

ΜΠΣ ΠΛΗΡΟΦΟΡΙΚΗ

Διακριτά Μαθηματικά

Ασκήσεις φροντιστηρίου 2

x	y	xy
0	0	0
0	1	1
1	0	1
1	1	0

1 Άλγεβρα Boole

Ιδιότητες

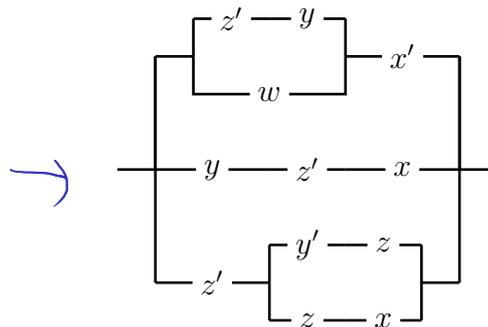
Στη δυαδική άλγεβρα Boole ισχύουν οι παρακάτω ιδιότητες:

$$\begin{array}{l}
 \left. \begin{array}{l} x + y = y + x \\ x \cdot y = y \cdot x \end{array} \right\} \text{(αντιμεταθετικότητα)} \\
 \left. \begin{array}{l} x + (y + z) = (x + y) + z \\ x \cdot (y \cdot z) = (x \cdot y) \cdot z \end{array} \right\} \text{(προσεταιριστικότητα)} \\
 \left. \begin{array}{l} x + (x \cdot y) = x \\ x \cdot (x + y) = x \end{array} \right\} \text{(απορροφητικότητα)} \\
 \left. \begin{array}{l} x + x = x \\ x \cdot x = x \end{array} \right\} \text{(αδυναμία)} \\
 \left. \begin{array}{l} x \cdot (y + z) = x \cdot y + x \cdot z \\ x + y \cdot z = (x + y) \cdot (x + z) \end{array} \right\} \text{(επιμεριστικότητα)}
 \end{array}$$

Ισχύουν επίσης οι παρακάτω ιδιότητες:

$$\begin{array}{l}
 \text{i. } (x')' = x \\
 \text{ii. } x + 0 = x \text{ και } x + 1 = 1. \\
 \text{iii. } x \cdot 0 = 0 \text{ και } x \cdot 1 = x. \\
 \text{iv. } x + x' = 1 \text{ και } x \cdot x' = 0. \\
 \text{v. } x' + x \cdot y = x' + y. \\
 \text{vi. } \left. \begin{array}{l} (x + y)' = x' \cdot y' \\ (x \cdot y)' = x' + y' \end{array} \right\} \text{(τύποι De Morgan).}
 \end{array}$$

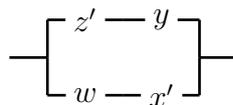
Άσκηση. Να απλοποιηθεί το παρακάτω δίπολο, με χρήση των συναρτήσεων Boole.



Λύση. Η συνάρτηση Boole που αντιστοιχεί στο παραπάνω δίπολο είναι η

$$\begin{aligned}
 f &= (z'y + w)x' + yz'x + z'(y'z + zx) \\
 &= z'yx' + wx' + yz'x + z'z(y' + x) \\
 &= z'y(x' + x) + wx' + 0 = z'y1 + wx' \\
 &= z'y + wx'
 \end{aligned}$$

Επομένως, το ισοδύναμο απλοποιημένο δίπολο είναι το ακόλουθο:



□

Άσκηση. Να λυθεί η εξίσωση

$$x + y' = x'$$

Λύση. (1ος τρόπος) Κατασκευάζουμε τον πίνακα αληθείας με όλες τις δυνατές επιλογές:

x	y	x'	x + y'
1	1	0	1
1	0	0	1
0	1	1	0
0	0	1	1

Άρα, η εξίσωση έχει μια λύση, την $(x, y) = (0, 0)$.

(2ος τρόπος) Αν $x = 1$, τότε $1 + y' = 0$, αδύνατο.

Αν $x = 0$, τότε θα πρέπει να ισχύει $0 + y' = 1$. Επομένως, $y' = 1$, δηλαδή $y = 0$.

Άρα, η εξίσωση έχει μια λύση, την $(x, y) = (0, 0)$.

□

Άσκηση. Να λυθεί η εξίσωση Boole

$$ax + y = b$$

όπου x, y είναι οι άγνωστοι και $a, b \in \{0, 1\}$ είναι παράμετροι.

Λύση. Μπορούμε να κατασκευάσουμε τον πίνακα αληθείας (με 16 γραμμές). Εναλλακτικά, διακρίνουμε περιπτώσεις για τις τιμές των παραμέτρων a, b .

- $a = b = 1$. Τότε, η εξίσωση γίνεται $x + y = 1$ και υπάρχουν 3 λύσεις:

$$1) x = y = 1, \quad 2) x = 1, y = 0, \quad 3) x = 0, y = 1.$$

- $a = b = 0$. Τότε, $y = 0$ και υπάρχουν 2 λύσεις:

$$1) x = y = 0, \quad 2) x = 1, y = 0.$$

- $a = 1, b = 0$. Τότε, $x + y = 0$ και υπάρχει μία λύση, η $x = y = 0$.

- $a = 0, b = 1$. Τότε, $y = 1$ και υπάρχουν 2 λύσεις:

$$1) x = y = 1, \quad 2) x = 0, y = 1. \quad \square$$

Άσκηση. Να λυθεί το σύστημα Boole

$$\left. \begin{array}{l} x' + (y' + x)y' = 1 \\ x + x'y' = 0 \end{array} \right\} \Leftrightarrow \left. \begin{array}{l} x' + (y' + x)y' = 1 \\ (x + x'y')' = 1 \end{array} \right\} \Leftrightarrow f = 1$$

Λύση. Διακρίνουμε περιπτώσεις:

- Αν $y = 0$, τότε η δεύτερη εξίσωση δίνει $x + x'1 = 0 \Rightarrow x + x' = 0$, που είναι αδύνατο.
- Αν $y = 1$, τότε η δεύτερη εξίσωση δίνει $x + x'0 = 0 \Rightarrow x = 0$ και η πρώτη εξίσωση δίνει $x' + (0 + x)0 = 1 \Rightarrow x' = 1 \Rightarrow x = 0$.

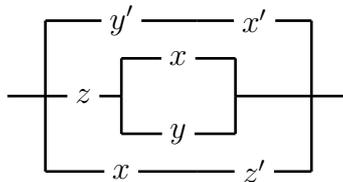
Επομένως, η μοναδική λύση του συστήματος είναι η $(x, y) = (0, 1)$.

2ος τρόπος: Το σύστημα επαληθεύεται αν η παράσταση $f = (x' + (y' + x)y')(x + x'y)'$ είναι ίση με 1. Απλοποιώντας την f

$$\begin{aligned} f &= (x' + (y' + x)y')(x + x'y)' = (x' + y' + xy')x'(x'y)' = (x' + x'y' + x'xy')(x + y) \\ &= (1 + y')x'(x + y) = 1(x'x + x'y) = x'y, \end{aligned}$$

έχουμε τελικά ότι $f = x'y$. Άρα, θα πρέπει να είναι $x = 0$ και $y = 1$. □

Άσκηση. Να βρεθεί η συνάρτηση που αντιστοιχεί στο δίπολο



Αν $xz = 1$, υπάρχει τιμή των μεταβλητών x, y, z ώστε η συνάρτηση που αντιστοιχεί στο δίπολο να λαμβάνει τιμή 1;

Λύση. Η συνάρτηση Boole που αντιστοιχεί στο παραπάνω δίπολο είναι η

$$\begin{aligned}
 f = f(x, y, z) &= y'x' + zx + zy + xz' && \underline{x=z=1} \quad 1+y=1 \\
 &= y'x' + (z+z')x + zy \\
 &= y'x' + x + zy \\
 &= (y'+x)(x'+x) + zy \\
 &= y' + x + zy \\
 &= x + (y'+z)(y'+y) \\
 &= x + y' + z
 \end{aligned}$$

Αν $xz = 1$, τότε αναγκαστικά είναι $x = z = 1$. Στην περίπτωση αυτή, είναι $f = 1 + y' + 1 = 1$, δηλαδή η f λαμβάνει τιμή 1 για κάθε τιμή της y . Επομένως, οι ζητούμενες τιμές (x, y, z) είναι οι $(1, 0, 1)$ και $(1, 1, 1)$. \square

Άσκηση. Να βρεθεί μια συνάρτηση Boole που έχει 3 μεταβλητές x, y, z και λαμβάνει την τιμή 1 μόνο όταν ισχύει η σχέση $x + y = z$.

Λύση. Θα φτιάξουμε τον πίνακα αληθείας της συνάρτησης f που ψάχνουμε

x	y	z	f
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

$$\begin{aligned}
 f &= \underline{(x+y)z} + \underline{(x+y)'z'} \\
 &= \underline{xz + yz} + \underline{x'y'z'}
 \end{aligned}$$

Επομένως, μπορούμε να βρούμε (έναν) τύπο της ως εξής:

dnf:

$$f = \underline{xyz} + \underline{xy'z} + x'yz + x'y'z' = xz(y+y') + x'yz + x'y'z'$$

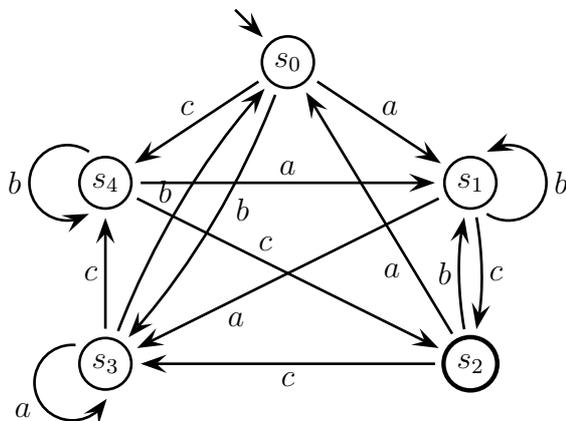
cnf:

$$f = (x' + y' + z)(x' + y + z)(x + y' + z)(x + y + z')$$

\square

3 Αυτόματα

Άσκηση. Δίδεται το παρακάτω αυτόματο



$f^*(ab^m, s_4)$

(i) Να εξετασθεί αν το αυτόματο αναγνωρίζει τις λέξεις

$w_1 = c^2b^3a^4$ (δηλαδή $w_1 = cbbbaaaaa$),

$w_2 = abcabcabc,$

$w_3 = ba^lcb^mab^n$, όπου $l, m, n \in \mathbb{N}^*$.

οχι διότι $f^*(w_3, s_0) = f^*(cb^mab^n, s_3)$

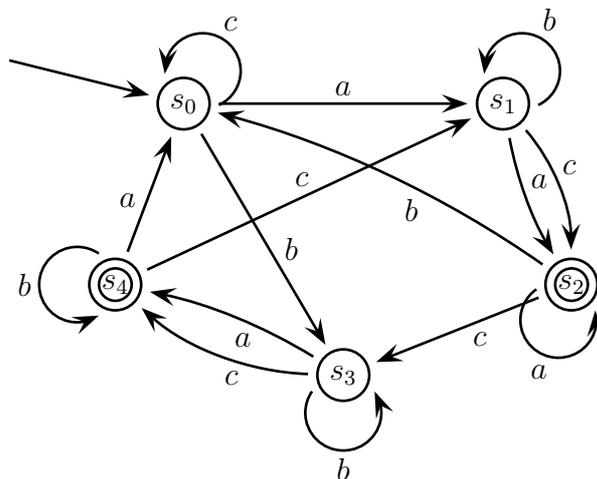
(ii) Να βρεθούν οι τιμές των $m, n \in \mathbb{N}^*$, ώστε το αυτόματο να αναγνωρίζει τη λέξη $w = ab^m c^n$.

Απάντηση. i) Δεν αναγνωρίζει την w_1 , ούτε την w_3 . Αναγνωρίζει την w_2 .

ii) Αναγνωρίζει την w αν $m \in \mathbb{N}^*$ και $n \in \{3k + 1 : k \in \mathbb{N}\}$.

□

Άσκηση. Δίδεται το παρακάτω D-αυτόματο:



i) Να εξετασθεί αν το παραπάνω D-αυτόματο αναγνωρίζει τις λέξεις:

$w_1 = c b c b c b c,$ $w_2 = a^5 b^5 c^5,$ $w_3 = b^5 a^5 c^5$

ii) Να βρεθεί για ποιες τιμές των $k, \lambda \in \mathbb{N}^*$, το παραπάνω D-αυτόματο αναγνωρίζει τη λέξη $w = a^2 b^k c^\lambda$.

$k=1 : f^*(w, s_0) = f^*(c^\lambda, s_0) = s_0 \notin T$

$k \geq 2 : f^*(w, s_0) = f^*(c^\lambda, s_3) = \begin{cases} s_4, & \lambda = 1 + 4m, m \in \mathbb{N} \\ s_2, & \lambda = 3 + 4m, m \in \mathbb{N} \\ s_1, s_3, & \text{αλλιώς} \end{cases}$

4 Αρχές E

Άσκηση. 1323 φοιτητές που συμμετείχαν σε μια έρευνα, απάντησαν (με ναι ή όχι) στις παρακάτω ερωτήσεις:

- A_1 • Έχετε γεννηθεί στην Αθήνα;
- A_2 • Το Τμήμα στο οποίο μπήκατε ήταν η πρώτη σας προτίμηση;
- A_3 • Είστε ευχαριστημένοι με το Τμήμα σας;

Οι καταφατικές απαντήσεις (ναι) στις παραπάνω ερωτήσεις ήταν 464, 355 και 561 αντίστοιχα. Επίσης:

- $A_1 \cap A_2$ • 120 από τους φοιτητές είναι Αθηναίοι και μπήκαν στην πρώτη τους προτίμηση.
- $A_1 \cap A_3$ • 120 από τους φοιτητές είναι Αθηναίοι και είναι ευχαριστημένοι με το Τμήμα τους.
- $A_2 \cap A_3$ • 100 από τους φοιτητές που μπήκαν στην πρώτη τους προτίμηση είναι ευχαριστημένοι με το Τμήμα τους.
- $A_1 \cap A_2 \cap A_3$ • 20 Αθηναίοι φοιτητές μπήκαν στην πρώτη τους προτίμηση και είναι ευχαριστημένοι με το Τμήμα τους.

Να βρεθεί το πλήθος των φοιτητών που ανήκουν στις παρακάτω κατηγορίες:

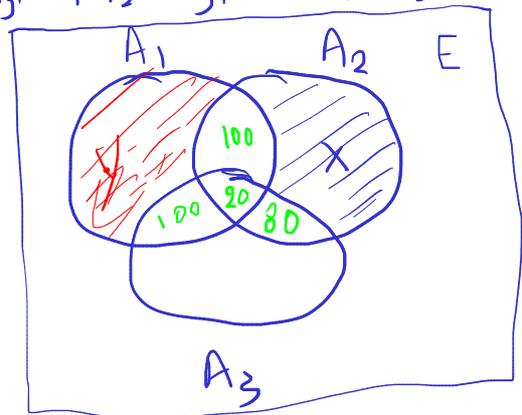
- $\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3$ i) Κατάγονται από την επαρχία, δεν μπήκαν στην πρώτη τους προτίμηση και δεν είναι ευχαριστημένοι από το Τμήμα τους.
- $x = \bar{A}_1 \cap A_2 \cap \bar{A}_3$ ii) Κατάγονται από την επαρχία, μπήκαν στην πρώτη τους προτίμηση και δεν είναι ευχαριστημένοι από το Τμήμα τους.
- $y = A_1 \cap \bar{A}_2 \cap \bar{A}_3$ iii) Είναι Αθηναίοι, δεν μπήκαν στην πρώτη τους προτίμηση και δεν είναι ευχαριστημένοι από το Τμήμα τους.

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = |E| - |A_1 \cup A_2 \cup A_3|$$

$$|x| = |A_2| - 80 - 20 - 100 = 155$$

$$|y| = |A_1| - 100 - 100 - 20 = 244$$



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

Άσκηση. Αν για τα σύνολα A, B, C γνωρίζουμε ότι $|A \cup B \cup C| = 139$ και

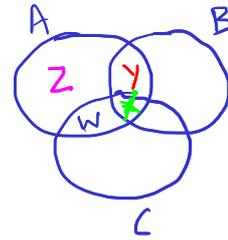
$$|A| = 63, \quad |B| = 91, \quad |C| = 44, \quad |A \cap B| = 25, \quad |A \cap C| = 23, \quad |B \cap C| = 21,$$

να βρεθούν οι πληθάρημοι των παρακάτω συνόλων:

i) $A \cap B \cap C, = x$

ii) $A \cap B \cap \bar{C}, = y = (A \cap B) \setminus (A \cap B \cap C)$

iii) $A \cap \bar{B} \cap \bar{C}. = z = A \setminus y \setminus (A \cap C)$



$$|y| = 25 - |x|$$

$$|z| = |A| - |y| - |A \cap C|$$

Άσκηση. Με πόσους τρόπους μπορούν να μπουν $n = 6$ διακεκριμένα άτομα σε $k = 3$ διακεκριμένα αυτοκίνητα, έτσι ώστε σε κάθε αυτοκίνητο να μπει τουλάχιστον 1 άτομο;

Λύση. Έστω E το σύνολο όλων των τρόπων χωρίς περιορισμούς. Ως γνωστό, είναι $|E| = k^n = 3^6$, διότι κάθε τρόπος αντιστοιχεί αμφιμονοσήμαντα σε μια λέξη $w = w_1 w_2 \dots w_n$ με n γράμματα w_1, w_2, \dots, w_n στο αλφάβητο $[k] = \{1, 2, \dots, k\}$. Η αντιστοιχία είναι η εξής: $w_i = j$ σημαίνει ότι το άτομο i μπήκε στο αυτοκίνητο j .

1 1 2 3 2 3

Ορίζουμε, για κάθε $j \in [k]$, το A_j να είναι το σύνολο των τρόπων που τα άτομα μπορούν να μπουν στα υπόλοιπα αυτοκίνητα εκτός του αυτοκινήτου j . Το ζητούμενο είναι λοιπόν το $|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}|$. Έχουμε ότι

$$|A_1| = |A_2| = |A_3| = 2^6, \quad |A_1 \cap A_2| = |A_1 \cap A_3| = |A_2 \cap A_3| = 1, \quad |A_1 \cap A_2 \cap A_3| = 0.$$

Επομένως,

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| = 3 \cdot 2^6 - 3$$

$$\text{και άρα } |\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| = |E| - |A_1 \cup A_2 \cup A_3| = 3^6 - 3 \cdot 2^6 + 3 = 540. \quad \square$$

Άσκηση. Ναδειχθεί ότι αν υπάρχουν n φωλιές για $kn + 1$ περιστέρια, τότε τουλάχιστον μια φωλιά θα έχει τουλάχιστον $k + 1$ περιστέρια.

Λύση. Έστω ότι κάθε φωλιά έχει το πολύ k περιστέρια. Τότε, οι n φωλιές θα έχουν συνολικά το πολύ kn περιστέρια. Άρα, τουλάχιστον 1 περιστέρι δεν βρίσκεται σε φωλιά, άτοπο. \square

Άσκηση. 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

i) να έχουμε σίγουρα 2 κάλτσες με το ίδιο χρώμα;

ii) να έχουμε σίγουρα 2 με διαφορετικό χρώμα;

Λύση. i) Έχουμε $n = 4$ διαφορετικά χρώματα. Άρα, πρέπει να βγάλουμε τουλάχιστον $n + 1 = 5$. ii) Έχουμε το πολύ $n = 12$ κάλτσες με ίδιο χρώμα (12 μαύρες). Άρα, πρέπει να βγάλουμε τουλάχιστον $n + 1 = 13$. \square

Άσκηση. Πόσοι αριθμοί πρέπει να επιλεγούν από το σύνολο $[10, 99] = \{10, 11, \dots, 98, 99\}$, 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;

Λύση. i) Το σύνολο περιέχει $99/3 - 9/3 = 30$ πολλαπλάσια του 3. Πράγματι, ένα πολλαπλάσιο του 3 στο σύνολο είναι της μορφής $3k$, με

$$10 \leq 3k \leq 99 \Leftrightarrow 10/3 \leq k \leq 99/3 \Leftrightarrow 3 + 1/3 \leq k \leq 33 \stackrel{k \in \mathbb{N}^*}{\Leftrightarrow} 4 \leq k \leq 33$$

και $|[4, 33]| = 30$. Άρα το σύνολο περιέχει $n = 60$ αριθμούς που δεν είναι πολλαπλάσια του 3 και επομένως πρέπει να επιλέξουμε τουλάχιστον $n + 1 = 61$ αριθμούς.

ii) Το σύνολο διαμερίζεται σε $n = 9$ υποσύνολα που το καθένα περιέχει 10 αριθμούς με ίδιο πρώτο ψηφίο. Τα σύνολα αυτά είναι τα

$$[10, 19], [20, 29], [30, 39], \dots, [90, 99].$$

Άρα, πρέπει να επιλέξουμε τουλάχιστον $n + 1 = 10$ αριθμούς, ώστε δύο να ανήκουν αναγκαστικά στο ίδιο υποσύνολο. \square

Ασκήσεις για την 2η απαλλακτική πρόοδο Διαλέξεις 7,10

Πολλαπλασιαστική αρχή ή Κανόνας γινομένου

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.

Έστω E ένα σύνολο με n στοιχεία, δηλαδή $|E| = n$. (Παρατήρηση: $|E|$ ονομάζεται **πληθάριθμος** ή **πληθικός αριθμός** του E).

Κάθε διατεταγμένη m -άδα (a_1, a_2, \dots, a_m) με $a_i \in E$ για κάθε $i \in [m] = \{1, 2, \dots, m\}$ ονομάζεται **διάταξη των n στοιχείων ανά m** (m -permutation of n elements).

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**.

Αριθμός διατάξεων $P(n, m)$ n στοιχείων ανά m

$$P(n, m) = \underbrace{n(n-1)(n-2) \cdots (n-m+1)}_{m \text{ όροι}} = \frac{n!}{(n-m)!}$$

όπου $n!$ (n παραγοντικό) ισούται με

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n, \text{ όταν } n \geq 1$$

και

$$0! = 1$$

Αριθμός μεταθέσεων n στοιχείων

$$P_n = n!$$

Αριθμός επαναληπτικών διατάξεων n στοιχείων ανά m

$$U(n, m) = n^m$$

Άσκηση 1. Πόσους πενταψήφιους φυσικούς αριθμούς μπορούμε να κατασκευάσουμε με τα ψηφία

1, 2, 3, 4, 5, 6, 7, 8, 9, όταν

- (i) πρέπει να έχουν τα ψηφία τους διαφορετικά,
- (ii) τα ψηφία τους μπορεί να επαναλαμβάνονται,
- (iii) πρέπει να είναι άρτιοι αριθμοί και τα ψηφία τους να είναι διαφορετικά
- (iv) το άθροισμα του πρώτου και του τελευταίου ψηφίου τους να είναι ίσο με 4 και τα ψηφία τους μπορούν να επαναλαμβάνονται.

Λύση. Ο τυχαίος πενταψήφιος αριθμός θα είναι της μορφής $x = x_1x_2x_3x_4x_5$, όπου $x_i \in [9]$, το i -οστό ψηφίο του αριθμού.

i) Για το x_1 υπάρχουν 9 επιλογές.

Για το x_2 υπάρχουν 8 επιλογές.

Για το x_3 υπάρχουν 7 επιλογές.

Για το x_4 υπάρχουν 6 επιλογές.

Για το x_5 υπάρχουν 5 επιλογές.

Άρα, από τον κανόνα του γινομένου υπάρχουν $P(9, 5) = \frac{9!}{(9-5)!} = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$

διαφορετικοί αριθμοί.

ii) Κάθε x_i επιλέγεται με 9 τρόπους, οπότε συνολικά υπάρχουν 9^5 τέτοιοι αριθμοί.

iii) Το x_5 επιλέγεται άρτιος με 4 τρόπους, δηλαδή $x_5 \in \{2, 4, 6, 8\}$, και τα υπόλοιπα 4 επιλέγοντας μεταξύ των υπόλοιπων 8 αριθμών με $P(8, 4)$ τρόπους. Συνολικά προκύπτουν $4P(8, 4) = 4 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ τρόποι.

iv) Θα πρέπει να είναι $x_1 + x_5 = 4$. Επειδή

$$4 = 1 + 3 = 2 + 2 = 3 + 1,$$

τα x_1, x_5 επιλέγονται με 3 τρόπους. Τα υπόλοιπα 3 ψηφία επιλέγονται με 9^3 τρόπους. Συνολικά προκύπτουν $3 \cdot 9^3 = 3^7$ τέτοιοι αριθμοί. \square

Έστω ένα σύνολο E με $|E| = n$.

Κάθε σύνολο που αποτελείται από m στοιχεία του E ονομάζεται **συνδυασμός των n στοιχείων ανά m** (m -combination of n elements).

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**.

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.

Αριθμός συνδυασμών $\binom{n}{m}$ n στοιχείων ανά m

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Αριθμός επαναληπτικών συνδυασμών των n στοιχείων ανά m

$$E(n, m) = \begin{bmatrix} n \\ m \end{bmatrix} = \binom{n+m-1}{m}$$

Άσκηση 2. Με πόσους τρόπους μπορούν να χωρισθούν 20 φοιτητές σε 3 ομάδες των 10, 6 και 4 ατόμων αντίστοιχα.

$a \quad b \quad c$

Λύση. Υπάρχουν $\binom{20}{10}$ τρόποι για να επιλέξουμε τους φοιτητές της ομάδας των 10 ατόμων. Στην συνέχεια, υπάρχουν $\binom{20-10}{6} = \binom{10}{6}$ τρόποι για να επιλέξουμε τους φοιτητές της ομάδας των 6 ατόμων. Και $\binom{10-6}{4} = \binom{4}{4} = 1$ τρόπος για να επιλέξουμε τους φοιτητές της ομάδας των 4 ατόμων.

Άρα, από τον κανόνα του γινομένου υπάρχουν $\binom{20}{10} \cdot \binom{10}{6} \cdot \binom{4}{4} = \frac{20!}{10! \cdot 6! \cdot 4!}$ τρόποι να χωρισθούν οι 20 φοιτητές σ αυτές τις 3 ομάδες. □

$a \quad b \quad c \quad \dots$

Άσκηση 3. Με πόσους τρόπους ένα τριμελές συμβούλιο μπορεί να σχηματισθεί από 4 αντρώγυνα

$A_1 \Gamma_1 \quad A_2 \Gamma_2 \quad A_3 \Gamma_3 \quad A_4 \Gamma_4$

1. αν όλοι είναι εξίσου εκλέξιμοι,
2. αν το συμβούλιο πρέπει να περιλαμβάνει δύο γυναίκες και έναν άντρα,
3. αν και οι δύο σύζυγοι δεν μπορούν να παρευρίσκονται στο συμβούλιο.

Λύση. i) Υπάρχουν συνολικά $n = 8$ άτομα, επομένως τα 3 μέλη επιλέγονται με $\binom{8}{3}$ τρόπους

ii) Επιλέγονται 2 από τις 4 γυναίκες με $\binom{4}{2}$ τρόπους και ένας από τους 4 άντρες με $\binom{4}{1}$ τρόπους, οπότε συνολικά υπάρχουν $\binom{4}{2} \binom{4}{1} = \frac{4!}{2!2!} 4 = 24$ τρόποι σχηματισμού του συμβουλίου.

iii) Αρχικά επιλέγουμε 3 από τα 4 ζευγάρια με $\binom{4}{3} = 4$ τρόπους και στη συνέχεια ένα άτομο από κάθε επιλεγμένο ζευγάρι. Για κάθε ένα από τα 3 ζευγάρια υπάρχουν 2 τρόποι να επιλέξουμε το άτομο που θα συμπεριληφθεί στο συμβούλιο, οπότε υπάρχουν 2^3 επιλογές των 3 ατόμων. Συνολικά προκύπτουν $4 \cdot 2^3 = 32$ τρόποι. □

Άσκηση 4. 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.

Λύση. 8Μ, 6Φ, 7Χ, $n = 8 + 7 + 6 = 21$. **(1ος τρόπος)** Διακρίνουμε περιπτώσεις για τον αριθμό των φυσικών που συμμετέχουν στην επιτροπή:

- 1 φυσικός.

Υπάρχουν $\binom{6}{1}$ τρόποι για να επιλέξουμε τον 1 φυσικό και $\binom{15}{4}$ τρόποι για να επιλέξουμε τα υπόλοιπα μέλη. Άρα, $\binom{6}{1} \cdot \binom{15}{4}$ τρόποι.

- 2 φυσικοί.

Υπάρχουν $\binom{6}{2}$ τρόποι για να επιλέξουμε τους 2 φυσικούς και $\binom{15}{3}$ τρόποι για να επιλέξουμε τα υπόλοιπα μέλη. Άρα, $\binom{6}{2} \cdot \binom{15}{3}$ τρόποι.

- 3 φυσικοί

Υπάρχουν $\binom{6}{3}$ τρόποι για να επιλέξουμε τους 3 φυσικούς και $\binom{15}{2}$ τρόποι για να επιλέξουμε τα υπόλοιπα μέλη. Άρα, $\binom{6}{3} \cdot \binom{15}{2}$ τρόποι.

- 4 φυσικοί

Υπάρχουν $\binom{6}{4}$ τρόποι για να επιλέξουμε τους 4 φυσικούς και $\binom{15}{1}$ τρόποι για να επιλέξουμε τα υπόλοιπα μέλη. Άρα, $\binom{6}{4} \cdot \binom{15}{1}$ τρόποι.

- 5 φυσικοί

Υπάρχουν $\binom{6}{5}$ τρόποι για να επιλέξουμε τους 5 φυσικούς και $\binom{15}{0} = 1$ τρόποι για να επιλέξουμε τα υπόλοιπα μέλη. Άρα, $\binom{6}{5} \cdot \binom{15}{0}$ τρόποι.

Συνολικά, υπάρχουν $\binom{6}{1} \cdot \binom{15}{4} + \binom{6}{2} \cdot \binom{15}{3} + \binom{6}{3} \cdot \binom{15}{2} + \binom{6}{4} \cdot \binom{15}{1} + \binom{6}{5} \cdot \binom{15}{0}$ τρόποι σχηματισμού της επιτροπής.

(2ος τρόπος) Το πλήθος των επιτροπών χωρίς περιορισμό είναι ίσο με $\binom{21}{5}$.

Το πλήθος των επιτροπών χωρίς φυσικό είναι ίσο με $\binom{15}{5}$.

Άρα το ζητούμενο πλήθος είναι $\binom{21}{5} - \binom{15}{5}$. □

Αριθμός μεταθέσεων k ειδών στοιχείων με
 n_1, n_2, \dots, n_k στοιχεία αντίστοιχα.

$$M(n_1, n_2, \dots, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}$$

όπου $n = n_1 + n_2 + \dots + n_k$.

Άσκηση 5. Πόσες είναι οι μεταθέσεις των γραμμάτων της λέξης
 Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Υ Π Ο Λ Ι Σ

Λύση. Ας συμβολίσουμε με W την τυχαία λέξη και με $|W|_x$ το πλήθος των εμφανίσεων του γράμματος x στην W . Το μήκος της W είναι $n = 18$. Το ζητούμενο πλήθος είναι

$$\frac{n!}{|W|_{\Pi}! |W|_A! |W|_N! |W|_E! |W|_I! |W|_{\Sigma}! |W|_T! |W|_H! |W|_M! |W|_O! |W|_Y! |W|_{\Lambda}!} = \frac{18!}{3!1!1!1!3!2!1!1!2!1!1!} \quad \square$$

Άσκηση 6. 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.

Λύση. Όπως σε προηγούμενη άσκηση, προκύπτουν $\frac{8!}{1!1!1!1!1!1!1!} = 8!$ τρόποι.

Αν τα Α, Ρ πρέπει να είναι διαδοχικά, τότε θεωρούνται ως ένα γράμμα και προκύπτουν $7! \cdot 2$ τρόποι. Ο συντελεστής 2 προκύπτει επειδή επιλέγουμε αν εμφανίζεται πρώτο το Α ή το Ρ. □

Άσκηση 7. Κατά πόσους τρόπους 4 λευκές 5 κίτρινες και 9 μαύρες μπάλες μπορούν να διαταχθούν:

Λ Κ Κ Μ Κ Π Π Κ Κ Μ Μ ---

1. Χωρίς περιορισμό.
2. Αν κάθε διάταξη τους αρχίζει με λευκή και τελειώνει με μαύρη μπάλα.

Λύση. i) Χωρίς περιορισμό, έχουμε $\frac{18!}{4!5!9!}$.

ii) Αφού συμπληρωθούν η πρώτη και τελευταία θέση (με έναν τρόπο), απομένουν 16 μπάλες οι οποίες έχουν $\frac{16!}{3!5!8!}$ τρόποι για να διαταχθούν. □

Ακέραιες Λύσεις Γραμμικής Εξίσωσης

Ο αριθμός των μη αρνητικών ακέραιων λύσεων $x_i, i \in [n]$ της γραμμικής εξίσωσης

$$x_1 + x_2 + \dots + x_n = m \tag{1}$$

όπου $m, n \in \mathbb{N}^*$ είναι ίσος με $\begin{bmatrix} n \\ m \end{bmatrix} = \binom{n+m-1}{m}$.

Άσκηση 8. 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;

Λύση. (1ος τρόπος) Κατανέμουμε τους 4 ορόφους στα 5 άτομα, επαναληπτικά, με

$$\begin{bmatrix} 4 \\ 5 \end{bmatrix} = \binom{4+5-1}{5} = \binom{8}{5} \quad x_1 \ x_2 \ x_3 \ x_4$$

(2ος τρόπος) Κάθε κατανομή των 5 ατόμων στους 4 ορόφους αντιστοιχεί σε μη αρνητική ακέραια λύση της εξίσωσης

$$\overset{1}{x_1} + \overset{0}{x_2} + \overset{2}{x_3} + \overset{1}{x_4} = 5$$

όπου x_i είναι ο αριθμός των ατόμων που βγαίνουν στον όροφο $i, i \in [4]$. Επομένως, ο ζητούμενος αριθμός ισούται με πλήθος των λύσεων της εξίσωσης, δηλαδή με $\begin{bmatrix} 4 \\ 5 \end{bmatrix} = \binom{4+5-1}{5} = \binom{8}{5}$. □

Έστω $a, b \in \mathbb{N}^*$ με $a = \pi b + \nu$, όπου $0 \leq \nu < b$. Τότε ισχύει ότι

$$\text{ΜΚΔ}(a, b) = \text{ΜΚΔ}(b, \nu).$$

Επιπλέον, αν $\nu = 0$, τότε $\text{ΜΚΔ}(a, b) = b$.

Άσκηση 9. Να βρεθεί ο ΜΚΔ των 12075 και 4655.

Λύση. Έχουμε ότι

$$12075 = 2 \cdot 4655 + 2765$$

$$4655 = 1 \cdot 2765 + 1890$$

$$2765 = 1 \cdot 1890 + 875$$

$$1890 = 2 \cdot 875 + 140$$

$$875 = 6 \cdot 140 + \underline{35}$$

$$140 = 4 \cdot \underline{35} + 0.$$

Άρα, $\text{ΜΚΔ}(12075, 4655) = 35$. □

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 $\mathbf{a} \equiv \mathbf{b} \pmod{\mathbf{n}}$ αν και μόνο αν n 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** .

Άσκηση 10. Για ποιους φυσικούς αριθμούς m ισχύουν οι ισοδυναμίες

i) $35 \equiv 2 \pmod{m}$.

iii) $347 \equiv 0 \pmod{m}$.

ii) $1000 \equiv 1 \pmod{m}$.

Λύση. i) $35 \equiv 2 \pmod{m} \Leftrightarrow m \mid 35 - 2 \Leftrightarrow m \mid 33$. Οπότε τα ζητούμενα m είναι οι θετικοί διαιρέτες του 33 δηλαδή τα 1, 3, 11 και 33.

ii) Ομοίως, $m \mid 347 - 0$. Επειδή 347 είναι πρώτος έπεται ότι $m = 1, 347$.

iii) Ομοίως, $m \mid 1000 - 1 = 999 = 3^3 \cdot 37$. Οπότε τα ζητούμενα m είναι οι αριθμοί 1, 3, 3^2 , 3^3 , 37, $3 \cdot 37$, $3^2 \cdot 37$, $3^3 \cdot 37 = 999$. □

$$m = 3^x \cdot 37^y, 0 \leq x \leq 3, 0 \leq y \leq 1$$

Έστω $\phi(n)$ το πλήθος των αριθμών m που είναι μικρότεροι ή ίσοι από το n και ισχύει ότι $\text{GCD}(n, m) = 1$, δηλαδή τα n και m είναι σχετικά πρώτοι μεταξύ τους.

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, \dots, p_k είναι πρώτοι αριθμοί και a_1, a_2, \dots, a_k είναι φυσικοί αριθμοί. Τότε

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}).$$

Άσκηση 11. 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 $m, n \in \mathbb{N}^*$.

Λύση. i)

$$\phi(31) = 31^1 - 31^0 = 30. \text{ (Ο 31 είναι πρώτος αριθμός)}$$

$$\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100.$$

$$\phi(55) = \phi(5 \cdot 11) = (5^1 - 5^0)(11^1 - 11^0) = 40.$$

$$\phi(7!) = \phi(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7) = \phi(2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7) = \phi(2^4 \cdot 3^2 \cdot 5 \cdot 7) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0) = 8 \cdot 6 \cdot 4 \cdot 6 = 192.$$

ii)

$$\phi(30^m) = \phi((2 \cdot 3 \cdot 5)^m) = \phi(2^m \cdot 3^m \cdot 5^m) = (2^m - 2^{m-1})(3^m - 3^{m-1})(5^m - 5^{m-1}).$$

$$\phi(10^m \cdot 20^n) = \phi(2^m \cdot 5^m \cdot (2^2)^n \cdot 5^n) = \phi(2^{m+2n} 5^{m+n}) = (2^{m+2n} - 2^{m+2n-1})(5^{m+n} - 5^{m+n-1}). \quad \square$$

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 $p(x) = c_0 + c_1x + \dots + c_kx^k$ είναι ένα πολυώνυμο με ακέραιους συντελεστές και $a \equiv b \pmod{n}$, τότε

$$p(a) \equiv p(b) \pmod{n}.$$

Θεώρημα Euler. Αν a, m είναι φυσικοί αριθμοί και $\text{ΜΚΔ}(a, m) = 1$, τότε ισχύει ότι

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Άσκηση 12. Να βρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί τις εξισώσεις

$$i) x \equiv 2^{304} \pmod{7}. \quad iv) x \equiv 20^{640} \pmod{17}. \quad vii) x \equiv 13^{802} \pmod{55}.$$

$$ii) x \equiv 15^{101} \pmod{8}. \quad v) x \equiv 20^{323} \pmod{17}. \quad viii) x \equiv 18^{51} \pmod{30}.$$

$$iii) x \equiv 15^{2011} \pmod{3}. \quad vi) x \equiv 11^{481} \pmod{45}. \quad ix) x \equiv 31^{30} \pmod{100}.$$

Λύση. i) Επειδή $\text{ΜΚΔ}(7, 2) = 1$ και $\phi(7) = 6$ έπεται ότι $2^6 \equiv 1 \pmod{7}$. Επομένως,

$$x \equiv 2^{304} \equiv 2^{6 \cdot 50 + 4} \equiv (2^6)^{50} 2^4 \equiv 1^{50} \cdot 16 \equiv 2 \pmod{7}.$$

Άρα, $x = 2$.

v) Επειδή $\text{ΜΚΔ}(20, 17) = 1$ και $\phi(17) = 16$ έπεται ότι $20^{16} \equiv 1 \pmod{17}$.

Επιπλέον, $20 \equiv 3 \pmod{17}$. Επομένως,

$$x \equiv 20^{323} \equiv 3^{323} \equiv 3^{16 \cdot 20 + 3} \equiv (3^{16})^{20} 3^3 \equiv 1^{20} \cdot 27 \equiv 10 \pmod{17}.$$

Άρα, $x = 10$.

viii) Επειδή $\text{MKL}(18, 30) = 6 \neq 1$. Δεν μπορεί να εφαρμοσθεί το θεώρημα του Euler. Πρέπει να χρησιμοποιήσουμε τις γενικές ιδιότητες των ισотиμιών.

$$x \equiv 18^{51} \equiv (18)^{2 \cdot 25 + 1} \equiv 324^{25} \cdot 18 \pmod{30}.$$

Όμως $324 = 10 \cdot 30 + 24$, οπότε $324 \equiv 24 \pmod{30}$. Άρα,

$$x \equiv 18^{51} \equiv 24^{25} \cdot 18 \equiv 24^{2 \cdot 12 + 1} \cdot 18 \equiv 576^{12} \cdot 24 \cdot 18 \pmod{30}$$

Όμως $576 = 19 \cdot 30 + 6$ οπότε $576 \equiv 6 \pmod{30}$. Άρα,

$$x \equiv 576^{12} \cdot 24 \cdot 18 \equiv 6^{12} \cdot 24 \cdot 18 \equiv (6^2)^6 \cdot 432 \equiv 36^6 \cdot 432 \pmod{30}.$$

Όμως, $432 = 14 \cdot 30 + 12$ και $36 = 1 \cdot 30 + 6$ οπότε $432 \equiv 12 \pmod{30}$ και $36 \equiv 6 \pmod{30}$. Άρα,

$$\begin{aligned} x &\equiv 36^6 \cdot 432 \equiv 6^6 \cdot 12 \equiv 36 \cdot 36 \cdot 36 \cdot 12 \equiv 6 \cdot 6 \cdot 6 \cdot 2 \cdot 6 \equiv 36 \cdot 36 \cdot 2 \\ &\equiv 6 \cdot 6 \cdot 2 \equiv 36 \cdot 2 \equiv 6 \cdot 2 \equiv 12 \pmod{30}. \end{aligned}$$

Άρα, $x = 12$.

ix) Επειδή $\text{MKL}(100, 31) = 1$ και $\phi(100) = 40$ έπεται ότι $31^{40} \equiv 1 \pmod{100}$

Στην περίπτωση μας ο εκθέτης του 31 είναι 30 που είναι μικρότερος του 40 οπότε δεν μπορούμε να αξιοποιήσουμε το θεώρημα του Euler. Πρέπει να αρκεστούμε στις γενικές ιδιότητες των ισottiμιών.

$$x \equiv 31^{30} \equiv (31^2)^{15} \equiv 961^{15} \pmod{100}.$$

Όμως, $961 \equiv 61 \pmod{100}$ οπότε

$$x \equiv 961^{15} \equiv 61^{15} \equiv 61 \cdot (61^2)^7 \equiv 61 \cdot (3721)^7 \pmod{100}$$

Όμως, $3721 \equiv 21 \pmod{100}$ οπότε

$$x \equiv 61 \cdot (3721)^7 \equiv 61 \cdot 21^7 \equiv 61 \cdot 21 \cdot (21^2)^3 \equiv 1281 \cdot 441^3 \pmod{100}$$

Όμως, $1281 \equiv 81 \pmod{100}$ και $441 \equiv 41 \pmod{100}$ οπότε

$$x \equiv 1281 \cdot 441^3 \equiv 81 \cdot 41^3 \equiv 81 \cdot 41 \cdot 41^2 \equiv 3321 \cdot 1681 \equiv 21 \cdot 81 \equiv 1701 \equiv 1 \pmod{100}.$$

Άρα $x = 1$. □

Άσκηση 13. Να δειχθεί ότι ο 13 διαιρεί τον $2^{70} + 3^{70}$.

Λύση. Αρκεί να δειχθεί ότι $2^{70} + 3^{70} \equiv 0 \pmod{13}$. Επειδή $\text{MKL}(13, 2) = \text{MKL}(13, 3) = 1$ και $\phi(13) = 12$ έπεται ότι $2^{12} \equiv 1 \pmod{13}$ και $3^{12} \equiv 1 \pmod{13}$. Επομένως,

$$2^{70} + 3^{70} \equiv 2^{5 \cdot 12 + 10} + 3^{5 \cdot 12 + 10} \equiv (2^{12})^5 \cdot 2^{10} + (3^{12})^5 \cdot 3^{10} \equiv 2^{10} + 3^{10} \equiv 4^5 + 9^5 \pmod{13}$$

Όμως $4^5 = 4 \cdot 4^4 = 4 \cdot 16^2$ και $9^5 = 9 \cdot 9^4 = 9 \cdot 81^2$. Επιπλέον, $16 \equiv 3 \pmod{13}$ και $81 \equiv 3 \pmod{13}$. Επομένως,

$$4^5 + 9^5 \equiv 4 \cdot 16^2 + 9 \cdot 81^2 \equiv 4 \cdot 3^2 + 9 \cdot 3^2 \equiv 13 \cdot 9 \equiv 0 \pmod{13} \quad \square$$

Άσκηση 14. Ναδειχθεί ότι ο $11 \cdot 31$ διαιρεί τον $20^{15} - 1$.

Λύση. Επειδή οι αριθμοί 11 και 31 είναι πρώτοι αριθμοί πρέπει ναδειχθεί ότι $11|20^{15} - 1$ και $31|20^{15} - 1$. Ισοδύναμα, $20^{15} \equiv 1 \pmod{11}$ και $20^{15} \equiv 1 \pmod{31}$

Επειδή $\text{ΜΚΔ}(11, 20) = \text{ΜΚΔ}(31, 20) = 1$ και $\phi(11) = 10$, $\phi(31) = 30$ έπεται ότι $20^{10} \equiv 1 \pmod{11}$, $20^{30} \equiv 1 \pmod{31}$.

Επομένως, για το 11 έχουμε ότι:

$$20^{15} \equiv 20^{10} \cdot 20^5 \equiv 1^{10} \cdot 20^5 \equiv 20^2 \cdot 20^2 \cdot 20 \equiv 400 \cdot 400 \cdot 20 \pmod{11}.$$

Όμως, $20 \equiv 9 \pmod{11}$ και $400 = 36 \cdot 11 + 4$ οπότε $400 \equiv 4 \pmod{11}$. Άρα,

$$400 \cdot 400 \cdot 20 \equiv 4 \cdot 4 \cdot 9 \equiv 16 \cdot 9 \equiv 5 \cdot 9 \equiv 45 \equiv 1 \pmod{11}$$

Επίσης, για το 31 έχουμε ότι:

$$20^{15} \equiv (20^2)^7 \cdot 20 \equiv 400^7 \cdot 20 \pmod{31}$$

Όμως, $400 = 12 \cdot 31 + 28$ οπότε $400 \equiv 28 \equiv -3 \pmod{31}$. Άρα,

$$400^7 \cdot 20 \equiv (-3)^7 \cdot 20 \equiv (-1)^7 \cdot 3^7 \cdot 20 \equiv (-1) \cdot 3^7 \cdot (-11) \equiv 11 \cdot 3^7 \pmod{31}$$

Όμως $3^7 = 3^4 \cdot 3^3 = 81 \cdot 3 \cdot 9$ και $81 = 3 \cdot 31 + 19$ οπότε $81 \equiv 19 \pmod{31}$. Άρα,

$$11 \cdot 3^7 \equiv 11 \cdot 19 \cdot 3 \cdot 9 \equiv 99 \cdot 57 \pmod{31}$$

Όμως $99 = 3 \cdot 31 + 6$ και $57 = 1 \cdot 31 + 26$ οπότε $99 \equiv 6 \pmod{31}$ και $57 \equiv 26 \pmod{31}$. Άρα,

$$99 \cdot 57 \equiv 6 \cdot 26 \equiv 156 \equiv 1 \pmod{31}$$

αφού $156 = 5 \cdot 31 + 1$.

Επομένως, οι αριθμοί 11 και 31 διαιρούν τον $20^{15} - 1$. □