ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ
1η ΔΙΑΛΕΞΗ

- **Διαιρετότητα**
  - **Αλγόριθμος διαίρεσης**
  - **Ιδιότητες διαιρετότητας**
- **Μέγιστος κοινός διαιρέτης**
  - **Αλγόριθμος του Ευκλείδη**
  - **Επεκταμένος αλγόριθμος του Ευκλείδη**

Διαιρετότητα

Έστω $a, b \in \mathbb{Z}$. Λέμε ότι ο b **διαιρεί** τον a αν υπάρχει ακέραιος αριθμός $\pi \in \mathbb{Z}$ τέτοιος $a = \pi b$. Στην περίπτωση αυτή γράφουμε $\mathbf{b \mid a}$ και λέμε ότι ο b είναι **διαιρέτης** του a, ενώ ο a είναι **πολλαπλάσιο** του b:

$$b \mid a \Leftrightarrow \text{Υπάρχει ακέραιος } \pi \in \mathbb{Z} \text{ ώστε } a = \pi b$$

- (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 δεν υπάρχει ακέραιος αριθμός π που επαληθεύει την εξίσωση $a = \pi b$ λέμε ότι ο b **δεν διαιρεί** τον a και γράφουμε $\mathbf{b \nmid a}$.

Για παράδειγμα,

$$13 \mid 26 \text{ διότι } 26 = 2 \cdot 13$$

και

$$13 \nmid 17 \text{ διότι δεν υπάρχει ακέραιος } \pi \text{ ώστε } 17 = \pi \cdot 13.$$

Γενικότερα ισχύει η επόμενη πρόταση.

Πρόταση 1 (Αλγόριθμος της διαίρεσης)

Αν a είναι ακέραιος και b είναι μη μηδενικός ακέραιος, τότε υπάρχουν μοναδικοί ακέραιοι π και υ ώστε

$$a = \pi b + \upsilon, \ \text{όπου } 0 \leq \upsilon < |b|.$$

Απόδειξη. Έστω S το σύνολο των **μη αρνητικών αριθμών** της μορφής $r = a - k \cdot b$ όπου $k \in Z$.

Το S είναι μη κενό σύνολο φυσικών αριθμών, αφού

- αν a, b θετικοί, τότε περιέχει τον αριθμό $a - (-1) \cdot b = a + b \geq 0$.
- αν a, b αρνητικοί, τότε περιέχει τον αριθμό $a - (-a) \cdot b = a(1 + b) \geq 0$.
- αν a θετικός, b αρνητικός, τότε περιέχει τον αριθμό $a - 1 \cdot b = a - b \geq 0$.
- αν a αρνητικός, b θετικός, τότε περιέχει τον αριθμό $a - a \cdot b = a(1 - b) \geq 0$.

Από την αρχή της καλής διάταξης, κάθε μη κενό σύνολο φυσικών έχει ελάχιστο στοιχείο.

Έστω υ το ελάχιστο στοιχείο του S και π η τιμή του k ώστε

$$\upsilon = a - \pi b$$

Προφανώς $\upsilon \geq 0$. Επειδή το υ είναι το ελάχιστο στοιχείο του S

- Αν $b > 0$ τότε $r = a - (\pi + 1)b = a - \pi b - b = \upsilon - b < \upsilon$ οπότε $r \notin S$, δηλαδή $\upsilon - b < 0$, άρα $\upsilon < b = |b|$.
- Αν $b < 0$, τότε $r = a - (\pi - 1)b = a - \pi b + b = \upsilon + b < \upsilon$ οπότε $r \notin S$, δηλαδή $\upsilon + b < 0$, άρα $\upsilon < -b = |b|$.

Επομένως, υπάρχουν ακέραιοι π, υ ώστε $a = \pi b + \upsilon$ και $0 \leq \upsilon < |b|$.
Στην συνέχεια θα δείξουμε ότι οι αριθμοί π, υ είναι μοναδικοί. Έστω ότι για τους φυσικούς αριθμούς π' και υ' ισχύει ότι

$$a = \pi' b + \upsilon' \text{ όπου } 0 \leq \upsilon' < |b|.$$

Τότε $\pi b + \upsilon = \pi' b + \upsilon'$ οπότε $(\pi - \pi')b = \upsilon' - \upsilon$.
Αν $\pi - \pi' \neq 0$ τότε $\upsilon' - \upsilon$ είναι ακέραιο πολλαπλάσιο του $|b|$, άρα

- είτε $\upsilon' - \upsilon \geq |b| \Leftrightarrow \upsilon' = |b| + \upsilon \geq |b|$,
- είτε $\upsilon' - \upsilon \leq -|b| \Leftrightarrow \upsilon \geq \upsilon' + |b| \geq |b|$,

άτοπο. Επομένως, οι αριθμοί π, υ είναι μοναδικοί. □.

Παραδείγματα. 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, $13 \nmid -20$.

Παρατηρήσεις

1. Η πρόταση αυτή αντιστοιχεί 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. Στην περίπτωση που $\upsilon = 0$ η διαίρεση ονομάζεται **τέλεια**, ενώ αν $\upsilon \neq 0$ τότε η διαίρεση ονομάζεται **ατελής**.
2. **Προσοχή!** Το υπόλοιπο της διαίρεσης υ είναι πάντα μη αρνητικός αριθμός φραγμένος από το 0 και το $|b| - 1$.
3. Αν μας δοθούν δύο ακέραιοι αριθμοί a, b είναι υπολογιστικά αποδοτικό να βρεθούν οι αριθμοί π, υ ώστε $a = \pi b + \upsilon$, όπου $0 \leq \upsilon < |b|$.
   Αντίθετα, αν δοθεί ένας ακέραιος αριθμός m θεωρείται υπολογιστικά ανέφικτο να βρεθούν οι διαιρέτες του m αν έχει για παράδειγμα 300 ή περισσότερο ψηφία.

Οι αριθμοί π και υ της διαίρεσης του a με τον b μπορούν να εκφραστούν με την βοήθεια του συμβολισμού του ακέραιου μέρους:

Λήμμα 1

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

$$\pi = \lfloor \frac{a}{b} \rfloor \text{ και } \upsilon = a - \lfloor \frac{a}{b} \rfloor b.$$

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 $\upsilon = a - \pi b = a - \lfloor \frac{a}{b} \rfloor b$. □

Χρησιμοποιώντας την Πρόταση 1, 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** $a \mid c$**, τότε** $a \mid (xb + yc)$ **για οποιουσδήποτε ακέραιους** x, y**.**
5. Αν $a \mid b$ και $a \nmid c$, τότε $a \nmid (b + c)$.
6. Αν $a \mid b$, τότε $a \mid bc$.
7. Αν $a \mid b$ και $b \mid c$, τότε $a \mid c$, (για $b \neq 0$).
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 $a \mid |b|$.
12. **Ο μέγιστος διαιρέτης του** a **είναι ο** $|a|$**.**

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 $3 \mid 21$.

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 $\mu\kappa\delta(a, b)$, ή $\gcd(a, b)$.
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,
- 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 $\gcd(12, 4) = 4$.

Παρατήρηση. Ο απλοϊκός τρόπος υπολογισμού του ΜΚΔ δύο αριθμών a και b απαιτεί την εύρεση όλων των διαιρετών των a και b και στη συνέχεια την επιλογή του μεγαλύτερου από αυτούς.
Η διαδικασία αυτή είναι ανέφικτη για αριθμούς με πολλά ψηφία.
Μια αποτελεσματικότερη μέθοδος είναι ο **αλγόριθμος του Ευκλείδη** ο οποίος παρουσιάζεται στις προτάσεις 1 και 2 του 7ου βιβλίου των Στοιχείων (περίπου 300 π.Χ).

Αλγόριθμος του Ευκλείδη

Πρόταση 2 (Αλγόριθμος του Ευκλείδη)

Έστω $a, b \in \mathbb{N}^*$ *με* $a = \pi b + \upsilon$, *όπου* $0 \leq \upsilon < b$ *και* $\pi, \upsilon \in \mathbb{N}$.

- *Αν* $\upsilon = 0$ *τότε* $\gcd(a, b) = b$.
- *Ισχύει ότι* $\gcd(a, b) = \gcd(b, \upsilon)$.

Απόδειξη.

- Αν $\upsilon = 0$, τότε $b|a$ οπότε $\gcd(a, b) = b$.
- Έστω $d = \gcd(a, b)$ και $d' = \gcd(b, \upsilon)$.
  − Επειδή $d|a$ και $d|b$ έπεται ότι $d|\upsilon = a - \pi b$, άρα ο d είναι κοινός διαιρέτης των b, υ οπότε $d \leq d'$.
  − Επειδή $d'|b$ και $d'|\upsilon$ έπεται ότι $d'|a = \pi b + \upsilon$, άρα ο d' είναι κοινός διαιρέτης των a, b, οπότε $d' \leq d$.
  Επομένως, $d = d'$. □

Για παράδειγμα, ο υπολογισμός του ΜΚΔ των 168 και 25 προκύπτει με τη βοήθεια των παρακάτω ισοτήτων που περιγράφουν τις διαιρέσεις κάθε βήματος:

$$\begin{aligned} 168 &= 6 \cdot 25 + 18, \\ 25 &= 1 \cdot 18 + 7, \\ 18 &= 2 \cdot 7 + 4, \\ 7 &= 1 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Άρα, $\text{ΜΚΔ}(168, 25) = 1$.

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, $\text{ΜΚΔ}(2520, 154) = 14$.

Παρατηρήσεις

- Σημαντική συνέπεια του αλγορίθμου του Ευκλείδη είναι ότι ο ΜΚΔ των a, b προσδιορίζεται **χωρίς την εύρεση των διαιρετών τους** αλλά με επαναλαμβανόμενη εφαρμογή του αλγορίθμου της διαίρεσης μέχρις ότου το υπόλοιπο γίνει μηδέν. (Μια απόδειξη ότι οι διαιρέσεις που απαιτούνται είναι πεπερασμένες σε δίδεται στην Πρόταση 3)
- Ο υπολογισμός του $\gcd(a, b)$ για τους φυσικούς αριθμούς a, b, με τον αλγόριθμο του Ευκλείδη μπορεί να γίνει χρησιμοποιώντας τις αναδρομικές σχέσεις

$$\gcd(a, 0) = a,$$
$$\gcd(a, b) = \gcd(b, v),$$

όπου v 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.

```
import numpy as np
n = 14954241426040742485625500091643838845577609609481205 0
m = 36171876776892343456810139793949710076323434096763430097 50
#numpy version
print("gcd(",n,",",m,")=",np.gcd(n,m))
#recursive version
def gcd2(a, b):
    upoloipo = a % b
    if(upoloipo==0): turn b
    else: return gcd2(b,upoloipo)
print("gcd(",n,",",m,")=",gcd2(n,m))
#iterative version
def gcd3(a, b):
    upoloipo = a % b
    while(upoloipo != 0):
        a = b
        b = upoloipo
        upoloipo = a % b
    return b
print("gcd(",n,",",m,")=",gcd3(n,m))
```

Παρατηρήσεις

1. Ο μέγιστος κοινός διαιρέτης των a και b είναι ο μέγιστος θετικός ακέραιος d που ικανοποιεί τις παρακάτω δύο ιδιότητες:
   1. $d \mid a$ και $d \mid b$, και
   2. 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

$$\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n).$$

Παρατήρηση. Χρησιμοποιώντας το Λήμμα 1:

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

$$\pi = \lfloor \frac{a}{b} \rfloor \text{ και } \upsilon = a - \lfloor \frac{a}{b} \rfloor b.$$

μπορούμε να αποδείξουμε ότι ο αλγόριθμος του Ευκλείδη τερματίζει μετά από πεπερασμένο αριθμό βημάτων.

Πρόταση 3

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 (v_i) είναι γνησίως φθίνουσα ακολουθία φυσικών αριθμών.
Πράγματι, επειδή $v_{-1} = a$ και $v_0 = b$, από το Λήμμα 1 προκύπτει ότι το v_i είναι το υπόλοιπο της διαίρεσης του v_{i-2} με το v_{i-1}, οπότε $v_i \in \mathbb{N}$ και $v_i < v_{i-1}$. Επομένως, από την αρχή της καλής διάταξης, η (v_i) λαμβάνει πεπερασμένες τιμές. Έστω m η ελάχιστη τιμή της και $v_k = m$. Αν $m > 0$ έπεται ότι ορίζεται ο v_{k+1} και ισχύει ότι $v_{k+1} < v_k = m$, άτοπο. Άρα, $m = 0$.
Έστω $u_k = 0$. Για κάθε $i \in [k]$ ισχύει ότι $v_i = v_{i-2} - \lfloor \frac{v_{i-2}}{v_{i-1}} \rfloor \cdot v_{i-1}$, ή ισοδύναμα $v_{i-2} = \lfloor \frac{v_{i-2}}{v_{i-1}} \rfloor \cdot v_{i-1} + v_i$, οπότε από την Πρόταση 2 προκύπτει ότι

$$\gcd(v_{i-2}, v_{i-1}) = \gcd(v_{i-1}, v_i) \text{ για κάθε } i \in [k].$$

Επομένως, λόγω μεταβατικότητας, προκύπτει ότι $\gcd(a, b) = \gcd(v_{i-1}, v_i)$ για κάθε $i \in [k]$. Με $i = k$ έχουμε ότι

$$\gcd(a, b) = \gcd(v_{k-1}, v_k) = \gcd(v_{k-1}, 0) = v_{k-1}.$$

□

Για παράδειγμα, ο υπολογισμός του μκδ των 168 και 25 προκύπτει ως εξής:
Αρχικά, θέτουμε $v_{-1} = 168$ και $v_0 = 25$. Στην συνέχεια, για κάθε $i \geq 1$ και όσο $v_{i-1} \neq 0$, υπολογίζουμε τον όρο v_i χρησιμοποιώντας τη σχέση

$$v_i = v_{i-2} - \lfloor \frac{v_{i-2}}{v_{i-1}} \rfloor v_{i-1},$$

οπότε έχουμε ότι

$$v_1 = v_{-1} - \lfloor \frac{v_{-1}}{v_0} \rfloor v_0 = 168 - \lfloor \frac{168}{25} \rfloor 25 = 168 - 6 \cdot 25 = 18$$

$$v_2 = v_0 - \lfloor \frac{v_0}{v_1} \rfloor v_1 = 25 - \lfloor \frac{25}{18} \rfloor 18 = 25 - 1 \cdot 18 = 7$$

$$v_3 = v_1 - \lfloor \frac{v_1}{v_2} \rfloor v_2 = 18 - \lfloor \frac{18}{7} \rfloor 7 = 18 - 2 \cdot 7 = 4$$

$$v_4 = v_2 - \lfloor \frac{v_2}{v_3} \rfloor v_3 = 7 - \lfloor \frac{7}{4} \rfloor 4 = 7 - 1 \cdot 4 = 3$$

$$v_5 = v_3 - \lfloor \frac{v_3}{v_4} \rfloor v_4 = 4 - \lfloor \frac{4}{3} \rfloor 3 = 4 - 1 \cdot 3 = 1$$

$$v_6 = v_4 - \lfloor \frac{v_4}{v_5} \rfloor v_5 = 3 - \lfloor \frac{3}{1} \rfloor 1 = 3 - 3 \cdot 1 = 0.$$

Άρα, $\gcd(168, 25) = v_5 = 1$.

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 4. Για την απόδειξή της, θα χρειαστούμε το επόμενο λήμμα.

Λήμμα 2

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
$\upsilon = a - b < a - a/2 = a/2$. □

Παρατήρηση. Από το προηγούμενο λήμμα προκύπτει ότι σε κάθε επανάληψη του αλγορίθμου του Ευκλείδη ένας από τους δυο αριθμούς υποδιπλασιάζεται.

Πρόταση 4 (**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. □

Παρατήρηση. Η προηγούμενη Πρόταση 4 αποδείχθηκε από το Γάλλο μαθηματικό Gabriel Lamé το 1844.
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.

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

$$\begin{aligned} 14 &= 1 \cdot 56 + (-1) \cdot 42 \\ &= 1 \cdot 56 + (-1) \cdot (1 \cdot 154 + (-2) \cdot 56) = (-1) \cdot 154 + 3 \cdot 56 \\ &= (-1) \cdot 154 + 3 \cdot (1 \cdot 2520 + (-16) \cdot 154) \\ &= 3 \cdot 2520 + (-49) \cdot 154, \end{aligned}$$

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 $(x, y) \in \{(4, 3), (7, 4), (18, 7), (25, 18), (168, 25)\}$

Άσκηση 1

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, $\gcd(12075, 4655) = 32 \cdot 12075 + (-83) \cdot 4655$.

Παρατηρήσεις

- Έστω a, b ακέραιοι αριθμοί, όχι και οι δύο μηδέν. Οι αριθμοί s, t για τους οποίους $gcd(a, b) = as + bt$ δεν είναι μοναδικοί.
  Πράγματι, για κάθε $k \in \mathbb{Z}$ ισχύει ότι $\gcd(a, b) = as' + bt'$ όπου $s' = s + kb$ και $t' = t - ka$.
  Πράγματι
  $as' + bt' = a(s + kb) + b(t - ka) = a + bt + kab - kab = \gcd(a, b)$.
- Ο αριθμός $\gcd(a, b)$ είναι ο ελάχιστος θετικός αριθμός που εκφράζεται ως γραμμικός συνδυασμός των a, b με ακέραιους συντελεστές.
  Πράγματι, αν $d = \gcd(a, b)$ τότε κάθε θετικός $x = as + bt$ διαιρείται από το d άρα $d \leq x$.

ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ
2η ΔΙΑΛΕΞΗ

- **Γραμμικές διοφαντικές εξισώσεις**
- **Πρώτοι αριθμοί**

Γραμμικές διοφαντικές εξισώσεις

- Οι εξισώσεις στις οποίες αναζητούμε **λύσεις ακέραιους αριθμούς** (ή, και σε ορισμένες περιπτώσεις ρητούς) ονομάζονται **διοφαντικές εξισώσεις**.
  Παραδείγματα
  $5x + 17y + 32z = 20$, $x^2 + y^2 = 100$, $xyz = 500$, $x^n + y^n = z^n$, $n \geq 3$,
  $50x + 20y = 170$, $x - y + 90z = 5$, $2x + 4y = 9$, $69x + 39y = 15$, κ.ο.κ.
- Οι διοφαντικές εξισώσεις της μορφής

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

  όπου $a_1, a_2, \ldots, a_n$ είναι ακέραιοι ονομάζονται **γραμμικές διοφαντικές εξισώσεις**.
- Οι ακέραιοι που επαληθεύουν μια διοφαντική εξίσωση ονομάζονται **λύσεις της εξίσωσης**.
  Παραδείγματα
  Οι λύσεις της διοφαντικής εξίσωσης $69x + 39y = 15$ είναι τα ζεύγη της μορφής $(x, y) = (20 + 13\lambda, -35 - 23\lambda),$ όπου $\lambda \in \mathbb{Z}$.

Παρατήρηση. Έστω a, b, c τρεις ακέραιοι αριθμοί με $a \neq 0 \neq b$. Η γραμμική εξίσωση

$$ax + by = c$$

περιγράφει τα σημεία μιας ευθείας L του επιπέδου με συντεταγμένες (x, y). Η διοφαντική εξίσωση έχει λύση όταν η ευθεία L διέρχεται από σημεία με ακέραιες συντεταγμένες (x, y).

Τρεις ιδέες για την επίλυση της διοφαντικής εξίσωσης $ax + by = c$**.**

- Γνωρίζουμε ότι αν a, b είναι δύο φυσικοί αριθμοί, τότε μπορούμε να χρησιμοποιήσουμε τον επεκτεταμένο αλγόριθμο του Ευκλείδη προκειμένου να προσδιορίσουμε ακέραιους αριθμούς x_0, y_0 έτσι ώστε

$$ax_0 + by_0 = \gcd(a, b)$$

  δηλαδή το ζεύγος (x_0, y_0) είναι λύση της διοφαντικής εξίσωσης $ax + by = \gcd(a, b)$.

- Επιπλέον, για κάθε ακέραιο k ισχύει ότι

$$akx_0 + bky_0 = k \gcd(a, b)$$

  δηλαδή το ζεύγος (kx_0, ky_0) είναι λύση της διοφαντικής εξίσωσης $ax + by = k \gcd(a, b)$.

- Τέλος, για κάθε ακέραιο λ ισχύει ότι τα ζεύγη $(x_0 + \lambda b, y_0 - \lambda a)$ είναι επίσης λύσεις της εξίσωσης $ax + by = \gcd(a, b)$, αφού

$$a(x_0 + \lambda b) + b(y_0 - \lambda a) = ax_0 + by_0 = \gcd(a, b).$$

Παράδειγμα

Για την γραμμική διοφαντική εξίσωση

$$527x + 341y = 93$$

έχουμε $a = 527$, $b = 341$, $c = 93$.

- Από τον αλγόριθμο του Ευκλείδη υπολογίζουμε ότι $\gcd(341, 527) = 31$ και

  $$2 \cdot 527 - 3 \cdot 341 = 31$$

  δηλαδή το ζεύγος $(x_0, y_0) = (2, -3)$ είναι λύση της εξίσωσης $527x + 341y = 31$.

- Οπότε

  $$6 \cdot 527 - 9 \cdot 341 = 3 \cdot 31 = 93$$

  δηλαδή το ζεύγος $(x_0, y_0) = (6, -9)$ είναι λύση της εξίσωσης $527x + 341y = 93$.

- Συνεπώς, και τα ζεύγη $(x, y) = (6 + 341\lambda, -9 - 527\lambda)$, $\lambda \in \mathbb{Z}$, είναι επίσης λύσεις της εξίσωσης $527x + 341y = 93$. (**Προσοχή! Υπάρχουν και άλλες λύσεις στο παράδειγμα αυτό**)

Αυτές οι τρεις ιδέες συστηματοποιούνται στην επόμενη πρόταση.

Πρόταση 5 (Λύσεις γραμμικής διοφαντικής εξίσωσης)

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*

$$(x, y) = (x_0 + \lambda \frac{b}{\gcd(a, b)}, y_0 - \lambda \frac{a}{\gcd(a, b)}), \text{όπου } \lambda \in \mathbb{Z}.$$

Επιπρόσθετα, η (απλούστερη) εξίσωση

$$\frac{a}{\gcd(a, b)}x + \frac{b}{\gcd(a, b)}y = \frac{c}{\gcd(a, b)}$$

έχει τις ίδιες ακέραιες λύσεις.

Απόδειξη.

(**1ο μέρος: Ύπαρξη λύσης**). 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 λύση της εξίσωσης $ax + by = c$.

Άρα, η εξίσωση $ax + by = c$ έχει λύση αν και μόνο αν $\gcd(a, b) \mid c$.

(2ο μέρος: Μορφή λύσεων). 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.

Άσκηση 2

Η διοφαντική εξίσωση

$$12x + 27y = 2$$

δεν έχει λύση, διότι $\gcd(12, 27) = 3$ *και* $3 \nmid 2$.

Άσκηση 3

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 4

Η διοφαντική εξίσωση

$$69x + 39y = 15$$

έχει λύση, διότι $\gcd(69, 39) = 3$.

Λύση. 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

$$\begin{aligned} 1 &= 1 \cdot 10 + (-3) \cdot 3 = 1 \cdot 10 + (-3) \cdot (1 \cdot 13 + (-1) \cdot 10) \\ &= (-3) \cdot 13 + 4 \cdot 10 = (-3) \cdot 13 + 4 \cdot (1 \cdot 23 + (-1) \cdot 13) \\ &= 4 \cdot 23 + (-7) \cdot 13, \end{aligned}$$

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

$$(x, y) = (20 + 13\lambda, -35 - 23\lambda), \text{ όπου } \lambda \in \mathbb{Z}.$$

Άσκηση 5

Να δειχθεί ότι η εξίσωση $84x - 44y = 6$ δεν έχει ακέραιες λύσεις.

Λύση. Παρατηρούμε ότι
κάθε λύση (x, y) της εξίσωσης $84x + 44y = 6$
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 6

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

$$\sqrt{(15 + 7\lambda)^2 + (-40 - 19\lambda)^2} = \sqrt{410\lambda^2 + 1730\lambda + 1825}.$$

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 $\lambda = -1$ το σημείο $(8, 21)$ ικανοποιεί την εξίσωση της ευθείας και απέχει απόσταση $\sqrt{505}$ από την αρχή των αξόνων,
για $\lambda = -2$ το σημείο $(1, -2)$ ανήκει στην ευθεία και απέχει απόσταση $\sqrt{5}$ και
για $\lambda = -3$ 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 7

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:

$$30 = 7 \cdot 4 + 2$$

$$4 = 2 \cdot 2 + 2.$$

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

$(x, y, z) = (-189+45\lambda_2-17\lambda_1, 1386-330\lambda_2+125\lambda_1, 9-2\lambda_2)$ όπου $\lambda_1, \lambda_2 \in \mathbb{Z}$.

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 Möller von Königsberg[1]) (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).

[1] Πρόκειται για το Königsberg της Βαυαρίας και όχι για το πιο γνωστό Königsberg 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.

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.
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.

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 έως το 100, (συνολικά υπάρχουν 25 πρώτοι αριθμοί στο διάστημα 1 έως 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. Θα δούμε ορισμένα προκαταρκτικά αποτελέσματα σχετικά με τους πρώτους αριθμούς.

Πρόταση 6

Κάθε φυσικός αριθμός $n \geq 2$ είναι πρώτος, ή γινόμενο πρώτων αριθμών.

Άραγε υπάρχουν άπειροι πρώτοι αριθμοί; Η απάντηση είναι καταφατική. Ο Ευκλείδης στο βιβλίο του Στοιχεία δίνει την επόμενη πρόταση.

Πρόταση 7

Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.

Πρόταση 8 (**Λήμμα του Ευκλείδη**)

Έστω p πρώτος αριθμός και $a, b \in \mathbb{Z}$. Τότε

1. $p|a$ *ή* $\gcd(a, p) = 1$,
2. *Αν* $p|ab$, *τότε* $p|a$ *ή/και* $p|b$.

Απόδειξη:

1. 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, $p \mid a$ ή $\gcd(a, p) = 1$.
2. 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 $4 \nmid 10$.

Η προηγούμενη πρόταση είναι πολύ χρήσιμη σε συνδυασμό με την επόμενη.

Πρόταση 9

Έστω ακέραιοι a, b, c με $gcd(a, c) = 1$.
Αν $c|ab$, τότε $c|b$.

Πόρισμα 1

Έστω ακέραιοι a, b και p πρώτος αριθμός με $p \nmid a$.
Αν $p|ab$, τότε $p|b$.

Εφαρμογή 1

Έστω p πρώτος αριθμός. Να δειχθεί ότι για κάθε φυσικό αριθμό k με $1 < k < p$ ισχύει ότι $p \mid \binom{p}{k}$.

Λύση: Επειδή ο αριθμός $\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k!}$ είναι ακέραιος, έπεται ότι $k! \mid p(p-1)\cdots(p-k+1)$.

Όμως, επειδή $k < p$, έπεται ότι $\gcd(k!, p) = 1$.

Άρα, $k! \mid (p-1)\cdots(p-k+1)$, δηλαδή $\dfrac{(p-1)\cdots(p-k+1)}{k!} \in \mathbb{N}^*$.

Επομένως, $\binom{p}{k} = p \cdot \dfrac{(p-1)\cdots(p-k+1)}{k!}$.

Όπως φαίνεται στην επόμενη πρόταση οι πρώτοι αριθμοί μπορούν να θεωρηθούν ως οι ``δομικοί λίθοι'' των φυσικών αριθμών.

Πρόταση 10 (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).

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 $p_1, p_2, \ldots, p_k$ είναι πρώτοι αριθμοί (διαφορετικοί ανά δύο) και $a_1, a_2, \ldots, a_k$ 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.

ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ
3η ΔΙΑΛΕΞΗ

- **Ισοτιμίες**
- **Συνάρτηση φ του Euler**
- **Θεώρημα Euler - Fermat**

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 $\mathbf{a \equiv b \pmod{n}}$ 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

$$\begin{aligned}
15 &\equiv 10 \pmod{5} \text{ αφού ισχύει ότι } 5 \mid (15 - 10),\\
27 &\equiv 7 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (27 - 7),\\
7 &\equiv 27 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (7 - 27),\\
27 &\equiv 3 \pmod{3} \text{ αφού ισχύει ότι } 3 \mid (27 - 3),\\
7 &\equiv 3 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (7 - 3),\\
27 &\equiv -1 \pmod{4} \text{ αφού ισχύει ότι } 4 \mid (27 - (-1)),\\
21 &\equiv 0 \pmod{3} \text{ αφού ισχύει ότι } 3 \mid (21 - 0),\\
25 &\not\equiv 12 \pmod{7} \text{ αφού ισχύει ότι } 7 \nmid (25 - 12).
\end{aligned}$$

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 11

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 $n \big| (a - b)$, 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 ακέραιοι που είναι ισότιμοι με 1 modulo 10 είναι οι εξής:

$$x = \ldots, -29, -19, -9, 1, 11, 21, 31, \ldots.$$

Πρόταση 12

Η σχέση ισοτιμίας $\mathrm{mod}\, n$ *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

- Με τη βοήθεια της σχέσης ισοτιμίας modulo n, όλοι οι ακέραιοι αριθμοί μπορούν να διαμεριστούν σε κλάσεις οι οποίες ονομάζονται **κλάσεις υπολοίπων** $\mathrm{mod}\, n$. 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 $\overline{a}$ ή με $[a]_n$.

- Κάθε ακέραιος αριθμός είναι ισοϋπόλοιπος $\bmod n$ με έναν ακριβώς από τους αριθμούς: $0, 1, 2, \ldots, n-1$. Επομένως το σύνολο των ακεραίων χωρίζεται σε n κλάσεις $\bmod n$ τέτοιες ώστε:

$$\begin{aligned}
\overline{0} &= \{\ldots, -2\cdot n, -n,\ 0,\ n,\ 2\cdot n,\ \ldots\},\\
\overline{1} &= \{\ldots, -2\cdot n+1, -n+1,\ 1,\ n+1,\ 2\cdot n+1,\ \ldots\},\\
\overline{2} &= \{\ldots, -2\cdot n+2, -n+2,\ 2,\ n+2,\ 2\cdot n+2,\ \ldots\},\\
&\vdots\\
\overline{n-1} &= \{\ldots, -n-1,\ -1,\ n-1,\ 2\cdot n-1,\ 3\cdot n-1,\ \ldots\}.
\end{aligned}$$

Άρα

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}\\
&= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}.
\end{aligned}$$

Με $\mathbb{Z}_n$ συμβολίζουμε το **σύνολο κλάσεων** modulo n

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Οι βασικές ιδιότητες της ισοτιμίας modulo n δίνονται στην επόμενη πρόταση.

Πρόταση 13

Αν n είναι ένας σταθερός φυσικός αριθμός και a, b, c, d ακέραιοι, τότε:

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 ιδιοτήτων των ισοτιμιών

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 2

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 3

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 4

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

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.

Η συνάρτηση ϕ του Euler

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 $\text{ΜΚΔ}(n, m) = 1$, δηλαδή τα n και m είναι σχετικά πρώτοι μεταξύ τους.

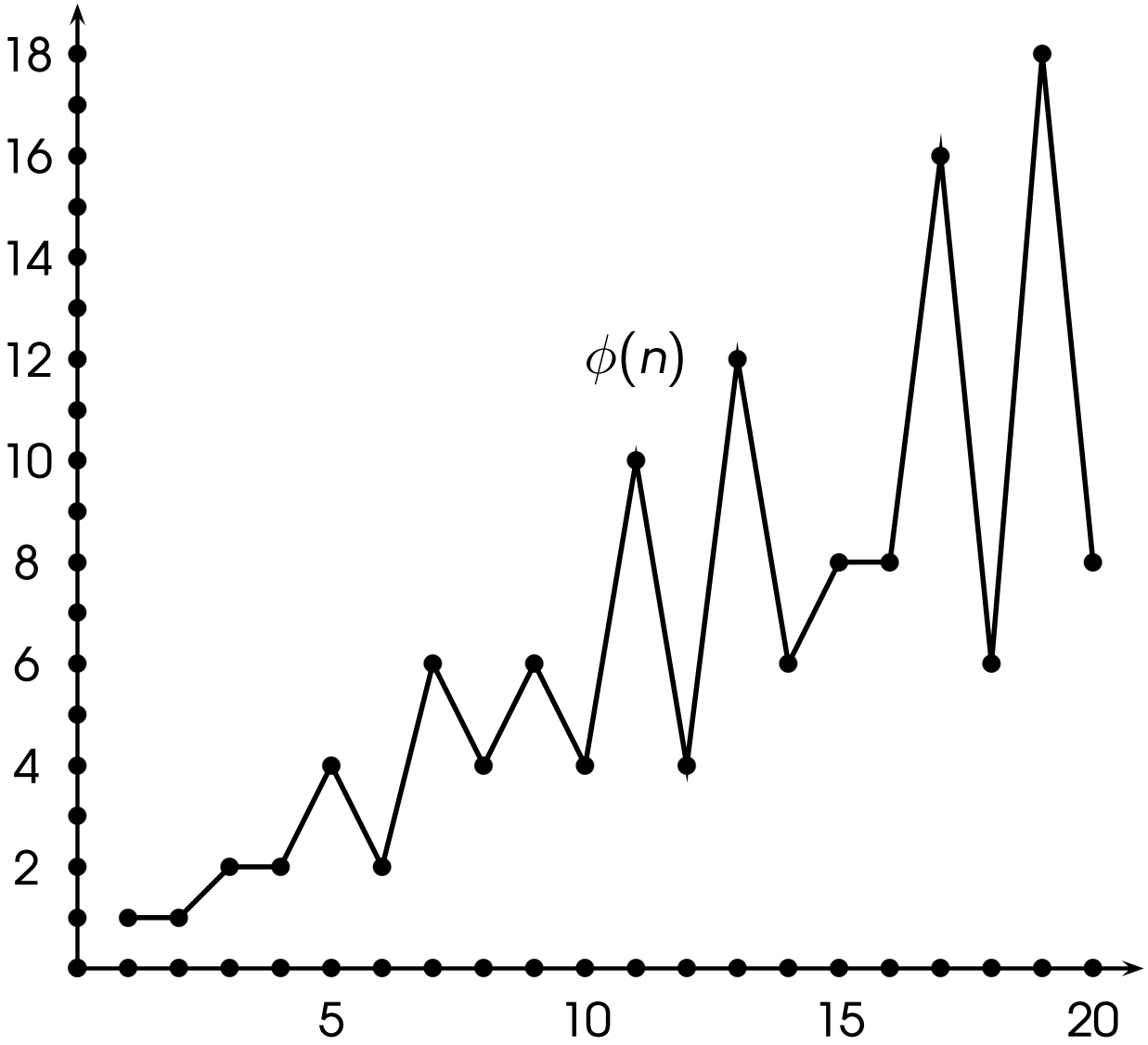
Για παράδειγμα, $\phi(12) = 4$, διότι από τους αριθμούς

$$1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6, \quad 7, \quad 8, \quad 9, \quad 10, \quad 11, \quad 12$$

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 $\text{ΜΚΔ}(12, 8) = 4$).

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



Ερώτημα: Υπάρχει τύπος για την συνάρτηση $\phi(n)$;

Η απάντηση είναι καταφατική.

Πρόταση 14

Αν p είναι πρώτος αριθμός και $k \in \mathbb{N}^*$. Τότε $\phi(p^k) = p^k - p^{k-1}$.
Αν m, n φυσικοί αριθμοί με ΜΚΔ$(m, n) = 1$. Τότε $\phi(mn) = \phi(m)\phi(n)$.

Από την προηγούμενη πρόταση άμεσα προκύπτει μια έκφραση για τον υπολογισμό της τιμής $\phi(n)$ όταν γνωρίζουμε την κανονική παραγοντοποίηση του n.

Πρόταση 15

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

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

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.

Να βρεθούν οι παρακάτω τιμές του $\phi(n)$.

- $\phi(31) = 31^1 - 30^0 = 30$. (Ο 31 είναι πρώτος αριθμός)
- $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100$.
- $\phi(55) = \phi(5 \cdot 11) = (5^1 - 5^0)(11^1 - 11^0) = 40$.
- $\phi(7!) = \phi(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7) = \phi(2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7) = \phi(2^4 \cdot 3^2 \cdot 5 \cdot 7) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0) = 8 \cdot 6 \cdot 4 \cdot 6 = 192$.
- $\phi(30^m) = \phi((2 \cdot 3 \cdot 5)^m) = \phi(2^m \cdot 3^m \cdot 5^m) = (2^m - 2^{m-1})(3^m - 3^{m-1})(5^m - 5^{m-1})$.
- $\phi(10^m \cdot 20^n) = \phi(2^m \cdot 5^m \cdot (2^2)^n \cdot 5^n) = \phi(2^{m+2n} 5^{m+n}) = (2^{m+2n} - 2^{m+2n-1})(5^{m+n} - 5^{m+n-1})$.

Θεώρημα Euler-Fermat

Πρόταση 16 (Θεώρημα του Euler)

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

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

Με τη βοήθεια του θεωρήματος του Euler προκύπτει η επόμενη πρόταση.

Πρόταση 17 (Μικρό θεώρημα του Fermat)

Αν p είναι πρώτος αριθμός και n φυσικός αριθμός, τότε

$$n^p \equiv n \pmod{p}.$$

Εφαρμογή 6

Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση

$$3^{1000} \equiv x \pmod{41}.$$

Λύση. Επειδή $\text{ΜΚΔ}(41, 3) = 1$, έπεται ότι

$$3^{\phi(41)} = 1 \pmod{41}.$$

Ο 41 είναι πρώτος, οπότε $\phi(41) = 41 - 1 = 40$.
Επομένως, $3^{40} \equiv 1 \pmod{41}$, οπότε

$$3^{1000} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1 \pmod{41}.$$

Εφαρμογή 7

Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση

$$x \equiv 18^{51} \pmod{30}$$

Λύση. Επειδή ΜΚΔ$(18, 30) = 6 \neq 1$. Δεν μπορεί να εφαρμοσθεί το θεώρημα του Euler. Πρέπει να χρησιμοποιήσουμε τις γενικές ιδιότητες των ισοτιμιών.

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

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,

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

Άρα, $x = 12$.

Εφαρμογή 8

Να ευρεθεί ο ελάχιστος φυσικός αριθμός που ικανοποιεί την εξίσωση

$$x \equiv 31^{30} \pmod{100}$$

Λύση. Επειδή ΜΚΔ$(100, 31) = 1$ 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 ισοτιμιών.

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

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

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

Άρα $x = 1$.

Εφαρμογή 9

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

Λύση. Αρκεί να δειχθεί ότι $2^{70} + 3^{30} \equiv 0 \pmod{13}$. Επειδή $\text{ΜΚΔ}(13, 2) = \text{ΜΚΔ}(13, 3) = 1$ και $\phi(13) = 12$ έπεται ότι $2^{12} \equiv 1 \pmod{13}$ και $3^{12} \equiv 1 \pmod{13}$. Επομένως,

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

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,

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

Εφαρμογή 10

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 11

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.

ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ
4η ΔΙΑΛΕΞΗ

- **Αντιστροφή modulo** n
- **Κινέζικο θεώρημα υπολοίπων**

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, για όλα τα n. Πράγματι, αν $n = 10$, τότε $4k \not\equiv 1 \pmod{10}$ για κάθε $k \in \mathbb{Z}$.
- 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 18 (Αντιστροφή modulo n)

Έστω a, n δύο ακέραιοι αριθμοί με $n \geq 2$.

- *Ο a έχει αντίστροφο modulo n αν και μόνο αν $\gcd(a, n) = 1$.*
- *Επιπλέον, αν s, t είναι ακέραιοι ώστε $as + tn = 1$ τότε ο s είναι ένας αντίστροφος του a modulo n.*
- *Επιπρόσθετα, $s = \pi n + \upsilon$, όπου $0 < \upsilon < n$ τότε ο υ είναι ο μοναδικός αντίστροφος του a modulo n στο διάστημα $[n - 1]$.*

Απόδειξη.

(**1ο μέρος: Ύπαρξη αντίστροφου**). Έστω ότι $\gcd(a, n) = 1$. Με βάση τον επεκταμένο αλγόριθμο του Ευκλείδη 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 $n(pa + t) = \pi na + tn = 1$ 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 $v \in [n-1]$ τέτοιο ώστε

$$av \equiv 1 \pmod{n},$$

οπότε υπάρχει ακέραιος αριθμός k ώστε

$$av = 1 + kn$$

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.

(**2ο μέρος: Μοναδικότητα αντίστροφου**). 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 1

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.

$$\begin{aligned} 18 &= 2 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1, \end{aligned}$$

έπειτα λύνουμε τις ισότητες ως προς τα υπόλοιπα κάθε διαίρεσης

$$\begin{aligned} 1 &= 1 \cdot 4 + (-1) \cdot 3 \\ 3 &= 1 \cdot 7 + (-1) \cdot 4 \\ 4 &= 1 \cdot 18 + (-2) \cdot 7, \end{aligned}$$

και στη συνέχεια κάνουμε διαδοχικές αντικαταστάσεις των πηλίκων και υπολοίπων, όπως παρακάτω:

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) = -1 \cdot 7 + 2 \cdot 4 \\ &= -1 \cdot 7 + 2 \cdot (18 - 2 \cdot 7) \\ &= -5 \cdot 7 + 2 \cdot 18 \end{aligned}$$

Επειδή $-5 = (-1) \cdot 18 + 13$ όπου $0 < 13 < 18$ έπεται ότι ο αντίστροφος του 7 modulo 18 είναι το 13.
Πράγματι, $7 \cdot 13 = 91$ και $91 \equiv 1 \mod 18$, 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 2

Να λυθεί η εξίσωση $7x \equiv 5 \mod 18$.

Λύση. Στο προηγούμενο παράδειγμα, υπολογίσαμε ότι ο αντίστροφος του 7 modulo 18 είναι το 13, δηλαδή $7 \cdot 13 \equiv 1 \mod 18$.
Πολλαπλασιάζοντας την εξίσωση κατά μέλη με το 13 έχουμε ισοδύναμα[2] ότι

$$x \equiv 5 \cdot 13 \equiv 65 \equiv 11 \mod 18.$$

Άρα, οι λύσεις της εξίσωσης είναι όλα τα $x = 11 + 18k$, $k \in \mathbb{Z}$.

[2] Αν $\gcd(c, n) = 1$ τότε $a \equiv b \pmod{n} \Leftrightarrow ac \equiv bc \pmod{n}$

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 3

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

$$100 = 14 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$

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:

$$x \equiv 7^{38} \equiv (7^2)^{19} \equiv 49^{19} \equiv 49 \cdot 49^{18} \equiv 49 \cdot (49^2)^9 \equiv 49 \cdot (2401)^9$$
$$\equiv 49 \cdot 1^9 \equiv 49 \bmod 100.$$

Το σύστημα κρυπτογράφησης RSA

Το σύστημα κρυπτογράφησης RSA επινοήθηκε το 1976 από τους Ronald **R**ivest, Adi **S**hamir και Leonard **A**dleman και 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.

Το κινέζικο θεώρημα υπολοίπων

Πρόταση 19 (**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

$$x = \frac{n}{n_1} b_1 a_1 + \frac{n}{n_2} b_2 a_2 + \cdots + \frac{n}{n_k} b_k a_k \pmod{n_1 \cdot n_2 \cdots n_k}.$$

Εφαρμογή 12

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

$$x \equiv 2 \mod 3$$
$$x \equiv 3 \mod 5$$
$$x \equiv 4 \mod 7.$$

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 $35 \equiv 2 \pmod 3$, $21 \equiv 1 \pmod 5$ και $15 \equiv 1 \pmod 7$, 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.

Παρατήρηση. Στην περίπτωση όπου τα $n_1, n_2, \ldots, n_k$ δεν είναι ανά δύο σχετικά πρώτοι μεταξύ τους, το σύστημα δεν έχει πάντα λύση. Στην περίπτωση που έχει λύση, η εύρεση της λύσης γίνεται όπως στο επόμενο παράδειγμα:

Παράδειγμα

Να λυθεί το σύστημα:

$$x \equiv a_1 \mod n_1$$
$$x \equiv a_2 \mod n_2$$

Ισοδύναμα έχουμε ότι υπάρχουν ακέραιοι k_1, k_2 ώστε

$$x = a_1 + k_1 n_1$$
$$x = a_2 + k_2 n_2$$

οπότε πρέπει

$$a_1 - a_2 = k_1 n_1 - k_2 n_2 \tag{1}$$

Η εξίσωση (1) έχει λύση αν ο $\gcd(n_1, n_2)$ διαιρεί το $a_1 - a_2$.

Στην περίπτωση αυτή βρίσκουμε κατά τα γνωστά τα k_1 , k_2 της εξίσωσης (1) οπότε $x = a_1 + k_1 n_1$.

Έστω s η (μοναδική) λύση modulo $\dfrac{n_1 n_2}{\gcd(n_1, n_2)}$ τότε οι δύο εξισώσεις γίνονται μια εξίσωση

$$x \equiv s \pmod{\frac{n_1 n_2}{\gcd(n_1, n_2)}}$$

Με τον τρόπο αυτό αν το σύστημα έχει πάνω από 2 εξισώσεις συγχωνεύουμε ανά δύο τις εξισώσεις με την παραπάνω μέθοδο, μέχρις ότου να καταλήξουμε σε μια εξίσωση που αποτελεί την λύση του συστήματος των ισοτιμιών.