υπάρχει ένα μοντέλο που ικανοποιεί το $\Sigma \setminus \{\varphi_i\}$ αλλά όχι την φ_i.

Αυτή η μέθοδος όμως δεν μπορεί να εφαρμοστεί για να δείξουμε ότι το σύνολο $\{\Pi_1, \Pi_2, \Pi_3\}$ των αξιωμάτων του συστήματός μας είναι ανεξάρτητο, διότι πρέπει για παράδειγμα να δείξουμε ότι $\{\Pi_2, \Pi_3\} \nvdash \Pi_1$. Αυτό όμως δεν είναι ισοδύναμο με το $\{\Pi_2, \Pi_3\} \not\models \Pi_1$, διότι τα σύμβολα $\models$ και $\vdash$ αποδείχθηκαν ισοδύναμα θεωρώντας ότι "αριστερά" τους υπήρχε όλο το σύστημα των αξιωμάτων (δηλαδή τα $\{\Pi_1, \Pi_2, \Pi_3\}$ και όχι μόνο δύο από αυτά).

Έτσι, ενώ είναι προφανές ότι $\{\Pi_2, \Pi_3\} \models \Pi_1$ (αφού όλα αυτά είναι ταυτολογίες), δεν έπεται ότι $\{\Pi_2, \Pi_3\} \vdash \Pi_1$. Αποδεικνύεται πάντως (με χρήση "τρίτιμων" εκτιμήσεων) ότι το σύνολο $\{\Pi_1, \Pi_2, \Pi_3\}$ των τριών αξιωμάτων είναι πράγματι ανεξάρτητο (δηλαδή, κανένα αξίωμα δεν είναι "περιττό").

6.5.2 Λυμένες ασκήσεις

Άσκηση 6.22. *Να δειχθεί ότι το σύνολο $\Sigma = \{p_1 \to p_2, p_2 \to p_1\}$ είναι ανεξάρτητο.*

Λύση. Έστω $\varphi_1 = p_1 \to p_2$ και $\varphi_2 = p_2 \to p_1$. Πρέπει λοιπόν να δειχθεί ότι $\Sigma \setminus \{\varphi_1\} \nvdash \varphi_1$, δηλαδή ότι $p_2 \to p_1 \nvdash p_1 \to p_2$ και επίσης να δειχθεί ότι $\Sigma \setminus \{\varphi_2\} \nvdash \varphi_2$, δηλαδή ότι $p_1 \to p_2 \nvdash p_2 \to p_1$.

Για το πρώτο, αν πάρουμε την εκτίμηση ν με $\nu(p_1) = 1$ και $\nu(p_2) = 0$, τότε πράγματι $\nu(p_2 \to p_1) = 1$ και $\nu(p_1 \to p_2) = 0$ δηλαδή $p_2 \to p_1 \not\models p_1 \to p_2$, οπότε ισοδύναμα $p_2 \to p_1 \nvdash p_1 \to p_2$.

Για το δεύτερο, αν πάρουμε την εκτίμηση ν με $\nu(p_1) = 0$ και $\nu(p_2) = 1$, τότε πράγματι $\nu(p_1 \to p_2) = 1$ και $\nu(p_2 \to p_1) = 0$ δηλαδή $p_1 \to p_2 \not\models p_2 \to p_1$, οπότε ισοδύναμα $p_1 \to p_2 \nvdash p_2 \to p_1$.

Άρα, το σύνολο Σ είναι ανεξάρτητο. □

Άσκηση 6.23. *Να δειχθεί ότι η πρόταση p_1 είναι ανεξάρτητη από το σύνολο $\Sigma' = \{p_1 \vee p_3, p_2 \to \neg p_1, p_2 \to (\neg p_1 \vee \neg p_3)\}$.*

Λύση. Αρκεί να βρεθεί ένα μοντέλο του Σ' το οποίο δεν επαληθεύει την p_1. Δηλαδή, αρκεί να βρεθεί εκτίμηση ν με $\nu(p_1) = 0$, η οποία επαληθεύει το Σ'.

Πρέπει $\nu(p_1 \vee p_3) = 1$, άρα αφού $\nu(p_1) = 0$ έπεται ότι $\nu(p_3) = 1$.

Πρέπει $\nu(p_2 \to (\neg p_1 \vee \neg p_3)) = 1$. Αρκεί $\nu(p_2) = 0$.

Επίσης, αν $\nu(p_2) = 0$, τότε $\nu(p_2 \to p_3) = 1$.

Άρα, η εκτίμηση ν με $\nu(p_1) = 0$, $\nu(p_2) = 0$ και $\nu(p_3) = 1$ είναι μοντέλο του Σ', αλλά δεν είναι μοντέλο της p_1. Επομένως, η p_1 είναι ανεξάρτητη από το Σ'. □

Άσκηση 6.24. *Να εξετασθεί αν η πρόταση $\neg p_2 \vee p_3$ είναι ανεξάρτητη από το σύνολο $\Sigma' = \{\neg p_1 \vee p_2, p_1 \wedge (p_2 \vee p_3)\}$.*

Λύση. Έστω v ένα μοντέλο του Σ'.

Πρέπει $v(p_1 \wedge (p_2 \to p_3)) = 1$, άρα $v(p_1) = 1$ και $v(p_2 \to p_3) = 1$.

Επειδή $v(p_1) = 1$ και $v(\neg p_1 \vee p_2) = 1$, έπεται ότι $v(p_2) = 1$.

Επειδή $v(p_2) = 1$ και $v(p_2 \to p_3) = 1$, έπεται ότι $v(p_3) = 1$.

Άρα, $v(\neg p_2 \vee p_3) = 1$.

Επομένως, η πρόταση $\neg p_2 \vee p_3$ δεν είναι ανεξάρτητη από το Σ', διότι κάθε μοντέλο του Σ' είναι και μοντέλο της πρότασης $\neg p_2 \vee p_3$. □

6.5.3 Ασκήσεις προς επίλυση

1) Έστω $\Sigma' = \{p_1 \to (p_2 \wedge \neg p_3), \quad p_3 \to p_2\}$. Να εξετασθεί αν η $p_1 \to p_3$ είναι ανεξάρτητη από το Σ'.

2) Έστω $\Sigma' = \{p_1 \to p_2, p_2 \to p_4, p_2 \to p_3, p_4 \to p_3, p_1 \to p_5, p_5 \to p_4\}$. Να εξετασθεί αν κάποια από τις προτάσεις $p_1 \to p_4$, $p_2 \to p_5$, $p_3 \to p_4$ είναι ανεξάρτητη από το Σ'.

6.6 Δένδρα αληθείας

Μπορούμε να αποδείξουμε μια πρόταση με πίνακα αληθείας: Ελέγχουμε ότι σε κάθε περίπτωση (δηλαδή για κάθε συνδυασμό των τιμών αληθείας των προτάσεων που υπεισέρχονται στο πρόβλημα) στην οποία αληθεύουν όλες οι υποθέσεις, αληθεύει και η αποδεικτέα.

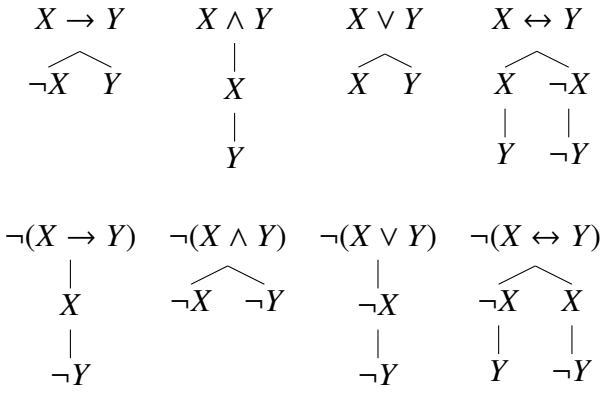
Για παράδειγμα, αν θέλουμε να δείξουμε ότι $\{A \to \neg B,\ \ \neg C \to A\} \models B \to C$) μπορούμε να χρησιμοποιήσουμε τον πίνακα:

A	B	C	$\neg B$	$A \to \neg B$	$\neg C$	$\neg C \to A$	$B \to C$
1	1	1	0	0	0	1	1
1	1	0	0	0	1	1	0
1	0	1	1	(1)	0	(1)	(1)
1	0	0	1	(1)	1	(1)	(1)
0	1	1	0	(1)	0	(1)	(1)
0	1	0	0	1	1	0	0
0	0	1	1	(1)	0	(1)	(1)
0	0	0	1	1	1	0	1

Πράγματι λοιπόν, σε κάθε περίπτωση που οι δύο υποθέσεις είναι αληθείς, ισχύει το συμπέρασμα. Παρατηρούμε όμως ότι έτσι, συνήθως κάνουμε "περιττό κόπο" (αφού οι γραμμές 1, 2, 6, 8 του πίνακα δεν χρειάζονται τελικά). Γι΄ αυτό θα παρουσιάσουμε μια άλλη μέθοδο απόδειξης η οποία χρησιμοποιεί τα **δένδρα αληθείας**.

Η μέθοδος αυτή στηρίζεται στην έννοια του αντιπαραδείγματος. Αν δηλαδή θέλουμε, από κάποιες υποθέσεις να αποδείξουμε κάποιο συμπέρασμα, αρκεί να αποδείξουμε ότι δεν υπάρχει αντιπαράδειγμα. Δηλαδή, υποθέτοντας ότι ισχύει η άρνηση του αποδεικτέου, φθάνουμε σε κάθε περίπτωση σε αντίφαση (αλλιώς θα έχουμε ένα αντιπαράδειγμα).

Χρειαζόμαστε γι΄ αυτό τους παρακάτω συμπερασματικούς κανόνες (δύο για κάθε σύνδεσμο: $\to, \wedge, \vee, \leftrightarrow$):



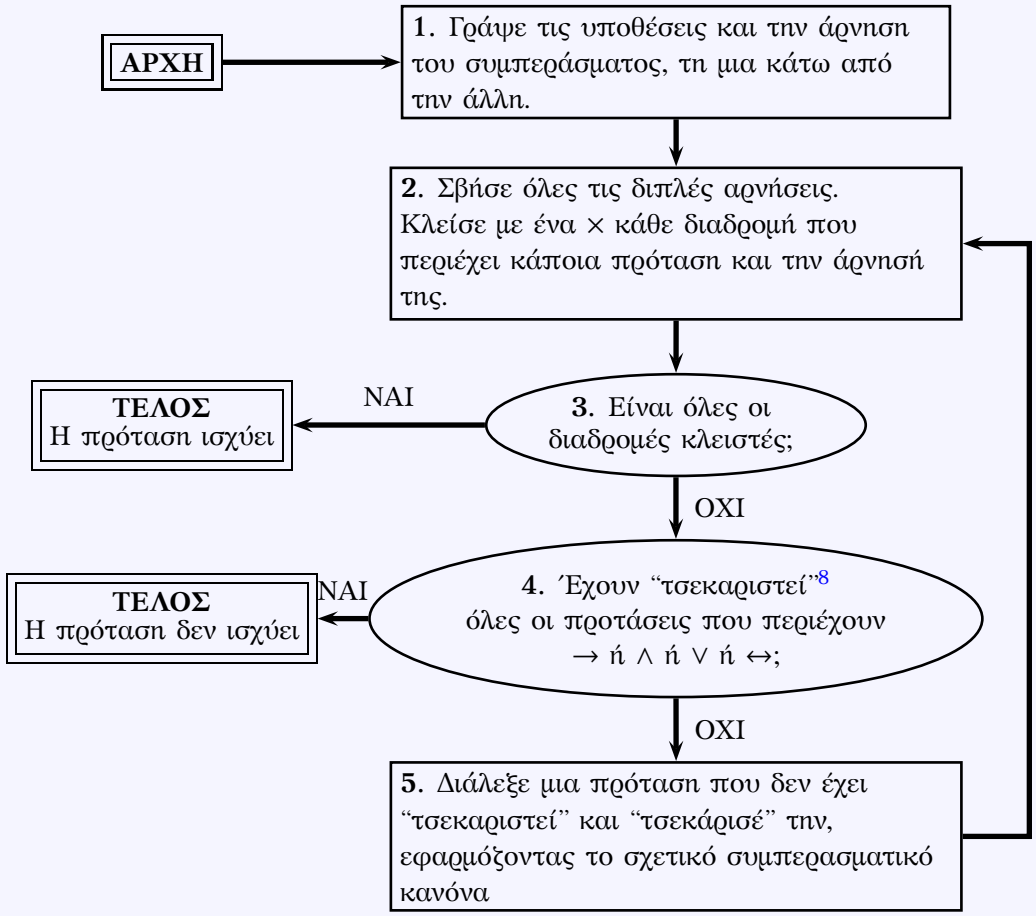
Οι κανόνες αυτοί προφανώς εκφράζουν τις ισοδυναμίες:

$$\begin{array}{lcllcl} X \to Y & \amalg & (\neg X) \vee Y & \neg(X \to Y) & \amalg & X \wedge \neg Y \\ X \wedge Y & \amalg & X \wedge Y & \neg(X \wedge Y) & \amalg & \neg X \vee \neg Y \\ X \vee Y & \amalg & X \vee Y & \neg(X \vee Y) & \amalg & \neg X \wedge \neg Y \\ X \leftrightarrow Y & \amalg & (X \wedge Y) \vee (\neg X \wedge \neg Y) & \neg(X \leftrightarrow Y) & \amalg & (\neg X \wedge Y) \vee (X \wedge \neg Y), \end{array}$$

με διακλάδωση για το $\vee$ και με διαδοχική παράθεση (το ένα κάτω από το άλλο) για το $\wedge$.

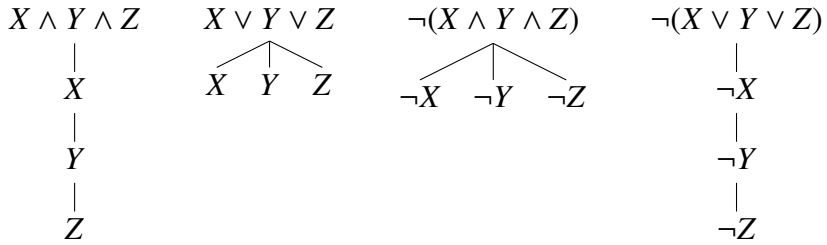
Αν σε μια διαδρομή του δένδρου αληθείας που δημιουργείται, εμφανίζονται μια πρόταση και η άρνησή της, τότε αυτή η διαδρομή λέγεται **κλειστή** (αυτό σημειώνεται με ένα $\times$ στο τέλος της διαδρομής).

Τα δένδρα αληθείας δημιουργούνται με βάση τον παρακάτω αλγόριθμο:



Παρατηρήσεις.

1. Φυσικά, μπορούμε να γενικεύσουμε κάποιους από τους παραπάνω συμπερασματικούς κανόνες:



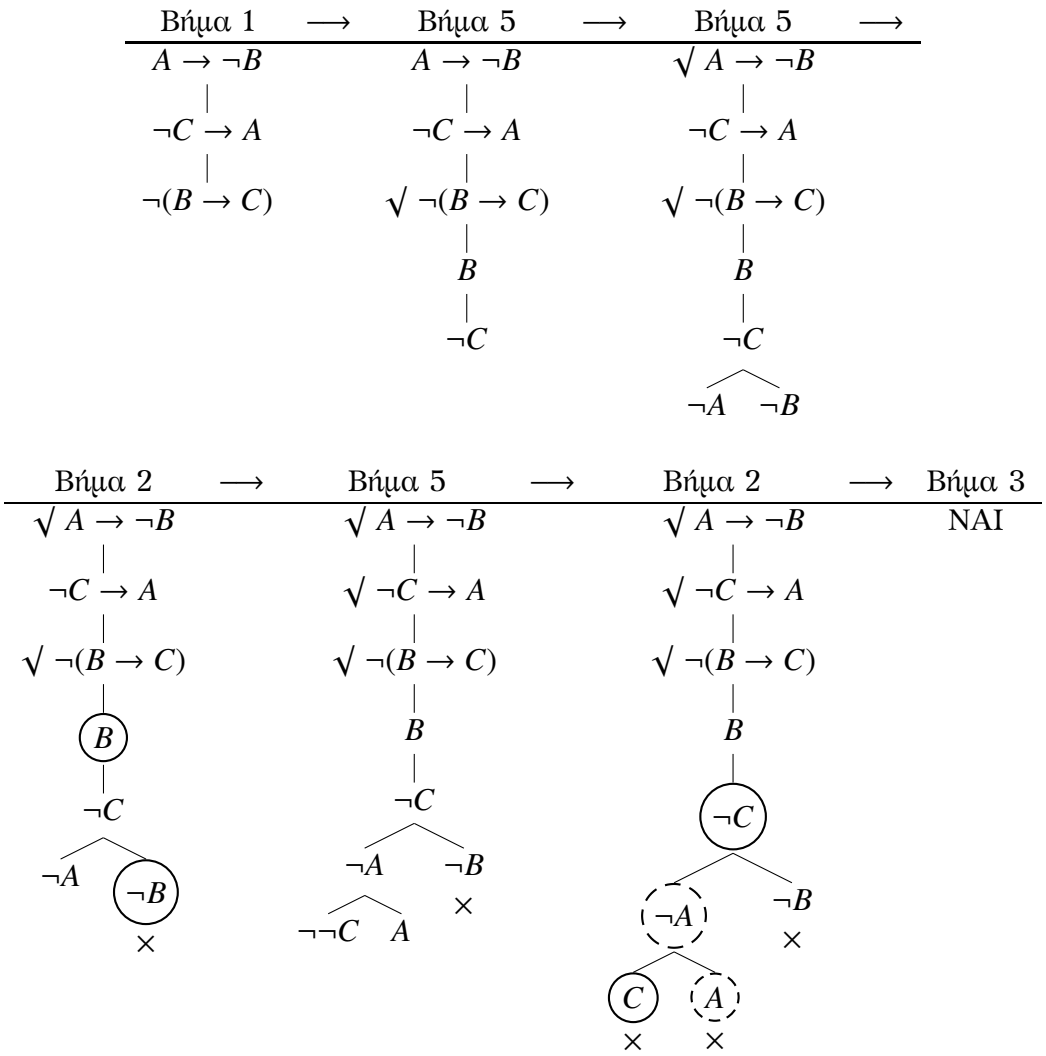
2. Μπορούμε να διαλέξουμε τις προτάσεις που "τσεκάρουμε" και διασπάμε (σύμφωνα με τους συμπερασματικούς κανόνες) με όποια σειρά θέλουμε. Συνήθως όμως, χρησιμοποιούμε πρώτα, αν γίνεται, τους κανόνες για τις $X \wedge Y$, $\neg(X \to Y)$, $\neg(X \vee Y)$ που δεν δημιουργούν διακλαδώσεις, (αν, φυσικά, οι περιπτώσεις αυτές εμφανίζονται στο δένδρο).

Στη συνέχεια, παρουσιάζονται μερικά παραδείγματα του αλγορίθμου. Στο πρώτο παράδειγμα, παρουσιάζεται βήμα προς βήμα η διαδικασία κατασκευής του δένδρου αληθείας. Στην πράξη, εμφανίζεται συνήθως μόνο το τελικό στιγμιότυπο της διαδικασίας αυτής, όπως φαίνεται στα υπόλοιπα παραδείγματα.

[8] "Τσεκάρουμε" μια πρόταση, όταν εφαρμόζουμε γι΄ αυτήν το σχετικό συμπερασματικό κανόνα.

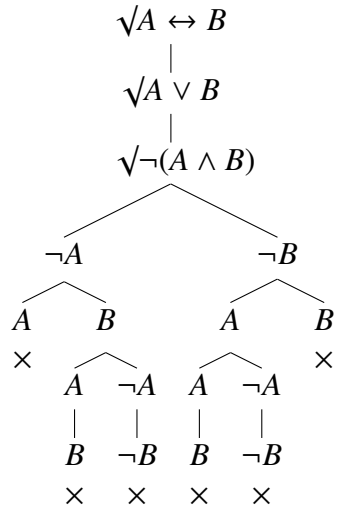
Παράδειγμα 6.6.1. *Να εξετασθεί αν ισχύει* $\{A \to \neg B, \quad \neg C \to A\} \models B \to C$.

(Το βήμα 2 δεν αναφέρεται όταν δεν υπάρχουν διπλές αρνήσεις ή δεν δημιουργούνται κλειστές διαδρομές, και επίσης δεν αναφέρονται τα βήματα 3 και 4 όταν η απάντησή τους είναι "ΟΧΙ", οπότε και συνεχίζεται η εκτέλεση του αλγορίθμου.)



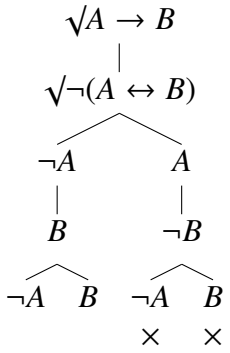
Επειδή η απάντηση στο Βήμα 3 είναι τώρα "ΝΑΙ", ο αλγόριθμος τερματίζει συμπεραίνοντας ότι η αποδεικτέα ισχύει.

Παράδειγμα 6.6.2. *Να εξετασθεί αν ισχύει ότι* $\{A \leftrightarrow B, \quad A \vee B\} \models A \wedge B$.



Όλες οι διαδρομές είναι κλειστές, άρα ισχύει.

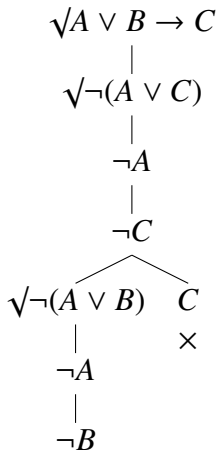
Παράδειγμα 6.6.3. *Να εξετασθεί αν ισχύει ότι* $A \rightarrow B \models A \leftrightarrow B$.



Οι δύο πρώτες διαδρομές δεν είναι κλειστές, άρα δεν ισχύει.

Παρατήρηση. Παρατηρούμε εδώ ότι οι διαδρομές που δεν κλείνουν περιέχουν τα $\neg A$, B. Άρα τα $\neg A$, B (δηλαδή $A : 0$, $B : 1$) δίνουν ένα αντιπαράδειγμα. Πράγματι, αν $A : 0$, $B : 1$, τότε ισχύει $A \rightarrow B : 1$ ενώ $A \leftrightarrow B : 0$.

Παράδειγμα 6.6.4. *Να εξετασθεί αν ισχύει ότι* $A \vee B \to C \models A \vee C$.



Η πρώτη διαδρομή δεν είναι κλειστή, άρα δεν ισχύει.

Παρατήρηση. Στη διαδρομή που δεν κλείνει εμφανίζονται τα $\neg A$, $\neg B$, $\neg C$ τα οποία δίνουν ένα αντιπαράδειγμα. Πράγματι, για $A, B, C : 0$, έχουμε $A \vee B \to C : 1$, ενώ $A \vee C : 0$.

6.6.1 Ασκήσεις προς επίλυση

Να εξετασθεί, με χρήση δένδρων αληθείας, αν ισχύει κάθε ένα από τα παρακάτω:

i) $\{A, \quad A \to B\} \models B$.

ii) $\{B, \quad A \to B\} \models A$.

iii) $\neg A \models A \to B$.

iv) $\{A \to B, \quad B \to C\} \models A \to C$.

v) $\neg A \to B \models B \to A$.

vi) $A \to B \models \neg B \to \neg A$.

vii) $(A \to B) \to C \models \neg C \to A$.

viii) $(A \to B) \to A \models A$.

ix) $(A \to B) \to B \models A$.

x) $\{A \to B, \quad B \to C, \quad C \to D\} \models A \to D$.

xi) $\{A \to B, \neg A \to C\} \models (B \to A) \to (B \wedge C)$.

xii) $\{\neg A \vee B, A\} \models (\neg B \to C) \wedge (A \wedge (B \vee C))$.

xiii) $\{\neg A \to B, \neg B \to C\} \models A \to (\neg C \to B)$.

xiv) $\{\neg A \wedge B, A \to \neg C\} \models A \vee (B \to C)$.

Όπου δεν ισχύει, να δοθούν όλα τα σχετικά αντιπαραδείγματα.

6.7 Αρχή της απόφασης

Η αρχή της απόφασης (resolution principle) οδηγεί, όπως θα δούμε, σε ένα τρόπο απόδειξης που είναι στην ουσία μια παραλλαγή της μεθόδου της εις άτοπον απαγωγής. Δίνουμε πρώτα τους ακόλουθους ορισμούς:

Έστω δύο προτάσεις φ, y με

$$\varphi = \varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_k, \qquad y = y_1 \vee y_2 \vee \cdots \vee y_l,$$

όπου οι $\varphi_1, \varphi_2, \ldots, \varphi_k, y_1, y_2, \ldots, y_l$ είναι προτασιακές μεταβλητές ή αρνήσεις προτασιακών μεταβλητών (για παράδειγμα, $\varphi = \varphi_1 \vee \neg\varphi_2 \vee \neg\varphi_3 \vee \varphi_4$). Αν η φ περιέχει την πρόταση z και η y περιέχει την $\neg z$, δημιουργούμε την πρόταση $w = \varphi^* \vee y^*$, όπου η φ^* (αντίστοιχα η y^*) προκύπτει από τη διαγραφή της z (αντίστοιχα της $\neg z$) από τη φ (αντίστοιχα από την y). Η w λέγεται **αποφαινόμενη** των φ, y ενώ οι φ, y λέγονται γονικές της w. Η δημιουργία της $w = \varphi^* \vee y^*$ σύμφωνα με την παραπάνω διαδικασία λέγεται **αρχή της απόφασης**.

Πριν προχωρήσουμε, υπενθυμίζουμε ότι προτάσεις της μορφής s, $\neg s$, $s_1 \vee s_2 \vee \cdots \vee s_k$ και $s_1 \wedge s_2 \wedge \cdots \wedge s_k$ (όπου $s_1, s_2, \ldots, s_k$ είναι άτομα, ή αρνήσεις ατόμων) μπορούν να θεωρηθούν ότι είναι γραμμένες σε κανονική συζευκτική μορφή.

Επίσης, είναι προφανές ότι αν θελήσουμε να βρούμε μια απόδειξη από ένα σύνολο υποθέσεων Σ' το οποίο αποτελείται από προτάσεις γραμμένες σε CNF, μπορούμε να θεωρήσουμε το σύνολο Σ'' το οποίο αποτελείται από τα μέρη της CNF που αποτελούνται μόνο από διαζεύξεις.

Παράδειγμα

Αντί για το σύνολο

$$\Sigma' = \{(p_1 \vee \neg p_2 \vee p_3) \wedge (p_4 \vee p_5), \neg p_6, p_7 \vee p_8, \neg p_9 \wedge p_{10}, (p_{11} \vee \neg p_{12}) \wedge p_{13} \wedge (p_{14} \vee \neg p_{15})\}$$

(και οι πέντε προτάσεις είναι σε CNF), μπορούμε να χρησιμοποιήσουμε το σύνολο

$$\Sigma'' = \{p_1 \vee \neg p_2 \vee p_3, p_4 \vee p_5, \neg p_6, p_7 \vee p_8, \neg p_9, p_{10}, p_{11} \vee \neg p_{12}, p_{13}, p_{14} \vee \neg p_{15}\}.$$

Για να αποδείξουμε μια πρόταση χρησιμοποιώντας την αρχή της απόφασης, χρησιμοποιούμε έναν αλγόριθμο απόδειξης που στηρίζεται στην παρακάτω διαδικασία:

Υποθέτουμε ότι η αποδεικτέα δεν είναι αληθής. Άρα η άρνησή της θα είναι αληθής. Εισάγουμε λοιπόν την άρνηση της αποδεικτέας στο σύνολο των αρχικών προτάσεων από τις οποίες προσπαθούμε να αποδείξουμε την αποδεικτέα πρόταση. Αφού γράψουμε όλες τις παραπάνω προτάσεις σε CNF και αφού τις διασπάσουμε (αν δεν είναι τετριμμένες) στα "μέρη" τους που χρησιμοποιούν μόνο διαζεύξεις, εφαρμόζουμε επαναληπτικά την αρχή της απόφασης, διαλέγοντας κάθε φορά δύο κατάλληλες προτάσεις του συνόλου που σχηματίσαμε, και παράγοντας την αποφαινόμενή τους, την οποία εισάγουμε στο αρχικό σύνολο προτάσεων. Συνεχίζουμε τη διαδικασία, μέχρι να φτάσουμε στην κενή πρόταση, που δίνει το άτοπο. (Στην ουσία, η κενή πρόταση προκύπτει από μια τελική εφαρμογή της αρχής της απόφασης, μεταξύ δύο προτάσεων π και $\neg\pi$, οι οποίες πράγματι δίνουν άτοπο.)

Ορισμός (**Απόδειξη με την αρχή της απόφασης**). *Απόδειξη της φ από το $\Sigma \subseteq P$ στο σύστημα παραγωγής που χρησιμοποιεί την αρχή της απόφασης (γράφουμε $\Sigma \vdash_r \varphi$) λέγεται μια πεπερασμένη ακολουθία προτάσεων $w_1, w_2, \ldots, w_n = \emptyset$ (η κενή πρόταση), όπου κάθε w_i είναι:*

1. *μια πρόταση του*[9] $\Sigma'' \cup \{\neg\varphi\}''$,
2. *παράγεται από δύο προηγούμενες προτάσεις της ακολουθίας με χρήση της αρχής της απόφασης.*

Αλγόριθμος απόδειξης με την αρχή της απόφασης

Βήμα 1. Μετατρέπουμε όλες τις προτάσεις του Σ σε CNF και δημιουργούμε έτσι το Σ'.

Βήμα 2. Δημιουργούμε την άρνηση της αποδεικτέας πρότασης φ (επίσης σε CNF).

Βήμα 3. Δημιουργούμε το σύνολο $\Sigma'' \cup \{\neg\varphi\}''$, διασπώντας (αν και όπου χρειάζεται) τις CNF στα "μέρη" που αποτελούνται από διαζεύξεις.

Βήμα 4. Επαναλαμβάνουμε τα παρακάτω, μέχρι να βρεθεί η κενή λέξη:

Διαλέγουμε δύο προτάσεις από το $\Sigma'' \cup \{\neg\varphi\}''$ και εφαρμόζουμε για αυτές την αρχή της απόφασης. Αν η παραγόμενη πρόταση (δηλαδή η αποφαινόμενη) είναι η κενή, τελειώσαμε. Αλλιώς, την προσθέτουμε στο σύνολο των διαθέσιμων προτάσεων και συνεχίζουμε, μέχρι να σχηματιστεί ως αποφαινόμενη η κενή πρόταση.

[9] Οι δύο τόνοι υποδηλώνουν μετατροπή των προτάσεων του Σ σε CNF και μετά, όπου χρειάζεται (δηλαδή για τις προτάσεις εκείνες που δεν είναι σε τετριμμένη μορφή), διάσπαση στα "μέρη" της CNF που αποτελούνται μόνο από διαζεύξεις.

Παράδειγμα 6.7.1. *Αν θέλουμε να δείξουμε ότι* $\Sigma \vdash_r \varphi$, *όπου* $\varphi = p_2 \wedge \neg p_3$ *και*

$$\Sigma = \{p_4 \wedge (p_4 \to p_1), \neg p_1 \vee \neg p_3, p_1 \to p_2, p_4 \vee \neg(p_2 \wedge p_5), p_6\},$$

ακολουθούμε τα εξής βήματα:

Βήμα 1:

1. Η $p_4 \wedge (p_4 \to p_1)$ γράφεται σε CNF: $(\neg p_1 \vee p_4) \wedge (\neg p_4 \vee p_1) \wedge (p_1 \vee p_4)$.
2. Η $\neg p_1 \vee \neg p_3$ είναι τετριμμένη (είναι ήδη σε CNF).
3. Η $p_1 \to p_2$ γράφεται σε CNF $\neg p_1 \vee p_2$.
4. Η $p_4 \vee \neg(p_2 \wedge p_5)$ γράφεται σε CNF $p_4 \vee \neg p_2 \vee \neg p_5$.
5. Η p_6 είναι τετριμμένη (είναι ήδη σε CNF).

Άρα, $\Sigma' = \{(\neg p_1 \vee p_4) \wedge (\neg p_4 \vee p_1) \wedge (p_1 \vee p_4), \neg p_1 \vee \neg p_3, \neg p_1 \vee p_2, p_4 \vee \neg p_2 \vee \neg p_5, p_6\}$.

Βήμα 2:
Η άρνηση της αποδεικτέας είναι η $\neg(p_2 \wedge \neg p_3)$, η οποία σε CNF γράφεται ως $\neg p_2 \vee p_3$.

Βήμα 3:
Διασπώντας την $(\neg p_1 \vee p_4) \wedge (\neg p_4 \vee p_1) \wedge (p_1 \vee p_4)$ (η οποία είναι η μόνη που χρειάζεται τέτοια διάσπαση) σε τρεις προτάσεις (τα "μέρη" της: $\neg p_1 \vee p_4$, $\neg p_4 \vee p_1$, $p_1 \vee p_4$), δημιουργούμε το σύνολο $\Sigma'' \cup \{\neg\varphi\}''$:

$$\Sigma'' \cup \{\neg\varphi\}'' = \{\neg p_1 \vee p_4, \neg p_4 \vee p_1, p_1 \vee p_4, \neg p_1 \vee \neg p_3, \neg p_1 \vee p_2, p_4 \vee \neg p_2 \vee \neg p_5, p_6, \underbrace{\neg p_2 \vee p_3}_{\{\neg\varphi\}''}\}.$$

Βήμα 4:
Εφαρμόζουμε επαναληπτικά την αρχή της απόφασης, μέχρι να πάρουμε την κενή πρόταση:

1.	$\neg p_2 \vee p_3$	Από το $\Sigma'' \cup \{\neg\varphi\}''$
2.	$\neg p_1 \vee p_4$	
3.	$\neg p_4 \vee p_1$	
4.	$p_1 \vee p_4$	
5.	$\neg p_1 \vee \neg p_3$	
6.	$\neg p_1 \vee p_2$	
7.	$p_4 \vee \neg p_2 \vee \neg p_5$	
8.	p_6	
9.	$p_1 \vee p_1$, (δηλαδή p_1)	(Από 3, 4 και αρχή απόφασης)
10.	p_2	(Από 6, 9 και αρχή απόφασης)
11.	$\neg p_1 \vee \neg p_2$	(Από 1, 5 και αρχή απόφασης)
12.	$\neg p_1$	(Από 10, 11 και αρχή απόφασης)
13.	η κενή πρόταση	(Από 9, 12 και αρχή απόφασης).

Παράδειγμα 6.7.2. *-Αν έχω TV και δεν είμαι απασχολημένος, θα δω το έργο.*
-Αν έχω video και είμαι απασχολημένος, θα γράψω το έργο.
-Αν γράψω το έργο, θα το δω.
-Έχω TV.
-Έχω video.
Να δειχθεί ότι θα δω οπωσδήποτε το έργο.

p :	Θα δω το έργο.
q :	Έχω TV.
r :	Είμαι απασχολημένος.
s :	Θα γράψω το έργο.
t :	Έχω video.

$$\Sigma = \{q \wedge \neg r \to p, \quad t \wedge r \to s, \quad s \to p, \quad q, \quad t\}.$$

Βήμα 1: $\Sigma' = \{\neg q \vee r \vee p, \quad \neg t \vee \neg r \vee s, \quad \neg s \vee p, \quad q, \quad t\}$.

Βήμα 2: Η άρνηση της αποδεικτέας είναι η $\neg p$ (η οποία είναι ήδη σε CNF).

Βήμα 3: Δεδομένου ότι $\Sigma'' = \Sigma'$, έχουμε ότι

$$\Sigma'' \cup \{\neg\phi\}'' = \{p \vee \neg q \vee r, \quad s \vee \neg t \vee \neg r, \quad p \vee \neg s, \quad q, \quad t, \quad \neg p\}.$$

Βήμα 4: Εφαρμόζουμε επαναληπτικά την αρχή της απόφασης, μέχρι να πάρουμε την κενή πρόταση:

1.	$p \vee \neg q \vee r$	Από το $\Sigma'' \cup \{\neg\varphi\}''$
2.	$\neg p$	
3.	q	
4.	$s \vee \neg t \vee \neg r$	
5.	$p \vee \neg s$	
6.	t	
7.	$\neg q \vee r$	(Από 1, 2 και αρχή απόφασης)
8.	r	(Από 3, 7 και αρχή απόφασης)
9.	$p \vee \neg t \vee \neg r$	(Από 4, 5 και αρχή απόφασης)
10.	$\neg t \vee \neg r$	(Από 2, 9 και αρχή απόφασης)
11.	$\neg r$	(Από 6, 10 και αρχή απόφασης)
12.	η κενή πρόταση	(Από 8, 11 και αρχή απόφασης).

6.7.1 Ασκήσεις προς επίλυση

1) Για τις προτάσεις p_1, p_2, p_3, p_4 γνωρίζουμε ότι

   (α΄) Αν η p_1 είναι αληθής, τότε και η p_2 είναι αληθής.

   (β΄) Η p_3 είναι αληθής αν και μόνο αν η p_4 είναι αληθής.

   (γ΄) Οι p_2 και p_4 δεν συναληθεύουν ποτέ.

   (δ΄) Η p_3 είναι αληθής.

   Να δειχθεί, με χρήση της αρχής της απόφασης, ότι οι p_1, p_2 είναι ψευδείς, ενώ οι p_3, p_4 είναι αληθείς.

2) Να αποδειχθεί, με χρήση της αρχής της απόφασης, ότι

   i) $\{\neg t \vee p, q \vee \neg p, t \vee \neg p\} \vdash_r q \vee (\neg p \wedge \neg q \wedge \neg t)$.

   ii) $\{\neg(p_1 \wedge p_6) \vee p_5, p_4, p_3 \rightarrow p_1, (p_5 \rightarrow p_3) \wedge p_5, \neg p_2 \vee \neg p_3\} \vdash_r \neg p_2 \wedge p_1$

   iii) $\{\neg p \vee s \vee \neg t, \neg t \vee p \vee \neg q, (q \wedge r) \rightarrow t, q \vee s \vee \neg t\} \vdash_r (q \wedge r) \rightarrow (s \vee \neg t)$.

6.8 Κατηγορηματικός Λογισμός

6.8.1 Εισαγωγή

Υπενθυμίζουμε ότι στη γλώσσα του Προτασιακού Λογισμού είχαν εισαχθεί

1. τα σύμβολα των ατόμων $p_1, p_2, \ldots$ (αριθμήσιμα σε πλήθος),
2. τα σύμβολα των συνδέσμων $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$,
3. οι παρενθέσεις $(,)$.

Τα σύμβολα αυτά ονομάζονται **λογικά σύμβολα**.

Ερώτηση
Μπορούν να εκφραστούν στη γλώσσα του προτασιακού λογισμού οι εκφράσεις:

1. Αν $x < 0$ και $y < 0$ τότε $x \cdot y > 0$.
2. Για κάθε x ισχύει ότι $\cos(x + 2\pi) = \cos(x)$.
3. Όλοι οι άνθρωποι είναι θνητοί.
   Ο Σωκράτης είναι άνθρωπος.
   Άρα, ο Σωκράτης είναι θνητός.

Απάντηση
Όχι, δεν μπορούν!
Θα χρειαστεί να εισάγουμε και **μη λογικά σύμβολα** στην γλώσσα του προτασιακού λογισμού.

Σταθερές
Η πρώτη κατηγορία μη λογικών συμβόλων είναι τα σύμβολα για **σταθερές**.

Παραδείγματα
Στην αριθμητική, σταθερά είναι το 0.
Στην άλγεβρα Boole, σταθερές είναι το 0 και 1.
Τις σταθερές θα τις συμβολίζουμε με $c_1, c_2, \ldots$ (αριθμήσιμες σε πλήθος).

Συναρτήσεις ή Πράξεις
Η δεύτερη κατηγορία μη λογικών συμβόλων είναι τα σύμβολα για **συναρτήσεις ή πράξεις**.

Παραδείγματα
Στην αριθμητική, η πράξη της πρόσθεσης + που αντιστοιχεί στους αριθμούς a, b το άθροισμά τους $+(a, b)$, (συνήθως γράφουμε $a + b$) και η πράξη του πολλαπλασιασμού $\cdot$ που αντιστοιχεί στους αριθμούς a, b το γινόμενό τους $\cdot(a, b)$, (συνήθως γράφουμε $a \cdot b$).

Στην θεωρία συναρτήσεων, η συνάρτηση cos που αντιστοιχεί στον αριθμό x την τιμή $\cos(x)$ του συνημιτόνου του, (συνήθως γράφουμε $\cos x$).

Στην αριθμητική, η πράξη του ΜΚΔ που αντιστοιχεί σε μια n-άδα φυσικών αριθμών τον μέγιστο κοινό διαιρέτη τους.

Παρατήρηση. Κάθε συνάρτηση μπορεί να θεωρηθεί μια πράξη και κάθε πράξη μια συνάρτηση.

Τις συναρτήσεις θα τις συμβολίζουμε με $f_1, f_2, \ldots$ (αριθμήσιμες σε πλήθος).

Ερώτηση

Τι κοινό έχουν τα μη λογικά σύμβολα των σταθερών και των συναρτήσεων;

Απάντηση

Και οι δύο κατηγορίες εκφράζουν αντικείμενα και όχι ιδιότητες αντικειμένων.

Μια συνάρτηση ή μια πράξη είναι ένας μηχανισμός ο οποίος αντιστοιχεί κάποια αντικείμενα σε ένα άλλο αντικείμενο.

Κατηγορήματα ή Σχέσεις

Η τρίτη κατηγορία μη λογικών συμβόλων είναι τα σύμβολα για **κατηγορήματα ή σχέσεις**.

Είναι εκφράσεις που περιγράφουν ιδιότητες αντικειμένων και "σχέσεις " μεταξύ τους.

Παραδείγματα

"x είναι περιττός".

"x είναι μικρότερο του y".

"x είναι ο μέγιστος κοινός διαιρέτης των y, z".

"Η σχέση R με $(x, y) \in R$ αν $x^2 - y > 5$".

Για μερικά κατηγορήματα στα Μαθηματικά χρησιμοποιούνται ειδικά σύμβολα π.χ. $=$, $<$, $\leq$, $\in$, κ.α.

Με τη βοήθεια των λογικών συνδέσμων σχηματίζουμε πιο σύνθετα κατηγορήματα από άλλα απλούστερα. Έτσι, η έκφραση

$$x \text{ είναι περιττός και } x \text{ είναι ο μέγιστος κοινός διαιρέτης των } y, z$$

είναι ένα νέο κατηγόρημα.

Παράδειγμα

Αν $x < 0$ και $y < 0$ τότε $x \cdot y > 0$.

Σύμβολα σταθερών: Η σταθερά 0.

Σύμβολα συναρτήσεων: Η συνάρτηση $\cdot$ που απεικονίζει το ζεύγος x, y στο γινόμενό του.

Σύμβολα κατηγορημάτων: Το κατηγόρημα $>$ που εκφράζει την ιδιότητα του μεγαλύτερου.

Μαζί με τα λογικά σύμβολα της γλώσσας του προτασιακού λογισμού, δίνουν

$$(x < 0) \wedge (y < 0) \rightarrow (x \cdot y > 0).$$

Εκτός από μη λογικά απαιτείται να εισάγουμε και νέα λογικά σύμβολα.

Ποσοδείκτες

Οι λέξεις "για κάθε" και "υπάρχει" λέγονται **καθολικός ποσοδείκτης** και **υπαρξιακός ποσοδείκτης** και συμβολίζονται με $\forall$ και $\exists$ αντίστοιχα.

Ισότητα

Το σύμβολο $\approx$ το οποίο αναφέρεται στην ισότητα της γλώσσας (και συμβολίζεται με $\approx$ για να διακρίνεται από την ισότητα $=$ της μεταγλώσσας).

Νέα κατηγορήματα σχηματίζουμε επίσης με τη χρήση των ποσοδεικτών "(για) κάθε" και "υπάρχει". Οι εκφράσεις

"κάθε x είναι περιττός",

"υπάρχει x μικρότερο του y",

"υπάρχει x που είναι μέγιστος κοινός διαιρέτης των y, z",

είναι πάλι κατηγορήματα.

Παράδειγμα

Για κάθε x ισχύει ότι $\cos(x + 2\pi) = \cos x$

Σύμβολα σταθερών: π.
Σύμβολα συναρτήσεων: n πρόσθεση $+$, ο διπλασιασμός d και n συνάρτηση cos.
Σύμβολα κατηγορημάτων: n ισότητα $\approx$.
Μαζί με τα λογικά σύμβολα του προτασιακού λογισμού και τον καθολικό ποσοδείκτη δίνουν

$$(\forall x)(\cos(x + d(\pi)) \approx \cos x.$$

6.8.2 Πρωτοβάθμια γλώσσα

α) λογικά σύμβολα:

i) συνδέσμοι : $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

ii) ποσοδείκτες : $\forall$ (καθολικός), $\exists$ (υπαρξιακός).

iii) ισότητα : $\approx$.

iv) μεταβλητές : $x_1, x_2, \ldots$ (αριθμήσιμο πλήθος).

v) παρενθέσεις : (,).

β) μη λογικά σύμβολα:

vi) σχέσεις[10] P_i, $i \in I$.

vii) συναρτήσεις f_j, $j \in J$.

viii) σταθερές c_k, $k \in K$.

όπου I, J, K είναι κάποια σύνολα δεικτών πεπερασμένα ή άπειρα (αλλά αριθμήσιμα).

Παρατήρηση. Επειδή τα λογικά σύμβολα είναι αναπόσπαστο κομμάτι κάθε πρωτοβάθμιας γλώσσας δε χρειάζεται να τα αναφέρουμε κάθε φορά.

Κάθε συγκεκριμένη γλώσσα προσδιορίζεται από τα μη λογικά της σύμβολα.
Γενικά μια πρωτοβάθμια γλώσσα έχει τη μορφή

$$L =< (P_i)_{i\in I}; (f_j)_{j\in J}; (c_k)_{k\in K} > .$$

Παραδείγματα[11]

1) **Η γλώσσα της ισότητας**

$$L =<; ; > .$$

2) **Η γλώσσα της συνολοθεωρίας**

$$L =<\in; ; > .$$

3) **Η γλώσσα της αριθμητικής**

$$L =<; +, \cdot, s, ; 0 > .$$

[10] Κάθε σχέση είναι ένα κατηγόρημα.

[11] Σε όποια από τις τρεις θέσεις δεν εμφανίζεται τίποτα, σημαίνει ότι το αντίστοιχο σύνολο λογικών συμβόλων (σχέσεων, συναρτήσεων, σταθερών) είναι κενό. Υπενθυμίζουμε πάντως ότι πάντα υπάρχουν τα λογικά σύμβολα.

4) **Η γλώσσα της διάταξης**

$$L = < \lhd ; ; > .$$

5) **Η γλώσσα των ομάδων**

$$L = <; +, ^{-}; 0 > .$$

6) **Η γλώσσα της άλγεβρας Boole**

$$L = <; +, \cdot, ^{-}; 0, 1 > .$$

Έστω L μια πρωτοβάθμια γλώσσα. **Έκφραση** της L είναι μια πεπερασμένη ακολουθία συμβόλων της γλώσσας.

Οι **ορθά σχηματισμένες εκφράσεις** μιας πρωτοβάθμιας γλώσσας είναι κάποιες εκφράσεις που υπακούουν σε ορισμένους κανόνες.

Υπάρχουν δύο είδη ορθά σχηματισμένων εκφράσεων:

1. οι **όροι** ή **ονόματα** (που περιγράφουν αντικείμενα) και
2. οι **τύποι** (που περιγράφουν ιδιότητες των αντικειμένων).

Όροι

α) Οι μεταβλητές και οι σταθερές της L είναι όροι.

β) Αν το f_j είναι σύμβολο n-μελούς πράξεις και οι $t_1, \ldots, t_n$ είναι όροι, η έκφραση $f_j(t_1, \ldots, t_n)$ είναι όρος.

γ) Το σύνολο $T(L)$ των όρων της L είναι το ελάχιστο που ικανοποιεί τις συνθήκες α), β).

Παραδείγματα

Στη γλώσσα L της αριθμητικής το $s(0)$ είναι όρος και το παριστάνουμε με 1. Το $s(s(0))$ είναι το 2 κ.ο.κ.

Αν τα x_1, x_2 είναι όροι τότε τα $x_1 + x_2$, $x_1 \cdot x_2$ είναι όροι.

Οι εκφράσεις $((s(x_1) + 0) \cdot s(s(x_2))) + s(s(s(0)))$, $((0 \cdot s(x_{10})) \cdot s(s(x_5))) + s(0)$ είναι όροι.

Δεν είναι όρος η έκφραση $s(x_1) \approx s(s(x_1))$.

Τύποι

Το σύνολο $F(L)$ των τύπων της L ορίζεται ως εξής:

α) Ατομικοί τύποι

i) Για κάθε σύμβολο n-μελούς σχέσης P_i και κάθε n-άδα όρων $(t_1, \ldots, t_n)$, η έκφραση

$$P_i(t_1, \ldots, t_n)$$

είναι τύπος.

ii) Για κάθε ζεύγος όρων (t, s) η έκφραση

$$t \approx s$$

είναι τύπος.

β) Αν οι ϕ, ψ είναι τύποι, οι εκφράσεις

$$\neg\phi, \phi \wedge \psi, \phi \vee \psi, \phi \to \psi, \phi \leftrightarrow \psi$$

είναι τύποι.

γ) Αν ο ϕ είναι τύπος, για κάθε μεταβλητή x_i οι εκφράσεις

$$(\forall x_i)\phi \text{ και } (\exists x_i)\phi$$

είναι τύποι.

δ) Το σύνολο $F(L)$ είναι το ελάχιστο που ικανοποιεί τις συνθήκες α)-γ).

Παράδειγμα.
Οι εκφράσεις

$$\neg(\exists x_i)(x_i \approx c_j)$$

$$(\forall x_i)((x_i \approx f_k(c_1, c_2)) \to P_x(x_i, c_3))$$

όπου f_k διμελής συνάρτηση και P_l διμελής σχέση, είναι τύποι.
Δεν είναι όμως τύπος η έκφραση

$$P_l(x_1, x_2) \to ((\exists x_k)(\neg x_k)).$$

6.8.3 Ελεύθερες και δεσμευμένες μεταβλητές

Στους τύπους $(\forall x)\phi$ και $(\exists x)\phi$, ο τύπος ϕ λέγεται **εμβέλεια** (ή ακτίνα) του αντίστοιχου ποσοδείκτη.

"Κανόνας": Η εμβέλεια ενός ποσοδείκτη είναι η ελάχιστη έκφραση που ακολουθεί αμέσως μετά τον ποσοδείκτη και είναι τύπος.

Παράδειγμα
Η εμβέλεια του $\exists x_2$ στον τύπο

$$\forall x_1(0 < x_1 \to \exists x_2(0 < x_2 \wedge x_2 \cdot x_1 \approx x_1))$$

είναι ο τύπος

$$(0 < x_2 \wedge x_2 \cdot x_1 \approx x_1)$$

Μια εμφάνιση της μεταβλητής x μέσα στον τύπο ϕ λέγεται **δεσμευμένη**, αν είναι εμφάνιση της μορφής $(\forall x)$, $(\exists x)$ ή είναι εμφάνιση στην εμβέλεια των ποσοδεικτών αυτών.

Κάθε άλλη εμφάνιση της μεταβλητής λέγεται **ελεύθερη**.

Η x λέγεται **ελεύθερη** στον τύπο ϕ αν έχει μια τουλάχιστον ελεύθερη εμφάνιση στο ϕ. Αλλιώς λέγεται **δεσμευμένη**.

Παράδειγμα
Ο τύπος

$$((\forall x)R(x, y)) \vee ((\exists y)R(x, y))$$

έχει μια ελεύθερη και μια δεσμευμένη εμφάνιση των μεταβλητών x, y. Άρα και η x και η y είναι ελεύθερες μεταβλητές στον παραπάνω τύπο.

Ο τύπος ϕ λέγεται **πρόταση** αν δεν περιέχει καθόλου ελεύθερες μεταβλητές. Άρα ο παραπάνω τύπος δεν είναι πρόταση.

Συμβολίζουμε με $S(L)$ το σύνολο των προτάσεων της L.

Οι τύποι με ελεύθερες μεταβλητές λέγονται **ανοιχτοί τύποι**, ενώ οι προτάσεις λέγονται **κλειστοί τύποι**.

Παραδείγματα

Ο τύπος

$$(\forall x_1)(\exists x_2)((x_1 < x_2) \vee (x_2 < x_1))$$

είναι πρόταση.

Ο τύπος

$$((\forall x)P(x)) \to ((\forall y)(x \approx y))$$

δεν είναι πρόταση, επειδή η x έχει μια ελεύθερη εμφάνιση (και δύο δεσμευμένες).

Παρόμοια ορολογία χρησιμοποιείται και για τους όρους.

Ένα όρος που περιέχει μεταβλητές (εδώ φυσικά δεν μιλούμε για ελεύθερες και δεσμευμένες) θα λέγεται **ανοιχτός**, ενώ στην αντίθετη περίπτωση θα λέγεται **κλειστός**.

Παραδείγματα

Αν x είναι μεταβλητή και a, b είναι σταθερές τότε:

Ο όρος $x + 3$ είναι ανοιχτός.

Ο όρος $f(a).g(b)$ είναι κλειστός.

6.8.4 Επαγωγικός ορισμός

Όλες οι έννοιες που ορίστηκαν επαγωγικά για τις προτάσεις του Προτασιακού Λογισμού, $\mathrm{sub}(\phi)$, $r(\phi)$ κ.λπ. μπορούν να ορισθούν όμοια για τους τύπους.

Η βασική ιδέα είναι ότι ορίζουμε πρώτα την αντίστοιχη έννοια για τους όρους και την επεκτείνουμε στους ατομικούς τύπους στη συνέχεια για όλους τους τύπους.

Συμβολίζουμε με F_0 το σύνολο των ατομικών τύπων της L.

Έστω $f : F_0 \to V$ μια απεικόνιση από το σύνολο F_0 στο σύνολο V.

Αν δοθούν απεικονίσεις $G_\square : V \times V \to V$, $G_\neg : V \to V$, $G_\forall : V \times N \to V$, $G_\exists : V \times N \to V$, τότε υπάρχει μοναδική συνάρτηση $\bar{f} : F(L) \to V$ τέτοια ώστε:

α) $\bar{f}(\phi) = f(\phi)$ για κάθε $\phi \in F_0$.

β) $\bar{f}(\phi \square \psi) = G_\square(\bar{f}(\phi), \bar{f}(\psi))$,

γ) $\bar{f}(\neg\phi) = G_\neg(\bar{f}(\phi))$,

δ) $\bar{f}((\forall x_i)\phi) = G_\forall(\bar{f}(\phi), i)$,

ε) $\bar{f}((\exists x_i)\phi) = G_\exists(\bar{f}(\phi), i)$.

Έστω $FV(t)$, $FV(\phi)$ τα σύνολα των μεταβλητών του όρου t και των ελεύθερων μεταβλητών του τύπου ϕ.

Ο επαγωγικός ορισμός τους είναι ο εξής:

Ορισμός του $FV(t)$:

i) $FV(x_i) = \{x_i\}$

ii) $FV(c_i) = \emptyset$.

iii) $FV(f(t_1, \ldots, t_n)) = FV(t_1) \cup \cdots \cup FV(t_n)$.

Ορισμός του $FV(\phi)$:

i) $FV(P(t_1, \ldots, t_n)) = FV(t_1) \cup \cdots \cup FV(t_n)$.

ii) $FV(t \approx s) = FV(t) \cup FV(s)$.

iii) $FV(\phi \square \psi) = FV(\phi) \cup FV(\psi)$.

iv) $FV(\neg\phi) = FV(\phi)$

v) $FV((\forall x_i)\phi) = FV((\exists x_i)\phi) = FV(\phi) \setminus \{x_i\}$.

Γράφουμε $\varphi(x_1, \ldots, x_n)$ για να δηλώσουμε ότι οι ελεύθερες μεταβλητές του τύπου ϕ περιλαμβάνονται στο σύνολο $\{x_1, \ldots, x_n\}$. Για συντομία, γράφουμε $\varphi(\vec{x})$, θεωρώντας $\vec{x} = (x_1, x_2, \ldots, x_n)$. Αν $\vec{t} = (t_1, t_2, \ldots, t_n)$ είναι μια ακολουθία όρων, με $\varphi(\vec{t})$ συμβολίζουμε τον τύπο που προκύπτει αντικαθιστώντας κάθε εμφάνιση του x_i με t_i.

Παράδειγμα

Για τον τύπο $\phi : (\forall x)(x = 5y)$ γράφουμε $\phi(y)$.

Αν $\phi(x)$ και t είναι ένας όρος τότε με $\phi(t)$ συμβολίζουμε την αντικατάσταση στον τύπο ϕ κάθε ελεύθερης εμφάνισης της x από τον όρο t.

Παράδειγμα

Για τον προηγούμενο τύπο έχουμε:
$\phi(z) : (\forall x)(x = 5z)$.
$\phi(x) : (\forall x)(x = 5x)$.

Παρατηρούμε ότι στην πρώτη αντικατάσταση ο τύπος παραμένει ο ίδιος ενώ στη δεύτερη ο τύπος διαφέρει σημαντικά από τον αρχικό καθώς είναι πλέον πρόταση και μάλιστα ψευδής. Πρόκειται για αντικατάσταση που άλλαξε τη δομή του τύπου. Τέτοιες αντικαταστάσεις δεν επιτρέπονται.

6.8.5 Αντικατάσταση

Επιτρέπεται η αντικατάσταση όταν ο όρος t που μπαίνει στην θέση της ελευθερης μεταβλητής **δεν περιέχει μεταβλητές που να μετατρέπονται σε δεσμευμένες μέσα στον** ϕ.

Αν $\phi(x)$ είναι ένας τύπος και t είναι ένας όρος τότε λέμε ότι η x είναι αντικαταστάσιμη από τον t στο $\phi(x)$ αν κάθε μεταβλητή του όρου t παραμένει ελεύθερη στον $\phi(t)$.

Ορισμός: Αν $\phi(x)$ είναι ένας τύπος και t είναι ένας όρος τότε λέμε ότι **η** x **είναι αντικαταστάσιμη από τον** t **στο** $\phi(x)$ αν καμιά ελεύθερη εμφάνιση της x στον ϕ δεν βρίσκεται στην εμβέλεια ενός ποσοδείκτη $\forall y$ ή $\exists y$, όπου y είναι μια μεταβλητή που εμφανίζεται στον t.

Παράδειγμα

Έστω ο τύπος ϕ:

$$((\exists x)\psi(x, y)).$$

Η y είναι ελεύθερη στον ϕ. Η y είναι αντικαταστάσιμη από τους όρους z, ή 2, ή ακόμα $f(w, w)$, οπότε προκύπτουν οι τύποι

$$((\exists x)\psi(x, z)), ((\exists x)\psi(x, 2)), ((\exists x)\psi(x, f(w, w))).$$

αντίστοιχα. Αντίθετα η y δεν είναι αντικαταστάσιμη από τον όρο $f(x,w)$ καθώς στον τύπο που προκύπτει

$$((\exists x)\psi(x,f(x,w)))$$

η μεταβλητή x του όρου $f(x,w)$ είναι δεσμευμένη.

Αν $\phi(x)$:

$$((\exists y)R(x,y)) \wedge ((\exists z)\neg Q(x,z))$$

και $t : f(w,u)$, τότε η x είναι αντικαταστάσιμη από τον t καθώς $\phi(t)$:

$$((\exists y)R(f(w,u),y)) \wedge ((\exists z)\neg Q((f(w,u),z))$$

και w,u ελεύθερες για τον ϕ. Αντίθετα, αν $t : g(y,s(y))$ τότε η x δεν είναι αντικαταστάσιμη από τον t καθώς η πρώτη ελεύθερη εμφάνιση της x στον φ βρίσκεται στην εμβέλεια του $\exists y$.

Αν η x είναι αντικαταστάσιμη από τον όρο t στον τύπο $\phi(x)$, συμβολίζουμε με $\varphi[\mathbf{x}/\mathbf{t}]$ την έκφραση που προκύπτει αν αντικαταστήσουμε την x με τον t στον $\varphi(x)$. Η έκφραση $[x/t]$ ονομάζεται **αντικατάσταση** της μεταβλητής x από τον όρο θ. Μπορούμε ανάλογα να ορίσουμε αντικαταστάσεις πολλών μεταβλητών π.χ. x,y,z από τους όρους π.χ. t,s,u αντίστοιχα και να την συμβολίζουμε με $[\theta] = [x/t, y/s, z/u]$. Αν μια μεταβλητή έχει πάνω από μια ελεύθερη εμφάνιση, μπορούμε να αντικαταστήσουμε μία ή περισσότερες από τις ελεύθερες εμφανίσεις της.

Δύο εκφράσεις φ_1 και φ_2 ονομάζονται **ενοποιήσιμες (unifiable)** αν και μόνο αν υπάρχει αντικατάσταση $[\theta]$ ώστε $\varphi_1[\theta] = \varphi_2[\theta]$, στην περίπτωση αυτή λέμε ότι οι φ_1, φ_2 **ενοποιούνται**.

Π.χ. οι τύποι $\varphi_1 = R(1,y)$ και $\varphi_2 = R(x,4)$ είναι ενοποιήσιμοι, διότι με την αντικατάσταση $[\theta] = [x/1, y/4]$ προκύπτει $\varphi_1[\theta] = \varphi_2[\theta] = R(1,4)$.

Οι όροι $t_1 = f(x,y,z)$ και $t_1 = f(z,y,y)$ είναι ενοποιήσιμοι, διότι με την αντικατάσταση $[\theta] = [y/x, z/x]$ προκύπτει $t_1[\theta] = t_2[\theta] = f(x,x,x)$.

Η διαδικασία με την οποία δύο εκφράσεις φ_1, φ_2 γίνονται (συντακτικά) ίδιες με την χρήση μιας αντικατάστασης $[\theta]$ ονομάζεται **ενοποίηση (unification)** και η αντικατάσταση $[\theta]$ ονομάζεται **ενοποιητής (unifyier)**.

i) Δύο σταθερές ενοποιούνται αν και μόνο αν είναι ίσες.

ii) Μια μεταβλητή ενοποιείται με οποιοδήποτε όρο.

iii) Δύο όροι $f_1(t_1,t_2,\ldots,t_n)$ και $f_2(t',t'_2,\ldots,t'_m)$ είναι ενοποιήσιμοι, αν και μόνο αν $f_1 = f_2$, $n = m$ και για κάθε $i \in [n]$ οι όροι t_i και t'_i είναι επίσης ενοποιήσιμοι.

iv) Δύο ατομικοί $R_1(t_1,t_2,\ldots,t_n)$ και $R_2(t'_1,t'_2,\ldots,t'_m)$ είναι ενοποιήσιμοι, αν και μόνο αν $R_1 = R_2$, $n = m$ και για κάθε $i \in [n]$ οι όροι t_i και t'_i είναι επίσης ενοποιήσιμοι.

6.8.6 Επαγωγική απόδειξη

Έστω $A(\phi)$ μια ιδιότητα της μεταγλώσσας που αναφέρεται στους τύπους. Αν

α) $A(\phi)$ αληθεύει για κάθε ατομικό τύπο,

β) $A(\phi)$ και $A(\psi) \Rightarrow A(\phi \square \psi)$,

γ) $A(\phi) \Rightarrow A(\neg\phi)$,

δ) $A(\phi) \Rightarrow A((\forall x_i)\phi)$ και $A((\exists x_i)\phi)$ για κάθε x_i,

τότε η $A(\phi)$ αληθεύει για κάθε $\phi \in F(L)$.

6.8.7 Ασκήσεις προς επίλυση

1) i) Να βρεθούν οι ελεύθερες και δεσμευμένες μεταβλητές στους παρακάτω τύπους :

$\phi_1 : (\forall x_1)((\forall x_2)(\forall x_3)(x_1 \in x_2) \vee (x_2 \in x_3) \vee (x_3 \in x_1))$

$\phi_2 : (\forall x_1)(\forall x_2)((\forall x_3)(x_1 \in x_2) \vee (x_2 \in x_3) \vee (x_3 \in x_1))$

$\phi_3 : (\forall x_1)(\forall x_2)(\forall x_3)((x_1 \in x_2) \vee (x_2 \in x_3) \vee (x_3 \in x_1))$

$\phi_4 : (\forall x_1)(x_1 \in x_2) \vee (\forall x_2)(x_2 \in x_1) \vee (\forall x_2)(x_2 \in x_1)$

$\phi_5 : (\forall x_1)((x_1 \in x_2) \vee (\forall x_2)(x_2 \in x_1) \vee (\forall x_1)(x_1 \in x_2))$

$\phi_6 : (\forall x_1)((x_1 \in x_2) \vee (\forall x_2)((x_2 \in x_1) \vee (\forall x_1)(x_1 \in x_2)))$

ii) Να εξετασθεί αν κάποιες από τις ϕ_1, ϕ_2, ϕ_3, ϕ_4, ϕ_5, ϕ_6 είναι προτάσεις.

2) i) Αν $x_1, x_2, \ldots$ είναι μεταβλητές και $c_1, c_2, \ldots$ είναι σταθερές, να εξετασθεί ποιες από τις παρακάτω εκφράσεις της γλώσσας της θεωρίας των συνόλων είναι τύποι.

α) $(\exists x_1)(x_1 \approx c_1)$

β) $(x_1 \approx x_3) \rightarrow (\forall x_1)(x_1 \vee x_2)$

γ) $(\forall x_1)((x_1 \in x_2) \vee ((\forall x_2)(x_2 \in x_1) \vee (\forall x_1)(x_1 \in x_2)))$

ii) Αν κάποια από τις προηγούμενες εκφράσεις είναι τύπος, να βρεθούν οι ελεύθερες και δεσμευμένες μεταβλητές του και να εξετασθεί αν είναι πρόταση.

3) i) Να βρεθούν οι ελεύθερες και δεσμευμένες μεταβλητές στους παρακάτω τύπους και να εξετασθεί ποιος από τους παρακάτω τύπους είναι πρόταση.

α) $(\forall x_1)\,((\exists x_2)(x_2 \leq x_1) \vee (x_2 \geq x_1))$.

β) $(\forall x_1)(\exists x_2)\,((x_1 \leq x_2) \vee (x_2 \geq x_1))$.

ii) Να εξετασθεί σε ποιους από τους παρακάτω τύπους η x_1 είναι αντικαταστάσιμη από τον όρο $x_3 \geq x_2$.

α) $(\exists x_2)(x_2 \leq x_3) \vee (x_2 \geq x_1)$.

β) $(\exists x_2)\,((x_3 \leq x_2) \vee (x_2 \geq x_1))$.

6.9 Παράρτημα: Λογικοί γρίφοι και προβλήματα

Παράδειγμα 6.9.1. *Έστω 5 κάρτες, οι οποίες περιέχουν από τη μία πλευρά έναν αριθμό και από την άλλη πλευρά ένα γράμμα.*

A	*K*	*5*	*6*	*7*

Ποιές κάρτες πρέπει να γυρίσουμε για να ελέγξουμε αν αληθεύει η πρόταση
S : Αν η κάρτα έχει φωνήεν στην μια πλευρά τότε έχει άρτιο αριθμό στην άλλη πλευρά.

Λύση. Αρκεί να γυρίσουμε τις κάρτες: Α, 5 και 7.

Έχουμε τις εξής περιπτώσεις:

Γράμμα	Ψηφίο	*S*
Φωνήεν	Άρτιος	Αληθής
Φωνήεν	Περιττός	Ψευδής
Σύμφωνο	Άρτιος	Αληθής
Σύμφωνο	Περιττός	Αληθής

Η περίπτωση όπου η S είναι ψευδής είναι μόνο όταν έχουμε φωνήεν μαζί με περιττό.
Άρα γυρίζω μόνο αυτές που έχουν ή φωνήεν, ή περιττό. □

Παράδειγμα 6.9.2. *Οι κάτοικοι ενός χωριού χωρίζονται σε δύο ομάδες. Όσοι ανήκουν στην πρώτη λένε πάντα αλήθεια, ενώ όσοι ανήκουν στη δεύτερη λένε πάντα ψέματα. Ένας τουρίστας φτάνει σε μια διχαλωτή διασταύρωση του χωριού, της οποίας μόνο ο ένας κλάδος οδηγεί στην πρωτεύουσα. Επειδή δεν υπάρχουν σχετικές πινακίδες, απευθύνεται σε ένα κάτοικο που συναντά. Ζητείται να ευρεθεί η ερώτηση που πρέπει να κάνει, ώστε να ακολουθήσει τον κλάδο που οδηγεί στην πρωτεύουσα.*

Λύση. Θεωρούμε τις προτάσεις:

p: Λέω την αλήθεια.

q: Ο αριστερός κλάδος οδηγεί στην πρωτεύουσα.

Μας ενδιαφέρει να εξακριβώσουμε αν η πρόταση q είναι αληθής ή όχι. Η τιμή αληθείας της πρότασης p δεν μας ενδιαφέρει.

Η βασική ιδέα της λύσης είναι να κατασκευάσουμε μια πρόταση φ τέτοια ώστε: Αν ρωτήσουμε οποιοδήποτε κάτοικο του χωριού αν η φ είναι αληθής ή όχι, τότε η *απάντηση που θα μας δώσει* να ταυτίζεται με την πραγματική τιμή αληθείας της πρότασης q.

Αν συμβολίσουμε με $ans(\varphi)$ την απάντηση στην ερώτηση αν η φ είναι αληθής, τότε υπάρχουν οι παρακάτω περιπτώσεις:

p	q	φ	$ans(\varphi)$
A		*A*	*A*
A		Ψ	Ψ
Ψ		*A*	Ψ
Ψ		Ψ	*A*

Συμπληρώνουμε τις τιμές αληθείας του q αντιγράφοντας τις απαντήσεις $ans(\varphi)$.

p	q	φ	$ans(\varphi)$
A	A	A	A
A	Ψ	Ψ	Ψ
Ψ	Ψ	A	Ψ
Ψ	A	Ψ	A

Επομένως, η ζητούμενη πρόταση φ έχει πίνακα αληθείας

p	q	φ
A	A	A
A	Ψ	Ψ
Ψ	Ψ	A
Ψ	A	Ψ

Άρα, η ζητούμενη πρόταση φ είναι λογικά ισοδύναμη με την πρόταση $p \leftrightarrow q$.

Επομένως, θα ρωτήσουμε οποιονδήποτε κάτοικο αν η πρόταση "Λες αλήθεια αν και μόνο αν ο αριστερός κλάδος οδηγεί στην πρωτεύουσα" είναι αληθής ή όχι.

Αν η απάντηση του είναι αληθής, τότε και η q είναι αληθής. Διαφορετικά, η q θα είναι ψευδής. □

Παράδειγμα 6.9.3. *Σε ένα ξενοδοχείο γίνονται ταυτόχρονα δύο συνέδρια: Ένα συνέδριο αστρονομίας και ένα συνέδριο αστρολογίας. Οι αστρονόμοι λένε πάντα την αλήθεια, ενώ οι αστρολόγοι λένε πάντα ψέματα. Οι σύνεδροι κάθε ομάδας γνωρίζονται μεταξύ τους.*

Συναντάμε δύο συνέδρους, τον A και τον B.

- Ο A λέει: Ο B είναι αστρονόμος.

- Ο B λέει: Οι δυο μας είμαστε διαφορετικοί.

Να βρεθεί τι είναι οι A, B.

Απόδειξη. Θεωρούμε τις προτάσεις:

p: Ο B είναι αστρονόμος.

q: Οι A, B είναι διαφορετικοί.

Διακρίνουμε περιπτώσεις:

1η περίπτωση: Ο A είναι αστρονόμος.

Επομένως, ο A λέει αλήθεια.

Επομένως, η πρόταση p είναι αληθής, δηλαδή ο B είναι αστρονόμος.

Επομένως, ο B λέει αλήθεια.

Επομένως, η πρόταση q είναι αληθής, το οποίο είναι άτοπο. Άρα, η περίπτωση αυτή δεν ισχύει.

2η περίπτωση: Ο A είναι αστρολόγος.

Επομένως, ο A λέει ψέματα.

Επομένως, η πρόταση p είναι ψευδής, δηλαδή ο B είναι αστρολόγος.

Επομένως, ο B λέει ψέματα.

Επομένως, η πρόταση q είναι ψευδής, το οποίο είναι σωστό. Άρα, η περίπτωση που ισχύει είναι ότι οι A, B είναι αστρολόγοι.

□

Παράδειγμα 6.9.4. *Επτά κωμικοί A, B, C, D, E, F, G πρόκειται να δώσουν παραστάσεις μιας βραδιάς, σε δύο από πέντε ξενοδοχεία μιας πόλης, κατά τη διάρκεια ενός τριήμερου φεστιβάλ. Σε κάθε παράσταση μπορεί να συμμετέχει μόνο ένας κωμικός. Κάθε ένας από αυτούς είναι διαθέσιμος, λόγω άλλων υποχρεώσεων, μόνο δύο από τις μέρες αυτές ως εξής:*

1) Ο A μπορεί να πάει στο Aladdin και στο Caesars τις μέρες 1 και 2.

2) Ο B μπορεί να πάει στο Bellagio και στο Excalibur τις μέρες 1 και 2.

3) Ο C μπορεί να πάει στο Desert και στο Excalibur τις μέρες 2 και 3.

4) Ο D μπορεί να πάει στο Aladdin και στο Desert τις μέρες 1 και 3.

5) Ο E μπορεί να πάει στο Caesars και στο Excalibur τις μέρες 1 και 3.

6) Ο F μπορεί να πάει στο Bellagio και στο Desert τις μέρες 2 και 3.

7) Ο G μπορεί να πάει στο Bellagio και στο Caesars τις μέρες 1 και 2.

Ζητείται να ευρεθεί αν είναι δυνατή η πραγματοποίηση των παραστάσεων αυτών.

Λύση. Θεωρούμε τις 7 προτάσεις:

a: Ο A πηγαίνει στο Aladdin την ημέρα 1 και στο Caesars την ημέρα 2.

b: Ο B πηγαίνει στο Bellagio την ημέρα 1 και στο Excalibur την ημέρα 2.

c: Ο C πηγαίνει στο Desert την ημέρα 2 και στο Excalibur την ημέρα 3.

d: Ο D πηγαίνει στο Aladdin την ημέρα 1 και στο Desert την ημέρα 3.

e: Ο E πηγαίνει στο Caesars την ημέρα 1 και στο Excalibur την ημέρα 3.

f: Ο F πηγαίνει στο Bellagio την ημέρα 2 και στο Desert την ημέρα 3.

g: Ο G πηγαίνει στο Bellagio την ημέρα 1 και στο Caesars την ημέρα 2.

Η άρνηση κάθε μιας από τις προτάσεις αυτές αντιστοιχεί στο ότι οι μέρες προγραμματίζονται ανάποδα, για παράδειγμα,

$\neg a$: Ο A πηγαίνει στο Aladdin την ημέρα 2 και στο Caesars την ημέρα 1.

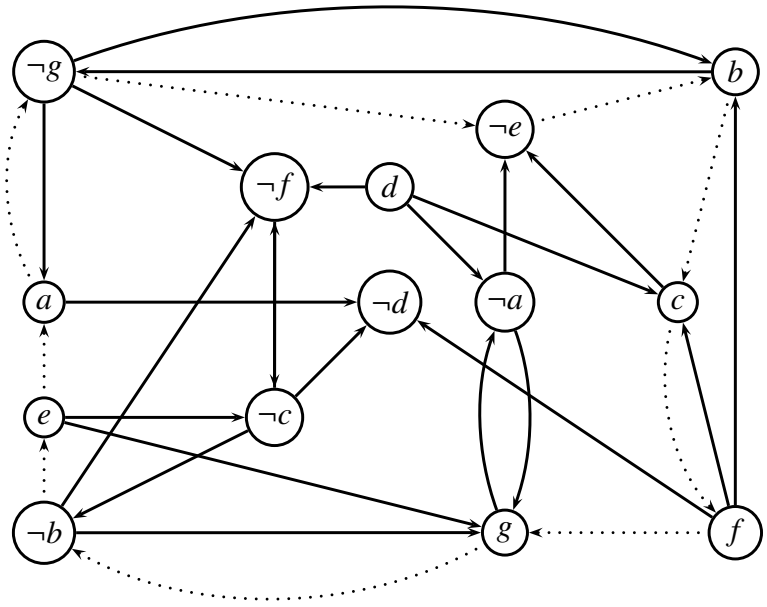
Έτσι, συγκεντρωτικά για κάθε κωμικό έχουμε τις παρακάτω περιπτώσεις:

Κωμικός	Πρόταση	1η μέρα	2η μέρα	3η μέρα
A	a	Aladdin	Caesars	-
A	$\neg a$	Caesars	Aladdin	-
B	b	Bellagio	Excalibur	-
B	$\neg b$	Excalibur	Bellagio	-
C	c	-	Desert	Excalibur
C	$\neg c$	-	Excalibur	Desert
D	d	Aladdin	-	Desert
D	$\neg d$	Desert	-	Aladdin
E	e	Caesars	-	Excalibur
E	$\neg e$	Excalibur	-	Caesars
F	f	-	Bellagio	Desert
F	$\neg f$	-	Desert	Bellagio
G	g	Bellagio	Caesars	-
G	$\neg g$	Caesars	Bellagio	-

Τώρα μπορούμε να γράψουμε τους περιορισμούς που εξασφαλίζουν ότι κανένα ζευγάρι κωμικών δε θα βρεθεί στο ίδιο ξενοδοχείο την ίδια μέρα.

$a \to \neg d$	και	$d \to \neg a$	$\neg b \to g$	και	$\neg g \to b$
$a \to \neg g$	και	$g \to \neg a$	$c \to f$	και	$\neg f \to \neg c$
$\neg a \to \neg e$	και	$e \to a$	$c \to \neg e$	και	$e \to \neg c$
$\neg a \to g$	και	$\neg g \to a$	$\neg c \to \neg d$	και	$d \to c$
$b \to \neg g$	και	$g \to \neg b$	$\neg c \to \neg f$	και	$f \to c$
$b \to c$	και	$\neg c \to \neg b$	$d \to \neg f$	και	$f \to \neg d$
$\neg b \to e$	και	$\neg e \to b$	$e \to g$	και	$\neg g \to \neg e$
$\neg b \to \neg f$	και	$f \to b$	$f \to g$	και	$\neg g \to \neg f$

Οι συνεπαγωγές αυτές μπορούν να αναπαρασταθούν στο παρακάτω γράφημα τόξων:



Δυστυχώς υπάρχουν φαύλοι κύκλοι. Για παράδειγμα υπάρχουν οι κύκλοι

$$e \to a \to \neg g \to \neg e \to b \to c \to f \to g \to \neg b \to e$$

και

$$e \to a \to \neg g \to \neg e \to b \to \neg g \to \neg f \to \neg c \to \neg b \to e$$

Αυτοί οι κύκλοι μας λέει ότι τα e και $\neg e$ πρέπει να έχουν την ίδια τιμή, άρα δεν υπάρχει τρόπος να προγραμματίσουμε όλες τις παραστάσεις. Οι διοργανωτές του φεστιβάλ πρέπει να επαναδιαπραγματευτούν τις συμφωνίες τους με τουλάχιστον ένα από τους έξι κωμικούς A, B, C, E, F, G (η διαθεσιμότητα του D δεν εμφανίζεται στους παραπάνω κύκλους) για να καταρτισθεί ένα ορθό πρόγραμμα. □

Παράδειγμα 6.9.5. *Ζητήθηκε από τους προπονητές έξι ποδοσφαιρικών ομάδων να κάνουν από δύο προβλέψεις ο καθένας για τις θέσεις που θα κατακτήσουν οι ομάδες αυτές στο πρωτάθλημα. Στο τέλος της περιόδου μόνο ένας προπονητής είχε δύο σωστές προβλέψεις και η ομάδα του κατέκτησε την πρώτη θέση. Επίσης, ακριβώς ένας άλλος είχε μια σωστή πρόβλεψη*

και η ομάδα του πήρε τη δεύτερη θέση. Όλοι οι υπόλοιποι προπονητές έκαναν λανθασμένες προβλέψεις. Καθορίστε τη θέση που κατέλαβε κάθε μια από τις έξι ομάδες, αν οι προβλέψεις ήταν οι εξής:

Προπονητής της ομάδας A: Η B θα έρθει δεύτερη και η F πέμπτη.
Προπονητής της ομάδας B: Η F θα έρθει πρώτη και η C δεύτερη.
Προπονητής της ομάδας C: Η D θα έρθει πρώτη και η E έκτη.
Προπονητής της ομάδας D: Η A θα έρθει πρώτη και η C τέταρτη.
Προπονητής της ομάδας E: Η B θα έρθει πέμπτη και η D τρίτη.
Προπονητής της ομάδας F: Η E θα έρθει τρίτη και η A τέταρτη.

Λύση. Γνωρίζουμε ότι ο προπονητής της πρώτης ομάδας έκανε δύο σωστές προβλέψεις, άρα η πρώτη ομάδα δεν μπορεί να είναι μια από τις B, C, D αφού οι προπονητές τους αναφέρουν ως πρώτη ομάδα κάποια άλλη.

Επομένως, η πρώτη ομάδα είναι είτε η A, είτε η E, είτε η F.

Η F δεν μπορεί να είναι πρώτη, διότι τότε ο προπονητής της B θα είχε μια σωστή πρόβλεψη, άρα η ομάδα του είναι δεύτερη και επομένως όλοι οι άλλοι έχουν λάθος προβλέψεις, το οποίο είναι άτοπο, αφού ο προπονητής της A δηλώνει ότι η B είναι δεύτερη.

Η A δεν μπορεί να είναι πρώτη, διότι τότε ο προπονητής της D θα είχε μια σωστή πρόβλεψη άρα η ομάδα του θα είναι η δεύτερη, όμως ο A που έχει δύο σωστές προβλέψεις λέει ότι δεύτερη είναι η B, το οποίο είναι άτοπο.

Άρα, **η πρώτη ομάδα είναι η** E.

Επομένως, **η** B **είναι πέμπτη και η** D **είναι τρίτη**.

Η δεύτερη ομάδα είναι είτε η A, είτε η C, είτε η F.

Η A δεν μπορεί να είναι δεύτερη, διότι και οι δύο προβλέψεις του προπονητή της είναι λάθος.

Η C δεν μπορεί να είναι δεύτερη, διότι και οι δύο προβλέψεις του προπονητή της είναι λάθος.

Άρα, **η δεύτερη ομάδα είναι** F.

Αφού ο προπονητής της F έχει κάνει ακριβώς μια σωστή πρόβλεψη έπεται ότι **η** A **είναι τέταρτη**.

Άρα, **η** C **είναι έκτη**.

Άρα, η τελική κατάταξη των ομάδων είναι E, F, D, A, B, C. □

6.9.1 Ασκήσεις προς επίλυση

1) Τρεις ύποπτοι συλλαμβάνονται για κάποιο έγκλημα.

- Ο A λέει: "Ο B το έκανε. Ο Γ είναι αθώος".
- Ο B λέει: "Αν ο A είναι ένοχος τότε και ο Γ είναι ένοχος".
- Ο Γ λέει: "Δεν το έκανα εγώ. Κάποιος από τους άλλους το έκανε".

i) Υποθέτωντας ότι όλοι είναι αθώοι, να βρεθεί ποιος λέει ψέματα.

ii) Υποθέτωντας ότι όλοι είναι ένοχοι, να βρεθεί ποιος λέει αλήθεια.

iii) Υποθέτωντας ότι όλοι λένε την αλήθεια, να βρεθεί ποιος είναι αθώος και ποιος ένοχος.

iv) Να δειχθεί ότι δεν μπορεί να λένε όλοι ψέματα.

2) Σε ένα ξενοδοχείο γίνονται ταυτόχρονα δύο συνέδρια: Ένα συνέδριο αστρονομίας και ένα συνέδριο αστρολογίας. Οι αστρονόμοι λένε πάντα την αλήθεια, ενώ οι αστρολόγοι λένε πάντα ψέματα. Οι σύνεδροι κάθε ομάδας γνωρίζονται μεταξύ τους.

Συναντάμε δύο συνέδρους, τον A και τον B.

- Ο A λέει: Και οι δύο είμαστε αστρονόμοι.

- Ο B λέει: Ο A είναι αστρολόγος.

Να βρεθεί τι είναι οι A, B.

3) Η Αθηνά έχει γενέθλια σε μια από τις παρακάτω 10 ημερομηνίες:

15 Φεβρουαρίου	16 Φεβρουαρίου	19 Φεβρουαρίου
17 Μαρτίου	18 Μαρτίου	
14 Απριλίου	16 Απριλίου	
14 Αυγούστου	15 Αυγούστου	17 Αυγούστου

Η Αθηνά αποκαλύπτει στην Βάσω μόνο το μήνα που έχει γενέθλια και στην Γεωργία μόνο την ημερομηνία του αντίστοιχου μήνα.

Ακολουθεί η εξής συζήτηση:

- Βάσω: Δεν μπορώ να βρω πότε είναι τα γενέθλια, αλλά γνωρίζω ότι ούτε και η Γεωργία μπορεί να βρει πότε είναι.

- Γεωργία: Αρχικά δεν μπορούσα να τα βρω, αλλά τώρα βρήκα πότε είναι!

- Βάσω: Τώρα βρήκα και εγώ πότε είναι!

Με βάση τις παραπάνω πληροφορίες να βρεθεί η ημερομηνία των γενεθλίων της Αθηνάς.

4) Σε μια διαδικασία επιλογής μεταξύ τριών αντικειμένων α, β, γ είναι απαραίτητη η ικανοποίηση των παρακάτω περιορισμών:

   1) Δεν μπορούν να επιλεχθούν και τα τρία.
   2) Αν επιλεχθεί το γ, τότε θα επιλεχθεί και το α.
   3) Αν δεν επιλεχθεί το β, τότε δεν θα επιλεχθεί και το α.
   4) Αν δεν επιλεχθεί το γ, τότε δεν θα επιλεχθεί και το α.

Μπορεί να γίνει αυτή η επιλογή;

5) Σε κάποια δίκη κλήθηκαν 4 μάρτυρες. Από τις καταθέσεις τους προέκυψαν τα ακόλουθα συμπεράσματα.

   1) Αν η μαρτυρία του M_1 είναι αληθής τότε και η μαρτυρία του M_2 είναι αληθής.
   2) Η μαρτυρία του M_3 είναι αληθής, αν και μόνο αν η μαρτυρία του M_4 είναι αληθής.
   3) Οι μαρτυρίες των M_2 και M_4 ουδέποτε συναληθεύουν.
   4) Η μαρτυρία του M_3 είναι αληθής.

Να βρεθεί, αν υπάρχει, τρόπος ώστε όλα τα παραπάνω συμπεράσματα να είναι αληθή.

6) Ζητείται να μελετηθεί το σύνολο των προτάσεων p_1, p_2, p_3, p_4 για τις οποίες ισχύουν τα ακόλουθα:

   1) Αν η p_1 είναι αληθής τότε και η p_2 είναι αληθής.

2) Η p_3 είναι αληθής, αν η p_4 είναι αληθής και μόνον τότε.

3) Οι p_2 και p_4 ουδέποτε συναληθεύουν.

4) Η p_3 είναι αληθής.

7) Για την ασφάλεια ενός γραφείου ισχύουν οι ακόλουθες οδηγίες:

1) Τα φώτα του γραφείου θα παραμένουν ανοιχτά την νύχτα, μόνο όταν δεν υπάρχει υπάλληλος στο γραφείο και δεν λειτουργεί το κλειστό κύκλωμα παρακολούθησης

2) Το κλειστό κύκλωμα παρακολούθησης θα λειτουργεί, αν και μόνον αν δεν υπάρχει υπάλληλος στο γραφείο ή υπάρχει σ' αυτό ένα μεγάλο χρηματικό ποσό.

Ζητείται να μελετηθούν οι οδηγίες.

Υπόδειξη: Να γίνει χρήση των ακόλουθων τεσσάρων προτάσεων.

p: Τα φώτα του γραφείου θα παραμένουν ανοιχτά την νύχτα.

q: Δεν υπάρχει υπάλληλος στο γραφείο.

r: Το κλειστό κύκλωμα παρακολούθησης λειτουργεί.

s: Στο γραφείο υπάρχει ένα μεγάλο χρηματικό ποσό.

8) Για την συγκρότηση μιας επιτροπής, με μέλη από τους α, β, γ, δ, ε, ισχύουν οι ακόλουθες προϋποθέσεις:

1) Είτε ο α, είτε ο β πρέπει να είναι μέλη, αλλά όχι και οι δύο.

2) Είτε ο γ, είτε ο ε, είτε και οι δύο πρέπει να είναι μέλη.

3) Είτε οι α και γ είναι μέλη, είτε κανείς τους.

4) Αν είναι μέλος ο δ, τότε πρέπει να είναι και ο β.

5) Αν είναι μέλος ο ε, τότε πρέπει να είναι μέλη και οι γ και δ.

Ζητείται να ευρεθούν τα μέλη της επιτροπής.

9) Για τα ζώα ενός σπιτιού ισχύουν οι εξής προτάσεις:

Δ1) Τα μοναδικά ζώα σ' αυτό το σπίτι είναι γάτες.

Δ2) Κάθε ζώο που απολαμβάνει να κοιτάει το φεγγάρι είναι κατάλληλο για κατοικίδιο.

Δ3) Όταν αντιπαθώ ένα ζώο, το αποφεύγω.

Δ4) Κανένα ζώο δεν είναι σαρκοφάγο, εκτός αν κυνηγάει το βράδυ.

Δ5) Οι γάτες σκοτώνουν τα ποντίκια.

Δ6) Κανένα ζώο δεν μου μιλάει, εκτός από αυτά που είναι σ' αυτό το σπίτι.

Δ7) Τα καγκουρό είναι ακατάλληλα για κατοικίδια.

Δ8) Μόνο τα σαρκοφάγα σκοτώνουν ποντίκια.

Δ9) Αντιπαθώ τα ζώα που δεν μου μιλάνε.

Δ10) Τα ζώα που κυνηγάνε το βράδυ απολαμβάνουν πάντα να κοιτάνε το φεγγάρι.

Ζητείται το τελικό συμπέρασμα, που προκύπτει από την μελέτη των προηγούμενων δέκα προτάσεων.

Υπόδειξη. Το τελικό συμπέρασμα μπορεί να προκύψει με τη βοήθεια:

α) Διαδοχικών συλλογισμών επί των δέκα προτάσεων.

β) Ενός δένδρου με φύλλα τις δέκα προτάσεις.

γ) Ενός κύκλου Hamilton και των εξής βοηθητικών προτάσεων, που αναφέρονται σε ζώο-/ζώα το οποίο/τα οποία:

p_1: είναι τα μοναδικά σ' αυτό το σπίτι
p_2: είναι γάτες
p_3: απολαμβάνει να κοιτάει το φεγγάρι
p_4: είναι κατάλληλο για κατοικίδιο
p_5: το αντιπαθώ
p_6: το αποφεύγω
p_7: είναι σαρκοβόρο
p_8: κυνηγάει το βράδυ
p_9: σκοτώνουν τα ποντίκια
p_{10}: μου μιλάνε
p_{11}: είναι καγκουρό

10) Σύμφωνα με την παράδοση ο Εύαθλος, όταν περάτωσε τις σπουδές του κοντά στον Πρωταγόρα, πλήρωσε στο δάσκαλό του τα μισά δίδακτρα με την συμφωνία ότι θα δώσει τα υπόλοιπα μισά όταν θα κερδίσει την πρώτη δίκη που θα αναλάβει.

Επειδή ο Εύαθλος δεν δικηγορούσε και δεν εξοφλούσε το χρέος του, ο Πρωταγόρας κατέφυγε στη δικαιοσύνη.

Στην δίκη που έγινε ο μαθητής υποστήριξε ότι και αν ακόμη δεν απαλλαγεί από το δικαστήριο και πάλι δεν υποχρεούται να πληρώσει, αφού δεν θα έχει κερδίσει την πρώτη δίκη του.

Ο δάσκαλος αντίστοιχα υπεστήριξε ότι και αν ακόμη δεν δικαιωθεί από το δικαστήριο πρέπει να πληρωθεί, αφού ο μαθητής του θα έχει κερδίσει τότε την πρώτη δίκη του.

Ποια ήταν η απόφαση του δικαστηρίου;

11) Κατά την έρευνα μιας υπόθεσης δωροδοκίας ενός ατόμου X από έναν όμιλο, όταν ρωτήθηκαν τα μέλη του A, B, C, D, E έδωσαν τα ακόλουθα ζεύγη απαντήσεων:

A_1 Κανένας από εμάς δεν είναι ταμίας
A_2 Ο X πήρε χρήματα προερχόμενα από τον B που τα πήρε από τον D μέσω του C
B_1 Ο X πήρε τα χρήματα
B_2 Ο C είναι ταμίας
C_1 Η δεύτερη δήλωση του A είναι αληθής
C_2 Η δεύτερη δήλωση του B είναι αληθής
D_1 Ο X δεν πήρε ποτέ χρήματα
D_2 Εγώ είμαι ο ταμίας
E_1 Ο D δεν ήταν ταμίας
E_2 Πήρα χρήματα από τον B και τα έδωσα στον X.

Ζητείται να ευρεθεί το τελικό συμπέρασμα της έρευνας, όταν είναι γνωστό ότι από τις δύο δηλώσεις κάθε ερωτηθέντος η μία είναι αληθής και η άλλη ψευδής.

Υπόδειξη. Το συμπέρασμα μπορεί να προκύψει με τη βοήθεια ακολουθίας συνεπαγωγών.

12) Πέντε αδέλφια έγιναν κάτοχοι της πατρικής περιουσίας μετά το θάνατο του πατέρα τους. Βρείτε το όνομα και την ηλικία του κάθε κληρονόμου, καθώς και το είδος και την αξία κάθε περιουσιακού στοιχείου.

Δ1. Η Μαρία, που δεν είναι ούτε η πρωτότοκη ούτε η μικρότερη, δεν κληρονόμησε το περιουσιακό στοιχείο που η αξία του αποτιμάται σε 12 εκατομμύρια.

Δ2. Το περιουσιακό στοιχείο που αποτιμάται σε 21 εκατομμύρια, που δεν είναι η κυνηγετική έκταση, περιέρχεται στο τρίτο παιδί της οικογενείας.

Δ3. Το δάσος περιέρχεται στην πρωτότοκη.

Δ4. Το αρχοντικό, που έχει αποτιμηθεί σε 14 εκατομμύρια, δεν περιέρχεται στον Διονύση.

Δ5. Ο Διονύσης, που είναι πιο μεγάλος από εκείνη που κληρονόμησε το διαμέρισμα, είναι νεότερος από τον αδελφό του Παύλο, κληρονόμο του περιουσιακού στοιχείου που αποτιμάται σε 17 εκατομμύρια.

Δ6. Το τελευταίο παιδί παντρεύτηκε πέρυσι την φίλη του Όλγα.

Δ7. Όλα τα περιουσιακά στοιχεία έχουν διαφορετική αξία.

13) Για πέντε άτομα, διαφορετικών εθνικοτήτων, ισχύουν οι εξής ιδιότητες:

Δ1) Ο Άγγλος μένει στο κόκκινο σπίτι.

Δ2) Ο Ισπανός έχει σκύλο.

Δ3) Ο Γιαπωνέζος είναι ζωγράφος.

Δ4) Ο Ιταλός πίνει τσάϊ.

Δ5) Ο Νορβηγός μένει στο πρώτο αριστερά σπίτι.

Δ6) Ο ιδιοκτήτης του πράσινου σπιτιού πίνει καφέ.

Δ7) Το πράσινο σπίτι είναι δεξιά από το λευκό σπίτι.

Δ8) Ο γλύπτης εκτρέφει σαλιγκάρια.

Δ9) Ο διπλωμάτης μένει στο κίτρινο σπίτι.

Δ10) Στο σπίτι που είναι στο μέσον πίνουν γάλα.

Δ11) Ο Νορβηγός μένει δίπλα από το γαλάξιο σπίτι.

Δ12) Ο βιολιστής πίνει χυμό.

Δ13) Η αλεπού βρίσκεται στο διπλανό σπίτι από το σπίτι του γιατρού.

Δ14) Το άλογο βρίσκεται στο διπλανό σπίτι από το σπίτι του διπλωμάτη.

Ζητείται να συμπληρωθεί ο ακόλουθος πίνακας:

Σπίτι	1^o	2^o	3^o	4^o	5^o
Χρώμα					
Εθνικότητα					
Επάγγελμα					
Κατοικίδιο					
Ποτό					

Υπόδειξη. Η συμπλήρωση του πίνακα μπορεί να γίνει:

α) Με διαδικασία ανάλογη της επίλυσης ενός sudoku.

β) Με τη βοήθεια της Άλγεβρας του Boole.

Κεφάλαιο 7

Άλγεβρα Boole

7.1 Δικτυωτά

Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο.

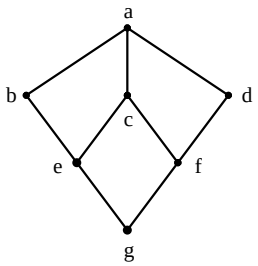
Λέμε ότι το y **καλύπτει** το x, αν $x < y$ και δεν υπάρχει $z \in A$ με $x < z < y$. Η σχέση αυτή ονομάζεται **σχέση κάλυψης**.

Το **διάγραμμα Hasse** ενός πεπερασμένου μερικώς διατεταγμένου συνόλου A είναι ένα σχήμα με κορυφές τα στοιχεία του A, οι οποίες συνδέονται όταν υπάρχει σχέση κάλυψης, και τέτοιο ώστε αν $x < y$ τότε το y σχεδιάζεται "πάνω" από το x.

Αν κάθε δύο στοιχεία του A έχουν ένα μοναδικό ελάχιστο άνω φράγμα (supremum) και ένα μοναδικό μέγιστο κάτω φράγμα (infimum), τα οποία ανήκουν στο A, τότε το σύνολο λέγεται **δικτυωτό**.

Για κάθε δικτυωτό $(A, \leq)$ υπάρχει ένας φυσικός τρόπος να ορίσουμε μια δομή $(A, \vee, \wedge)$, όπου $\vee, \wedge$ είναι δύο εσωτερικές διμελείς πράξεις στο A, τέτοιες ώστε για κάθε $a, \beta \in A$ το $a \vee \beta$ (αντίστοιχα το $a \wedge \beta$) να ισούται με το supremum τους (αντίστοιχα το infimum τους).

Παράδειγμα. 1 Το δικτυωτό που απεικονίζεται στο επόμενο διάγραμμα, για το σύνολο $A = \{a, b, c, d, e, f, g\}$

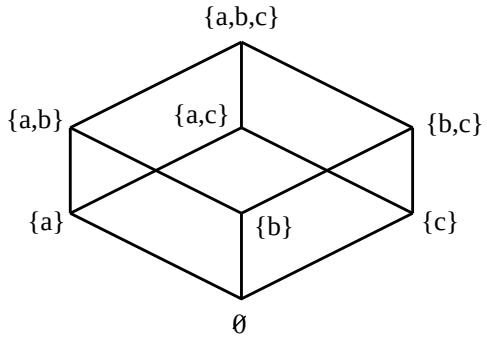


ορίζει τη δομή $(A, \vee, \wedge)$ όπου οι πράξεις $\vee, \wedge$ ορίζονται από τους παρακάτω πίνακες:

$\vee$	a	b	c	d	e	f	g
a	a	a	a	a	a	a	a
b	a	b	a	a	b	a	b
c	a	a	c	a	c	c	c
d	a	a	a	d	a	d	d
e	a	b	c	a	e	c	e
f	a	a	c	d	c	f	f
g	a	b	c	d	e	f	g

$\wedge$	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	b	e	g	e	g	g
c	c	e	c	f	e	f	g
d	d	g	f	d	g	f	g
e	e	e	e	g	e	g	g
f	f	g	f	f	g	f	g
g	g	g	g	g	g	g	g

Παράδειγμα. 2 Το δικτυωτό $(\mathcal{P}(S), \subseteq)$, όπου $S = \{a, b, c\}$, φαίνεται στο παρακάτω σχήμα:



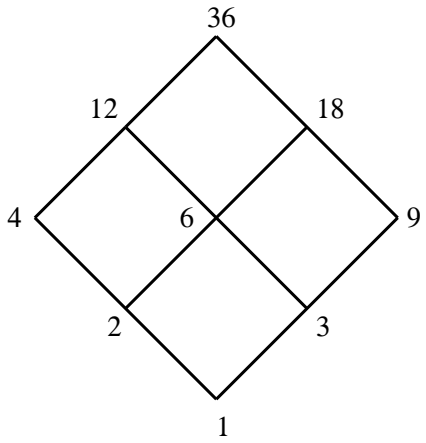
Για την αντίστοιχη δομή $(\mathcal{P}(S), \vee, \wedge)$ οι πράξεις $\vee, \wedge$ είναι οι γνωστές πράξεις $\cup, \cap$ αντίστοιχα που δίνονται από τους παρακάτω πίνακες:

$\cap$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\emptyset$
$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\emptyset$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a\}$	$\{b\}$	$\{a\}$	$\{b\}$	$\emptyset$	$\emptyset$
$\{a,c\}$	$\{a,c\}$	$\{a\}$	$\{a,c\}$	$\{c\}$	$\{a\}$	$\emptyset$	$\{c\}$	$\emptyset$
$\{b,c\}$	$\{b,c\}$	$\{b\}$	$\{c\}$	$\{b,c\}$	$\emptyset$	$\{b\}$	$\{c\}$	$\emptyset$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\emptyset$	$\emptyset$
$\{b\}$	$\{b\}$	$\{b\}$	$\emptyset$	$\{b\}$	$\emptyset$	$\{b\}$	$\emptyset$	$\emptyset$
$\{c\}$	$\{c\}$	$\emptyset$	$\{c\}$	$\{c\}$	$\emptyset$	$\emptyset$	$\{c\}$	$\emptyset$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

$\cup$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\emptyset$
$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$
$\{a,b\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b,c\}$	$\{a,b\}$
$\{a,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a,c\}$	$\{a,c\}$
$\{b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{b,c\}$	$\{a,b,c\}$	$\{b,c\}$	$\{b,c\}$	$\{b,c\}$
$\{a\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a\}$	$\{a,b\}$	$\{a,c\}$	$\{a\}$
$\{b\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,b,c\}$	$\{b,c\}$	$\{a,b\}$	$\{b\}$	$\{b,c\}$	$\{b\}$
$\{c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,c\}$	$\{b,c\}$	$\{a,c\}$	$\{b,c\}$	$\{c\}$	$\{c\}$
$\emptyset$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\emptyset$

Παρατήρηση. Το παραπάνω παράδειγμα προφανώς γενικεύεται για οποιοδήποτε σύνολο S.

Παράδειγμα. 3 Το δικτυωτό $(E, |)$, όπου $E = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ και $|$ είναι η σχέση διαιρετότητας, φαίνεται στο παρακάτω διάγραμμα:



Για την $(E, \vee, \wedge)$ οι πράξεις $\vee, \wedge$ είναι οι γνωστές πράξεις ΕΚΠ (Ελάχιστο Κοινό Πολλαπλάσιο), ΜΚΔ (Μέγιστος Κοινός Διαιρέτης) αντίστοιχα.

Οι πράξεις $\vee, \wedge$ της δομής που αντιστοιχεί σε ένα δικτυωτό, αποδεικνύεται ότι έχουν τις παρακάτω ιδιότητες, για κάθε $a, b, c \in A$:

$$\left.\begin{array}{l} a \vee b = b \vee a \\ a \wedge b = b \wedge a \end{array}\right\} \quad \text{(αντιμεταθετικές).}$$

$$\left.\begin{array}{l} a \vee (b \vee c) = (a \vee b) \vee c \\ a \wedge (b \wedge c) = (a \wedge b) \wedge c \end{array}\right\} \quad \text{(προσεταιριστικές).}$$

$$\left.\begin{array}{l} a \vee a = a \\ a \wedge a = a \end{array}\right\} \quad \text{(αδύναμες).}$$

$$\left.\begin{array}{l} a \vee (a \wedge b) = a \\ a \wedge (a \vee b) = a \end{array}\right\} \quad \text{(απορροφητικές).}$$

7.2 Δυαδική Άλγεβρα Boole

7.2.1 Ορισμός

Έστω $B = \{0, 1\}$ και οι εσωτερικές πράξεις $+, \cdot$ (αντί $\vee$, $\wedge$ αντίστοιχα) που ορίζονται ως εξής:

x	y	$x + y$	$x \cdot y$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

Αποδεικνύεται ότι η δομή $(B, +, \cdot)$ ορίζει ένα δικτυωτό και ότι επιπλέον ισχύουν οι ιδιότητες

$$\left.\begin{array}{l} x \cdot (y + z) = x \cdot y + x \cdot z \\ x + y \cdot z = (x + y) \cdot (x + z) \end{array}\right\} \quad \text{(επιμεριστικές).}$$

Ορίζουμε επίσης την εσωτερική μονομελή πράξη "συμπλήρωμα" στο B η οποία συμβολίζεται με $'$ (ή $\bar{}$) και ορίζεται ως εξής:

x	x'
1	0
0	1

Το δικτυωτό αυτό (όπου το B είναι δισύνολο και επιπλέον ισχύει η επιμεριστική ιδιότητα και ορίζεται η έννοια του συμπληρώματος) ονομάζεται **δυαδική άλγεβρα Boole**.

Παρατήρηση. Ο ορισμός της δυαδικής άλγεβρας Boole επεκτείνεται (γενικεύοντας την έννοια του συμπληρώματος) και στην περίπτωση όπου το B έχει πάνω από δύο στοιχεία.

7.2.2 Ιδιότητες

Αφού η δυαδική άλγεβρα Boole είναι δικτυωτό, ισχύουν τα παρακάτω:

$$\left.\begin{array}{l} x+y=y+x \\ x\cdot y=y\cdot x \end{array}\right\} \quad \text{(αντιμεταθετικότητα).}$$

$$\left.\begin{array}{l} x+(y+z)=(x+y)+z \\ x\cdot(y\cdot z)=(x\cdot y)\cdot z \end{array}\right\} \quad \text{(προσεταιριστικότητα).}$$

$$\left.\begin{array}{l} x+x=x \\ x\cdot x=x \end{array}\right\} \quad \text{(αδυναμία).}$$

$$\left.\begin{array}{l} x+(x\cdot y)=x \\ x\cdot(x+y)=x \end{array}\right\} \quad \text{(απορροφητικότητα).}$$

και επιπλέον,

$$\left.\begin{array}{l} x\cdot(y+z)=x\cdot y+x\cdot z \\ x+y\cdot z=(x+y)\cdot(x+z) \end{array}\right\} \quad \text{(επιμεριστικότητα).}$$

Ισχύουν επίσης οι παρακάτω ιδιότητες:

i. $(x')'=x$.

ii. $x+0=x$ και $x+1=1$.

iii. $x\cdot 0=0$ και $x\cdot 1=x$.

iv. $x+x'=1$ και $x\cdot x'=0$.

v. $x+x'\cdot y=x+y$.

vi. $\left.\begin{array}{l} (x+y)'=x'\cdot y' \\ (x\cdot y)'=x'+y' \end{array}\right\}$ (τύποι De Morgan).

Οι αποδείξεις των ιδιοτήτων γίνονται με πίνακες ή χρησιμοποιώντας προηγούμενες ιδιότητες.

Παραδείγματα

1. Απόδειξη της προσεταιριστικής ιδιότητας

$$x + (y + z) = (x + y) + z.$$

x	y	z	$y+z$	$x+(y+z)$	$x+y$	$(x+y)+z$
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	1	1	1
1	0	0	0	1	1	1
0	1	1	1	1	1	1
0	1	0	1	1	1	1
0	0	1	1	1	0	1
0	0	0	0	0	0	0

2. Απόδειξη των επιμεριστικών ιδιοτήτων

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

x	y	z	$y+z$	$x(y+z)$	xy	xz	$xy+xz$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

$$x + y \cdot z = (x + y) \cdot (x + z).$$

x	y	z	yz	$x+yz$	$x+y$	$x+z$	$(x+y)(y+z)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

3. Απόδειξη των ιδιοτήτων iv

$$x + x' = 1 \text{ και } x \cdot x' = 0.$$

x	x'	$x+x'$	xx'
0	1	1	0
1	0	1	0

4. Απόδειξη της απορροφητικής ιδιότητας

$$x + x \cdot y = x.$$

$$x + xy = x1 + xy = x(1 + y) = x1 = x.$$

7.2.3 Εξισώσεις

Θέλουμε να βρούμε τις τιμές του x, ή των x, y, ή των $x, y, z, \ldots$ για τις οποίες επαληθεύονται οι εξισώσεις. (Φυσικά $x, y, z, \ldots \in B = \{0, 1\}$.)

Παράδειγμα 7.2.1. *Να λυθεί η εξίσωση*

$$x'y + xy' = 0.$$

Λύση.

x	y	x'	$x'y$	y'	xy'	$x'y + xy'$
1	1	0	0	0	0	0
1	0	0	0	1	1	1
0	1	1	1	0	0	1
0	0	1	0	1	0	0

Άρα, $\begin{cases} x = y = 1, \\ \text{ή} \\ x = y = 0. \end{cases}$ □

Παράδειγμα 7.2.2. *Να λυθεί η εξίσωση*

$$xz' + x'yz + y'z' = 1.$$

Λύση. Έστω $F = xz' + x'yz + y'z'$.

x	y	z	z'	xz'	x'	yz	$x'yz$	y'	$y'z'$	$xz' + x'yz$	F
1	1	1	0	0	0	1	0	0	0	0	0
1	1	0	1	1	0	0	0	0	0	1	1
1	0	1	0	0	0	0	0	1	0	0	0
1	0	0	1	1	0	0	0	1	1	1	1
0	1	1	0	0	1	1	1	0	0	1	1
0	1	0	1	0	1	0	0	0	0	0	0
0	0	1	0	0	1	0	0	1	0	0	0
0	0	0	1	0	1	0	0	1	1	0	1

Άρα, $\begin{cases} x = y = 1, z = 0, \\ \text{ή} \\ x = 1, y = z = 0, \\ \text{ή} \\ x = 0, y = z = 1, \\ \text{ή} \\ x = y = z = 0. \end{cases}$ □

Παράδειγμα 7.2.3. *Να λυθεί (και διερευνηθεί) η εξίσωση*

$$ax + bx' = 0, \text{ όπου } a, b \in B.$$

Λύση.

a	b	$ax + bx'$	
1	1	$x + x'$ (=1)	→ Άρα αδύνατη.
1	0	x	→ Άρα $x = 0$.
0	1	x'	→ Άρα $x' = 0$, (δηλαδή $x = 1$).
0	0	0	→ Άρα ταυτότητα, δηλαδή ισχύει για κάθε x, (δηλαδή ισχύει για $x = 0$ και για $x = 1$).

□

7.2.4 Συστήματα

Παράδειγμα 7.2.4. *Να λυθεί το σύστημα* $\left\{ \begin{array}{rl} x' + xy' = & 1 \\ x + xy = & 0 \end{array} \right\}$.

Λύση.

x	y	x'	y'	xy'	xy	$x' + xy'$	$x + xy$
1	1	0	0	0	1	0	1
1	0	0	1	1	0	1	1
0	1	1	0	0	0	1	0
0	0	1	1	0	0	1	0

Άρα $(x, y) = (0, 1)$ ή $(x, y) = (0, 0)$. □

7.2.5 Συναρτήσεις Boole

Κάθε συνάρτηση $f : B^n \to B$ λέγεται **συνάρτηση Boole** ή **λογική συνάρτηση**.

Παράδειγμα. 1

$$f : B^2 \to B \text{ με } f(x, y) = xy' + x'y.$$

Η f παίρνει τις τιμές:
$f(1, 1) = 1 \cdot 0 + 0 \cdot 1 = 0 + 0 = 0,$
$f(1, 0) = 1 \cdot 1 + 0 \cdot 0 = 1 + 0 = 1,$
$f(0, 1) = 0 \cdot 0 + 1 \cdot 1 = 0 + 1 = 1,$
$f(0, 0) = 0 \cdot 1 + 1 \cdot 0 = 0 + 0 = 0,$
ή (με πίνακα):

x	y	y'	xy'	x'	$x'y$	f
1	1	0	0	0	0	0
1	0	1	1	0	0	1
0	1	0	0	1	1	1
0	0	1	0	1	0	0

Παράδειγμα. 2

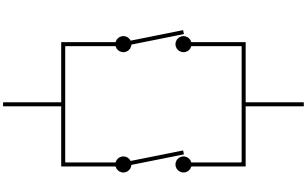
$$f : B^3 \to B \text{ με } f(x, y, z) = xy + z'.$$

Η f παίρνει τις τιμές:
$f(1, 1, 1) = 1 \cdot 1 + 0 = 1 + 0 = 1.$
$f(1, 1, 0) = 1 \cdot 1 + 1 = 1 + 1 = 1.$
$f(1, 0, 1) = 1 \cdot 0 + 0 = 0 + 0 = 0.$ κ.λπ.

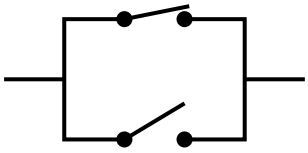
7.2.6 Εφαρμογές

1. Διακόπτες

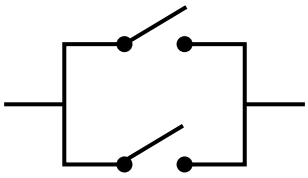
Διακόπτες 'παράλληλοι' ⟶ +



$1 + 1 = 1$



$1 + 0 = 1$
$(0 + 1 = 1)$



$0 + 0 = 0$

Διακόπτες 'σε σειρά'⟶ ·

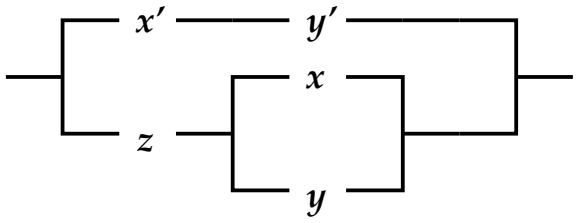
$1 \cdot 1 = 1$

$1 \cdot 0 = 0$
$(0 \cdot 1 = 0)$

$0 \cdot 0 = 0$

2. Δίπολα

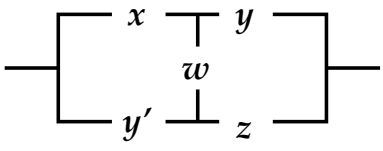
Σε κάθε συνάρτηση Boole αντιστοιχεί ένα δίπολο και αντίστροφα.
Για παράδειγμα, στο δίπολο



αντιστοιχεί η συνάρτηση

$$f(x, y, z) = x'y' + z(x + y).$$

Στο δίπολο



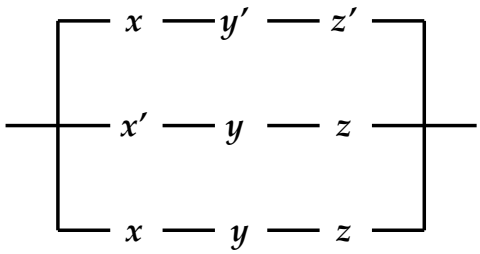
αντιστοιχεί η συνάρτηση

$$\begin{aligned} f(x, y, z, w) &= xy + xwz + y'wy + y'z \\ &= xy + xwz + y'yw + y'z \\ &= xy + xwz + 0w + y'z \\ &= xy + xwz + y'z. \end{aligned}$$

Αντίστροφα:
Στη συνάρτηση

$$f(x, y, z) = xy'z' + x'yz + xyz$$

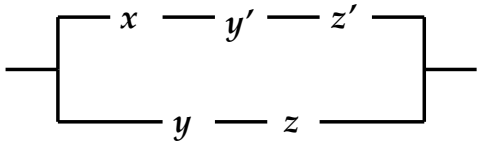
αντιστοιχεί το δίπολο



Αλλά

$$\begin{aligned} f(x, y, z) &= xy'z' + (x' + x)yz \\ &= xy'z' + 1 \cdot yz \\ &= xy'z' + yz, \end{aligned}$$

οπότε παίρνουμε το αντίστοιχο (απλούστερο) δίπολο



3. Άλγεβρα λογικών προτάσεων

Α (αληθής πρόταση) αντί 1.
Ψ (ψευδής πρόταση) αντί 0.
$\vee$ (ή) αντί +.
$\wedge$ (και) αντί $\cdot$.
$\neg$ (άρνηση) αντί $'$.
Οι τρεις πράξεις της Άλγεβρας Boole, δίνουν τις αντίστοιχες πράξεις της άλγεβρας λογικών προτάσεων.

p	q	$p \vee q$	$p \wedge q$
Α	Α	Α	Α
Α	Ψ	Α	Ψ
Ψ	Α	Α	Ψ
Ψ	Ψ	Ψ	Ψ

p	$\neg p$
Α	Ψ
Ψ	Α

Επίσης ορίζονται και οι πράξεις $\rightarrow$ (αν ... τότε), $\leftrightarrow$ (αν και μόνο αν) με βάση τον παρακάτω πίνακα:

p	q	$p \rightarrow q$	$p \leftrightarrow q$
Α	Α	Α	Α
Α	Ψ	Ψ	Ψ
Ψ	Α	Α	Ψ
Ψ	Ψ	Α	Α

Ο έλεγχος της αλήθειας των λογικών προτάσεων γίνεται με πίνακες αλήθειας.

Παράδειγμα. Για την πρόταση

$$(p \rightarrow q) \rightarrow (p \wedge q)$$

προκύπτει ο παρακάτω πίνακας αλήθειας:

p	q	$p \rightarrow q$	$p \wedge q$	$(p \rightarrow q) \rightarrow (p \vee q)$
Α	Α	Α	Α	Α
Α	Ψ	Ψ	Ψ	Α
Ψ	Α	Α	Ψ	Ψ
Ψ	Ψ	Α	Ψ	Ψ

Εκφράσεις της Λογικής και της Άλγεβρας Boole οι οποίες δίνουν σε κάθε περίπτωση αντίστοιχα αποτελέσματα (Α αντί 1 και Ψ αντί 0) θεωρούνται αντίστοιχες στη Λογική και την Άλγεβρα Boole.

Παράδειγμα. 1 Η συνεπαγωγή $p \to q$ της Λογικής αντιστοιχεί στην έκφραση $x' + y$ της Άλγεβρας Boole, αφού

p	q	$p \to q$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Α
Ψ	Ψ	Α

x	y	x'	$x' + y$
1	1	0	1
1	0	0	0
0	1	1	1
0	0	1	1

Παράδειγμα. 2 Η ισοδυναμία $p \leftrightarrow q$ της Λογικής αντιστοιχεί στην έκφραση $xy + x'y'$ της Άλγεβρας Boole αφού

p	q	$p \leftrightarrow q$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Ψ
Ψ	Ψ	Α

x	y	xy	x'	y'	$x'y'$	$xy + x'y'$
1	1	1	0	0	0	1
1	0	0	0	1	0	0
0	1	0	1	0	0	0
0	0	0	1	1	1	1

4. Αρχές Λογικής

Αρχή της διπλής άρνησης

Η $(x')' = x$ αντιστοιχεί στην $\neg(\neg p) \leftrightarrow p$.

Αρχή της του τρίτου αποκλείσεως

Η $x + x' = 1$ δίνει ότι $p \vee \neg p$: Αληθής.

Αρχή της αντίφασης

Η $xx' = 0$ δίνει ότι $p \wedge \neg p$: Ψευδής.

7.3 Ασκήσεις προς επίλυση

1) Στο σύνολο $\mathbb{N}^*$ ορίζεται η μερική διάταξη $|$ (διαιρετότητα), με $x \mid y$ αν και μόνο αν ο x διαιρεί τον y. Αν E είναι το σύνολο των διαιρετών του 24, να δειχθεί ότι το $(E, |)$ είναι ένα δικτυωτό, για το οποίο να δοθεί και το αντίστοιχο σχήμα.

2) Στο σύνολο $\mathbb{N}^2$ ορίζεται η μερική διάταξη $\leq$ (**διάταξη γινόμενο**), με

$$(x_1, y_1) \leq (x_2, y_2) \text{ αν και μόνο αν } x_1 \leq x_2 \text{ και } y_1 \leq y_2.$$

Αν $E = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$, να δειχθεί ότι το $(E, \leq)$ είναι ένα δικτυωτό, για το οποίο να δοθεί και το αντίστοιχο σχήμα.

3) Να αποδειχθούν οι ιδιότητες ν και νi (De Morgan) της Άλγεβρας Boole.

4) Με χρήση των ιδιοτήτων, να απλοποιηθούν οι παραστάσεις:

i) $xy' + yz + z'w + x'y'z$.

ii) $x(x' + y)(z' + w)z$.

iii) $x(x + yz'w) + w(x + x'y'z)$.

iν) $(x' + yz')(xw + yz)(y + z')$.

ν) $y'(u + uw)(x + z) + y'u + yz(y + x + u(u + x))$.

5) Να λυθούν οι εξισώσεις της Άλγεβρας Boole:

i) $x' + xy' = 1$.

ii) $xy' + x'y + yz' = 0$.

iii) $xyz' + x'yz + xyz = 1$.

6) Να λυθούν οι εξισώσεις της Άλγεβρας Boole:

i) $ax + by = 1$.

ii) $ax + by = x$.

iii) $ax' + y = b$.

iν) $x + y' + a = x + x'y + bx$.

ν) $ax' = by$.

όπου x, y είναι οι άγνωστοι και a, b είναι παράμετροι.

7) Να λυθούν οι εξισώσεις της Άλγεβρας Boole:

i) $ax + y = bz + y$.

ii) $a(x + y) = z + b$.

iii) $abx + y + z = bz$.

iν) $x + byz = ax' + yz$.

όπου x, y, z είναι οι άγνωστοι και a, b είναι παράμετροι.

8) Να λυθούν τα συστήματα της Άλγεβρας Boole:

i) $\begin{cases} x' + xy' = 1 \\ x + xy = 0. \end{cases}$

ii) $\begin{cases} y + x'y + z = 1 \\ y' + xz + y'z = 0. \end{cases}$

iii) $\begin{cases} x' + xy' + y' = 0 \\ y + x'y + x = 1. \end{cases}$

9) Να λυθούν τα συστήματα της Άλγεβρας Boole:

i) $\begin{cases} (a + b)x + y = a \\ ax + aby = b \end{cases}$

ii) $\begin{cases} x + y + z = x + y' \\ a + yz = b + yz \end{cases}$

iii) $\begin{cases} x + ay + bz = 1 \\ bx + ay = 0 \\ x + bz' = 1 \end{cases}$

όπου x, y, z είναι οι άγνωστοι και a, b είναι παράμετροι.

10) Να δειχθεί ότι αριθμός των συναρτήσεων Boole με n μεταβλητές ισούται με 2^{2^n}.

11) Να βρεθούν τα δίπολα που αντιστοιχούν στις συναρτήσεις:

i) $f(x, y, z) = (x + y)z + x'y'z'$.

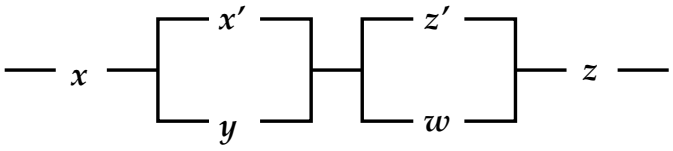
ii) $f(x, y, z) = xyz + x'yz + xy'z'$.

iii) $f(x, y, z) = (xyz)' + (x' + yz)'$.

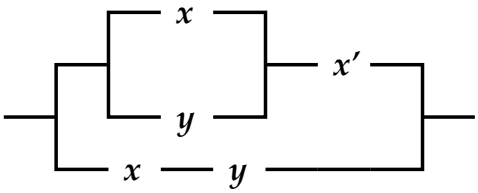
iv) $f(x, y, z) = (x + z + (x + y(x + yz)')')'$.

12) Να απλοποιηθούν τα παρακάτω δίπολα

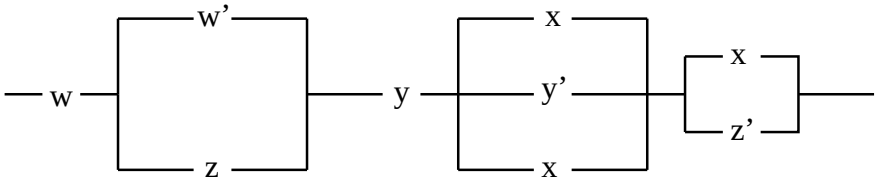
i)



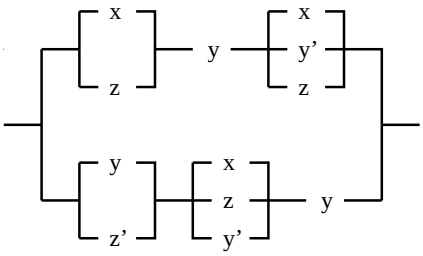
ii)



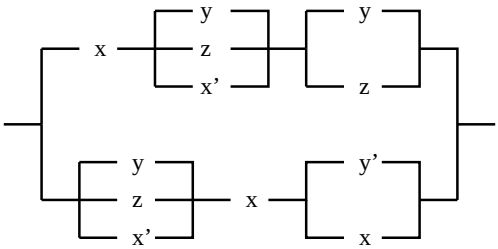
iii)



iν)



ν)



13) Να γραφεί ο πίνακας αλήθειας για τις παρακάτω λογικές προτάσεις:

i) $(p \vee q) \rightarrow (\neg p \vee q)$.

ii) $p \rightarrow (q \wedge r)$.

Βιβλιογραφία

[1] G. E. Andrews, *Number theory*, Dover, 1994.

[2] V. K. Balakrishnan, *Introductory discrete mathematics*, Dover, 1996.

[3] V. K. Balakrishnan, *Schaum's outlines of combinatorics, including concepts of graph theory*, McGraw-Hill, 1995.

[4] E. Bender, S. Gill Williamson, *A short course on discrete mathematics*, Dover, 2004.

[5] E. Bender, S. Gill Williamson, *Foundations of combinatorics with applications*, Dover, 2005.

[6] E. Bender, S. Gill Williamson, *Mathematics for algorithm and systems analysis*, Dover, 2005.

[7] A. Clark, *Elements of abstract algebra*, Dover, 1984.

[8] D. I. A. Cohen, *Basic techniques of combinatorial theory*, John Wiley & Sons, 1978.

[9] S. Cook, *Recursive and recursively enumerable sets*, web draft, 2008.

[10] D. DeTemple, W. Webb, *Combinatorial reasoning: an introduction to the art of counting*, Wiley, 2014.

[11] V. A. Dobrushkin, *Methods in algorithmic analysis*, CRC Press, 2010.

[12] A. Engel, *Problem-solving strategies*, Springer, 1998.

[13] M. Erickson, *Pearls of discrete mathematics*, CRC Press, 2000.

[14] P. Fannon, V. Kadelburg, B. Woolley, S. Ward, *Discrete mathematics for the ib diploma*, Cambridge University Press, 2013.

[15] H. G. Flegg, *Boolean algebra*, Transworld Publishers, 1972.

[16] A. Gardiner, *The mathematical olympiad handbook*, Oxford University Press, 1997.

[17] G. P. Gavrilov, A. A. Sapozhenko, *Problems and exercises in discrete mathematics*, Springer, 1996.

[18] S. I. Gelfand, M. L. Gerver, A. A. Kirillov, N. N. Konstantinov, A. G. Kushnirenko, *Sequences, combinations, limits*, Dover, 2002.

[19] D. Gunderson, *Handbook of mathematical induction*, Chapman & Hall/CRC, 2011.

[20] R. Hamming, *Methods of mathematics applied to calculus, probability, and statistics*, Dover, 2004.

[21] R. Honsberger, *From Erdos to Kiev: problems of olympiad caliber*, Mathematical Association of America, 1996.

[22] N. D. Kazarinoff, *Analytic inequalities*, Dover, 2003.

[23] D. E. Knuth, *The art of computer programming*, Vol. 4A, Pearson, 2011.

[24] T. Koshy, *Elementary number theory with applications*, Academic Press, 2006.

[25] I. Lavrov, L. Maksimova, G. Corsi, *Problems in set theory, mathematical logic and the theory of algorithms*, Kluwer Academic/Plenum Publishers, 2003.

[26] E. Lehman, T. Leighton, *Mathematics for computer science*, MIT, 2004.

[27] W. J. LeVeque, *Fundamentals of number theory*, Dover, 1996.

[28] L. Lovász, *Combinatorial problems and exercises*, 2nd edition, North Holland, 1993.

[29] D. Makinson, *Sets, logic and maths for computing*, 2nd edition, Springer, 2012.

[30] Z. A. Melzak, *Companion to concrete mathematics*, Dover, 2007.

[31] A. Pettofrezzo, *Introductory numerical analysis*, Dover, 1984.

[32] I. Petrică, I. Lazăr, *Probleme de algebra pentru liceu*, Vol. II, Editura Petrion, 1995.

[33] S. M. Ross, *Topics in finite and discrete mathematics*, Cambridge University Press, 2000.

[34] D. A. Santos, *Number theory for mathematical contests*, web draft, 2007.

[35] S. Savchev, T. Andreescu, *Mathematical miniatures*, Mathematical Association of America, 2003.

[36] F. Scheid, *Schaum's outline of theory and problems of numerical analysis*, 2nd edition, McGraw-Hill, 1988.

[37] M. Schroeder, *Fractals, chaos, power laws*, Dover, 2009.

[38] A. Soifer, *Geometric etudes in combinatorial mathematics*, 2nd edition, Springer, 2010.

[39] I. S. Sominskii, *The method of mathematical induction*, Braisdell Publishing Company, 1961.

[40] R. R. Stoll, *Set theory and logic*, Dover, 1979.

[41] I. Tomescu, *Problems in combinatorics and graph theory*, Wiley, 1985.

[42] N. Vilenkin, *Combinatorial mathematics for recreation*, Mir Publishers, 1972.

[43] J. E. Whitesitt, *Boolean algebra and its applications*, Dover, 1995.

[44] R. Wilson, *Combinatorics: a very short introduction*, Oxford University Press, 2016.

[45] G. Winskel, *Set theory for computer science*, web draft, 2010.

[46] P. Zeitz, *The art and craft of problem solving*, 2nd edition, John Wiley & Sons, 2007.

[47] Ν. Βασίλιεφ, Α. Γεγκόροφ, *Πανενωσιακές μαθηματικές ολυμπιάδες της Ε.Σ.Σ.Δ.*, τόμος 1, Εκδόσεις Κάτοπτρο, 1997.

[48] Ν. Βασίλιεφ, Α. Γεγκόροφ, *Πανενωσιακές μαθηματικές ολυμπιάδες της Ε.Σ.Σ.Δ.*, τόμος 2, Εκδόσεις Κάτοπτρο, 1998.

[49] Α. Βουτσαδάκης, Λ. Κυρούσης, Χ. Μπούρας, Π. Σπυράκης, *Διακριτά μαθηματικά: προβλήματα και λύσεις*, Πάτρα, 1994.

[50] Δ. Δεριζιώτης, *Μια εισαγωγή στη θεωρία αριθμών*, Εκδόσεις σοφία, 2007.

[51] H. Eves, *Μεγάλες στιγμές των μαθηματικών μετά το 1650*, Εκδόσεις Τροχαλία, 1990.

[52] Π. Κατερίνης, *Διακριτά μαθηματικά*, σημειώσεις μαθήματος, ΟΠΑ, 2014.

[53] Μ. Κολουντζάκης, Χ. Παπαχριστόπουλος, *Διακριτά μαθηματικά*, ΣΕΑΒ, 2015.

[54] Η. Κουτσουπιάς, *Μαθηματικά πληροφορικής*, Πανεπιστήμιο Αθηνών, 2009.

[55] C. Liu, *Διακριτά μαθηματικά*, Πανεπιστημιακές Εκδόσεις Κρήτης, 1999.

[56] M. Mano, *Ψηφιακή σχεδίαση*, Εκδόσεις Παπασωτηρίου, 1992.

[57] Γ. Ν. Μοσχοβάκης, *Σημειώσεις στη συνολοθεωρία*, Εκδόσεις Νεφέλη, 1993.

[58] Π. Δ. Μποζάνης, *Αλγόριθμοι*, Εκδόσεις Τζιόλα, 2006.

[59] Π. Δ. Μποζάνης, *Προβλήματα και ασκήσεις στους αλγόριθμους*, Εκδόσεις Τζιόλα, 2009.

[60] Μ. Μυτιληναίος, *Λογική*, ΟΠΑ, χ.χ.

[61] Χ. Θ. Μωϋσιάδης, *Συνδυαστική απαρίθμηση: Η τέχνη να μετράμε χωρίς μέτρημα*, Εκδόσεις Ζήτη, 2002.

[62] Σ. Νεγρεπόντης, Σ. Γιωτόπουλος, Ε. Γιαννακούλιας, *Απειροστικός λογισμός, τόμος Ι*, Εκδόσεις Συμμετρία, 1999.

[63] Α. Παναγιωτόπουλος, *Διακριτά Μαθηματικά*, Εκδόσεις Α. Σταμούλης, 1993.

[64] G. Polya, *Η μαθηματική ανακάλυψη*, τόμος 1, Εκδόσεις Κάτοπτρο, 2001.

[65] Α. Πούλος, *Συνδυαστική απαρίθμηση και συνδυαστική γεωμετρία*, Εκδόσεις Ζήτη, 2015.

[66] K. Rosen, *Διακριτά μαθηματικά και εφαρμογές*, 5η έκδοση, Εκδόσεις Τζιόλα, 2008.

[67] Α. Σαπουνάκης, Ε. Φούντας, *Ανάλυση και εφαρμογές*, τόμος Ι, Εκδόσεις Βαρβαρήγου, 2013.

[68] W. Sierpinski, *250 προβλήματα της στοιχειώδους θεωρίας αριθμών*, Εκδόσεις Κάτοπτρο, 2004.

[69] Ε. Σπανδάγος, Ρ. Σπανδάγου, *Εισαγωγή στην θεωρία συνόλων*, Εκδόσεις Αίθρα, 2014.

[70] Α. Τζουβάρας, *Στοιχεία μαθηματικής λογικής*, Εκδόσεις Ζήτη, 1998.

[71] Χ. Χαραλαμπίδης, *Συνδυαστική*, τεύχος 1, 2η έκδοση, Συμμετρία, 2000.