Θεμέλια των Μαθηματικών

Ελένη Τζανάκη & Θεόδουλος Γαρεφαλάκης

Εαρινο εξάμηνο 2019-20

Άσκηση 1

1. 53 δια 7, -53 δια 7, -53 δια -7, 53 δια -7.
2. 92 δια 4, -92 δια 4, -92 δια -4, 92 δια -4.

- $53 = 7 \cdot 7 + 4$
- $-53 = (-7) \cdot 7 - 4 = (-7) \cdot 7 - 7 + 7 - 4 = (-8) \cdot 7 + 3$
- $-53 = 7 \cdot (-7) - 4 = 7 \cdot (-7) - 7 + 7 - 4 = 8 \cdot (-7) + 3$
- $53 = 7 \cdot 7 + 4 = (-7) \cdot (-7) + 4$

- $92 = 23 \cdot 4$
- $-92 = (-23) \cdot 4$
- $-92 = 23 \cdot (-4)$
- $92 = (-23) \cdot (-4)$

Άσκηση 2

Έστω p πρώτος αριθμός και $a_1, \ldots, a_n \in \mathbb{Z}$. Αποδείξτε με επαγωγή στο n, ότι αν $p \mid a_1 \cdots a_n$ τότε $p \mid a_i$ για κάποιο $1 \leq i \leq n$.

Με επαγωγή στο πλήθος n των αριθμών.

- Βάση: Για $n = 1$, αν $p \mid a_1$ τότε $p \mid a_1$.
  Ισχύει και για $n = 2$: $p \mid a_1 a_2 \implies p \mid a_1$ ή $p \mid a_2$.
- Επαγωγική Υπόθεση: Αν $p \mid a_1 \cdots a_n$, τότε $p \mid a_i$ για κάποιο $1 \leq i \leq n$.
- Επαγωγικό Βήμα: Έστω $a_1, \ldots, a_{n+1} \in \mathbb{Z}$ και $p \mid a_1 \cdots a_{n+1}$.
  Θα δείξουμε ότι $p \mid a_i$ για κάποιο $1 \leq i \leq n+1$.
    - $p \mid (a_1 \cdots a_n) \cdot a_{n+1}$ άρα $p \mid a_1 \cdots a_n$ ή $p \mid a_{n+1}$.
    - Από Ε.Υ. $p \mid a_i$ για κάποιο $1 \leq i \leq n$ ή $p \mid a_{n+1}$.
    - Δηλαδή $p \mid a_i$ για κάποιο $1 \leq i \leq n+1$.

Άσκηση 3

Έστω $a, b \in \mathbb{Z}$. Εάν $a \mid b$, δείξτε ότι $(a, b) = |a|$.

- $|a| = a$ ή $|a| = -a$, άρα $|a| \mid a$.
- $|a| \mid a$ και $a \mid b$, άρα $|a| \mid b$.
- Έστω $d \mid a$ και $d \mid b$.
- Όμως $a \mid |a|$, οπότε $d \mid |a|$.

Καθώς $|a| \in \mathbb{N}$, έχουμε $(a, b) = |a|$.

Άσκηση 4

Δείξτε ότι αν $m, n, s \in \mathbb{N}$ και $m \mid s$, $n \mid s$ και $(m, n) = 1$,τότε $mn \mid s$.

Από τα δεδομένα:

$$\begin{aligned} m \mid s \quad &\Longrightarrow \quad s = am, \quad a \in \mathbb{Z} \\ n \mid s \quad &\Longrightarrow \quad s = bn, \quad b \in \mathbb{Z} \end{aligned}$$

- Άρα $am = bn$,
- οπότε $m \mid bn$.
- Όμως $(m, n) = 1$,
- άρα $m \mid b \implies b = cm, \quad c \in \mathbb{Z}$.
- Άρα $s = bn = cmn \implies mn \mid s$.

Άσκηση 5

Έστω $n, m \in \mathbb{Z}$. Εάν $(n, m) = 1$, αποδείξτε ότι $(m + n, mn) = 1$.

Άς υποθέσω ότι $(m + n, mn) > 1$. Τότε θα υπάρχει πρώτος $p \mid (m + n, mn)$.

- $p \mid mn$ άρα $p \mid m$ ή $p \mid n$. Ας υποθέσω ότι $p \mid m$.
- $p \mid m$ και $p \mid m + n$, άρα $p \mid n$.
- Τότε όμως $p \mid (n, m)$, δηλαδή $p \mid 1$, άτοπο!

Άσκηση 6

Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $(3n+1, 10n+3) = 1$.

Χρησιμοποιούμε το Λήμμα: $(a, b) = (a - qb, b)$, για κάθε $q \in \mathbb{Z}$.

$$
\begin{aligned}
(10n+3, 3n+1) &= (10n+3-3(3n+1), 3n+1) \\
&= (n, 3n+1) \\
&= (n, 3n+1-3n) \\
&= (n, 1) \\
&= 1.
\end{aligned}
$$

Άσκηση 7

Με χρήση του Ευκλείδιου αλγόριθμου:

1. Βρείτε όλους τους κοινούς διαιρέτες των 252 και 180.
2. Βρείτε $s, t \in \mathbb{Z}$ τέτοιους ώστε $252s + 180t = (252, 180)$.

Εφαρμόζω τον Ευκλείδιο αλγόριθμο στα 252 και 180:

$$\begin{aligned} 252 &= 180 + 72 \\ 180 &= 2 \cdot 72 + 36 \\ 72 &= 2 \cdot 36 \end{aligned}$$

Οι κοινοί διαιρέτες των 252 και 180 είναι ακριβώς οι διαιρέτες του $(252, 180) = 36$.
Οι θετικοί διαιρέτες είναι οι $1, 3, 9, 2, 6, 18, 4, 12, 36$.
Υπολογίζω τα s, t:

$$\begin{aligned} 36 &= 180 - 2 \cdot 72 \\ &= 180 - 2 \cdot (252 - 180) \\ &= (-2) \cdot 252 + 3 \cdot 180. \end{aligned}$$

Άσκηση 8

Έστω $a, b \in \mathbb{N}$. Εάν $(a, b) = 1$ και το γινόμενο ab είναι τετράγωνο ακεραίου, δείξτε ότι οι a, b είναι επίσης τεράγωνα ακεραίων.

Θα χρειαστεί να περιγράψουμε την ανάλυση σε πρώτους παράγοντες των τετραγώνων των ακεραίων.

Λήμμα

Έστω $a = p_1^{a_1} \cdots p_s^{a_s}$, με p_i διακεκριμένους πρώτους και $a_i \geq 1$. Ο a είναι τετράγωνο κάποιου ακεραίου αν και μόνο αν όλοι οι a_i είναι άρτιοι.

Έστω $a = c^2$, με $c \in \mathbb{N}$.

- Κάθε πρώτος που διαιρεί τον c, διαιρεί και τον a,
- άρα $c = p_1^{c_1} \cdots p_s^{c_s}$, $c_i \geq 0$.
- Άρα $a = p_1^{a_1} \cdots p_s^{a_s} = p_1^{2c_1} \cdots p_s^{2c_s}$.
- Από μοναδικότητα της ανάλυσης, $a_i = 2c_i$, για $1 \leq i \leq s$.

Αντίστροφα, εάν $a = p_1^{2c_1} \cdots p_s^{2c_s} = \left(p_1^{c_1} \cdots p_s^{c_s}\right)^2$.

Άσκηση 8

Έστω $a, b \in \mathbb{N}$. Εάν $(a, b) = 1$ και το γινόμενο ab είναι τετράγωνο ακεραίου, δείξτε ότι οι a, b είναι επίσης τεράγωνα ακεραίων.

Η περίπτωση που $a = 1$ ή $b = 1$ είναι προφανής. Υποθέτω ότι $a > 1$ και $b > 1$.

- $a = p_1^{a_1} \cdots p_s^{a_s}$, με p_i πρώτους, $a_i \geq 1$.
- $b = q_1^{b_1} \cdots q_t^{b_t}$, με q_j πρώτους, $b_j \geq 1$.
- $p_i \neq q_j$ για κάθε $1 \leq i \leq s$, $1 \leq j \leq t$, διότι $(a, b) = 1$.
- Οπότε $ab = p_1^{a_1} \cdots p_s^{a_s} q_1^{b_1} \cdots q_t^{b_t}$ είναι η κανονική ανάλυση του ab σε πρώτους παράγοντες.
- Άρα a_i και b_j είναι όλοι άρτιοι...

Χωρίς την υπόθεση $(a, b) = 1$, το συμπέρασμα *δεν ισχύει*.
Μπορείτε να δώσετε ένα αντιπαράδειγμα;

Άσκηση 9

Αν $(a, b) = 1$ ποιές είναι οι δυνατές τιμές για τον μέγιστο κοινό διαιρέτη

1. $(a + b, a - b)$,
2. $(a^2 + b^2, a + b)$.

Έστω $d = (a + b, a - b)$.

- $d \mid a + b$ και $d \mid a - b$
- $d \mid 2a$ και $d \mid 2b$
- $d \mid (2a, 2b) \implies d \mid 2(a, b) \implies d \mid 2$
- Άρα $d \in \{1, 2\}$. Και οι δύο τιμές είναι δυνατές...

Μία δυνατότητα είναι $(a^2 + b^2, a + b) = 1$. Για παράδειγμα, για $a = 2$ και $b = 3$.
Εάν $(a^2 + b^2, a + b) > 1$, έστω p ένας πρώτος διαιρέτης του $(a^2 + b^2, a + b)$.

- $p \mid a^2 + b^2$ και $p \mid a + b$
- $p \mid a + b \implies p \mid a^2 + 2ab + b^2$
- $p \mid a^2 + 2ab + b^2$ και $p \mid a^2 + b^2$, άρα $p \mid 2ab \implies p = 2$ ή $p \mid a$ ή $p \mid b$
- Αν $p \mid a$, τότε $p \mid b$, άτοπο! Όμοια αν $p \mid b$...
- Άρα $p = 2$. Η τιμή αυτή είναι επίσης δυνατή. Για παράδειγμα, $a = 1$ και $b = 1$.

Άσκηση 10

Έστω πρώτος αριθμός p και φυσικοί αριθμοί q, n. Εάν $p \mid q^n$ δείξτε ότι $p^n \mid q^n$.

- $p \mid q^n \implies p \mid q$
- $q = cp$ με $c \in \mathbb{N}$
- $q^n = (cp)^n = c^n p^n$
- Άρα $p^n \mid q^n$

Το συμπέρασμα *δεν* ισχύει εάν ο p δεν είναι πρώτος.
Μπορείτε να βρείτε ένα αντιπαράδειγμα;