ΔΙΑΙΡΕΤΟΤΗΤΑ

Ορισμός 1: Έστω $d,n\in\mathbb{Z}$. Λέμε ότι ο d διαιρεί τον n (συμβολισμός: $d|n$) αν υπάρχει $c\in\mathbb{Z}$ τέτοιο ώστε $n=cd$. □

Θεώρημα 2: Για $d,n,m,\alpha,b\in\mathbb{Z}$ ισχύουν:

i) $n|n$, $-n|n$ (άρα $|n|\|n$)

ii) $1|n$, $-1|n$

iii) $n|0$

iv) $0|n\Rightarrow n=0$

v) $\left.\begin{matrix}d|n\\ n|m\end{matrix}\right\}\Rightarrow d|m$

vi) $\left.\begin{matrix}d|n\\ d|m\end{matrix}\right\}\Rightarrow d|(\alpha n+bm)$

vii) $d|n\Rightarrow d|\alpha n$ (άρα $d||n|$)

viii) $d|n\Rightarrow \alpha d|\alpha n$

ix) $\left.\begin{matrix}\alpha d|\alpha n\\ \alpha\neq 0\end{matrix}\right\}\Rightarrow d|n$

x) $\left.\begin{matrix}d|n\\ n\neq 0\end{matrix}\right\}\Rightarrow |d|\leq|n|$

xi) $\left.\begin{matrix}d|n\\ n|d\end{matrix}\right\}\Rightarrow |d|=|n|$

xii) $\left.\begin{array}{l} d \mid n \\ d \neq 0 \end{array}\right\} \Rightarrow \frac{n}{d} \mid n$

Απόδειξη:

i) $n = 1 \cdot n \Rightarrow n \mid n$.

$n = -1 \cdot (-n) \Rightarrow -n \mid n$.

ii) $n = n \cdot 1 \Rightarrow 1 \mid n$.

$n = -n \cdot (-1) \Rightarrow -1 \mid n$.

iii) $0 = 0 \cdot n \Rightarrow n \mid 0$.

iv) $0 \mid n \Rightarrow n = \kappa \cdot 0,\ \kappa \in \mathbb{Z}$. Άρα $n = 0$.

v) $d \mid n \Rightarrow n = \lambda d,\ \lambda \in \mathbb{Z}$.

$n \mid m \Rightarrow m = \kappa n,\ \kappa \in \mathbb{Z}$.

Άρα $m = \kappa n = (\kappa\lambda) d,\ \kappa\lambda \in \mathbb{Z}$. Συνεπώς $d \mid m$.

vi) $d \mid n \Rightarrow n = \lambda d,\ \lambda \in \mathbb{Z}$.

$d \mid m \Rightarrow m = \kappa d,\ \kappa \in \mathbb{Z}$.

Άρα $\alpha n + bm = \alpha\lambda d + b\kappa d = (\alpha\lambda + b\kappa) d,\ \alpha\lambda + b\kappa \in \mathbb{Z}$. Συνεπώς $d \mid (\alpha n + bm)$.

vii) $d \mid n \Rightarrow n = \lambda d,\ \lambda \in \mathbb{Z}$.

Άρα $\alpha n = (\alpha\lambda) d,\ \alpha\lambda \in \mathbb{Z}$. Συνεπώς $d \mid \alpha n$.

viii) $d \mid n \Rightarrow n = \lambda d,\ \lambda \in \mathbb{Z}$.

Άρα $\alpha n = \alpha\lambda d = \lambda(\alpha d),\ \lambda \in \mathbb{Z}$. Συνεπώς $\alpha d \mid \alpha n$.

ix) $\alpha d \mid \alpha n \Rightarrow \alpha n = \lambda(\alpha d)$, $\lambda \in \mathbb{Z}$.

Άρα $\alpha n = \lambda(\alpha d) = \alpha(\lambda d) \underset{(\alpha \neq 0)}{\Rightarrow} n = \lambda d$. Συνεπώς $d \mid n$.

x) $d \mid n \Rightarrow n = \lambda d$, $\lambda \in \mathbb{Z}$.

Άρα $|n| = |\lambda||d|$. Επίσης $n \neq 0$. Άρα $\lambda \neq 0$ και επομένως $|\lambda| \geq 1$. Συνεπώς

$$|n| = |\lambda||d| \geq |d| \Rightarrow |d| \leq |n|$$

xi) A) Αν $n = 0$, τότε λόγω της σχέσης $n \mid d$ έχουμε αμέσως (βλ. **iv)**) ότι $d = 0$. Άρα $|d| = |n| = 0$.

B) Αν $n \neq 0$, τότε λόγω της σχέσης $d \mid n$ έχουμε αμέσως (βλ. **iv)**) ότι $d \neq 0$. Επομένως:

$$\left.\begin{array}{l} d \mid n \underset{x)}{\Rightarrow} |d| \leq |n| \\ n \mid d \underset{x)}{\Rightarrow} |n| \leq |d| \end{array}\right\} \Rightarrow |d| = |n|$$

Από **A)**, **B)** έπεται αμέσως ότι $|d| = |n|$.

xii) $d \mid n \Rightarrow n = \lambda d$, $\lambda \in \mathbb{Z}$.

Άρα $\lambda = \frac{n}{d} \in \mathbb{Z}$ και επομένως $n = \frac{n}{d} d$, $d \in \mathbb{Z}$. Συνεπώς $\frac{n}{d} \mid n$. □

<u>Ορισμός 3:</u> Έστω $n \in \mathbb{Z}$. Τότε ορίζουμε

$$\Delta_n := \{d \in \mathbb{Z} / d \mid n\}$$

(δηλ. το Δ_n είναι το σύνολο των διαιρετών του n). □

<u>Παρατήρηση 4:</u>

i) Από το **vii)** του Θεωρήματος 2 έπεται αμέσως ότι $\Delta_n = \Delta_{-n}$

ii) Από τα **i), ii)** του Θεωρήματος 2 έπεται αμέσως ότι για κάθε $n \in \mathbb{Z}$ έχουμε ότι

$$-n, n, -1, 1 \in \Delta_n$$

iii) Από τα **iii), iv)** του Θεωρήματος 2 έχουμε αμέσως ότι

$$0 \in \Delta_n \Leftrightarrow n = 0$$

iv) Από το **iii)** του Θεωρήματος 3 έχουμε αμέσως ότι $\Delta_0 = \mathbb{Z}$.

v) Από τα **x), iv)** του Θεωρήματος 3 έπεται αμέσως ότι για κάθε $n \in \mathbb{Z}^*$ έχουμε

$$\Delta_n \subseteq \{-|n|, -|n|+1, ..., -1, 1, ..., |n|, |n|+1\}$$

(άρα για $n \in \mathbb{Z}^*$ το σύνολο Δ_n είναι πεπερασμένο). □

<u>Ορισμός 5:</u> Έστω $\alpha, b \in \mathbb{Z}$. Τότε ως μέγιστο κοινό διαιρέτη των α, b (<u>συμβολισμός:</u> (α, b)) ορίζουμε το

$$(\alpha, b) := \begin{cases} \max(\Delta_\alpha \cap \Delta_b), & \text{αν } \alpha \in \mathbb{Z}^* \text{ ή } b \in \mathbb{Z}^* \\ 0, & \text{αν } \alpha = b = 0 \end{cases}$$ □

<u>Παρατήρηση 6:</u> Για κάθε $\alpha, b \in \mathbb{Z}$ έχουμε ότι $(\alpha, b) \in \Delta_\alpha \cap \Delta_b$. □

<u>Θεώρημα 7 (ταυτότητα Ευκλείδειας Διαίρεσης):</u> Έστω $\alpha, b \in \mathbb{Z}$ με $b \neq 0$. Τότε υπάρχουν <u>μοναδικά</u> $q, r \in \mathbb{Z}$ τέτοια ώστε $\alpha = qb + r$, $0 \leq r < |b|$ □

<u>Θεώρημα 8:</u> Έστω $\alpha, b \in \mathbb{Z}$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε

$$(\alpha, b) = \alpha x + by$$ □

<u>Θεώρημα 9:</u> Έστω $\alpha, b, d \in \mathbb{Z}$. Τα εξής είναι ισοδύναμα:

i) $d = (\alpha, b)$

ii) Ο d έχει τις ιδιότητες:

A) $d \geq 0$

B) $d \in \Delta_\alpha \cap \Delta_b$ (δηλ. $d \mid \alpha$ και $d \mid b$).

Γ) $\Delta_\alpha \cap \Delta_b \subseteq \Delta_d$ (δηλ. αν $e \in \mathbb{Z}$ με $e \mid \alpha$ και $e \mid b$ τότε $e \mid d$).

<u>Απόδειξη:</u>

i) $\Rightarrow$ **ii)** Έστω $d = (\alpha, b)$.

A) I) Αν $\alpha \in \mathbb{Z}^*$ ή $b \in \mathbb{Z}^*$ τότε $(\alpha, b) = \max(\Delta_\alpha \cap \Delta_b)$. Όμως $1 \in \Delta_\alpha \cap \Delta_b$ (βλ. το **i)** της Παρατήρησης 4). Άρα $(\alpha, b) \geq 1$. Συνεπώς $(\alpha, b) > 0$. Επομένως $d > 0$.

II) Αν $\alpha = b = 0$ τότε $(\alpha, b) = 0$. Άρα $d = 0$.

Από **I)** και **II)** έπεται αμέσως ότι $d \geq 0$.

B) I) Αν $\alpha \in \mathbb{Z}^*$ ή $b \in \mathbb{Z}^*$ τότε $(\alpha, b) = \max(\Delta_\alpha \cap \Delta_b)$. Δηλ. $d = \max(\Delta_\alpha \cap \Delta_b)$ και άρα $d \in \Delta_\alpha \cap \Delta_b$ (άμεσο αφού προφανώς $\max(\Delta_\alpha \cap \Delta_b) \in \Delta_\alpha \cap \Delta_b$).

II) Αν $\alpha = b = 0$ τότε $(\alpha, b) = 0$. Δηλ. $d = 0$. Επίσης αφού $\alpha = b = 0$ τότε $\Delta_\alpha = \Delta_b = \mathbb{Z}$ ((βλ. το **ii)** της Παρατήρησης 4). Άρα $\Delta_\alpha \cap \Delta_b = \mathbb{Z}$. Επομένως $d \in \Delta_\alpha \cap \Delta_b$.

Από **I)** και **II)** έπεται αμέσως ότι $d \in \Delta_\alpha \cap \Delta_b$.

Γ) Αφού $d = (\alpha, b)$, τότε από το Θεώρημα 8 έχουμε αμέσως ότι υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $d = \alpha x + by$.

Έστω τώρα $e \in \Delta_\alpha \cap \Delta_b$. Θα δείξουμε ότι $e \in \Delta_d$. <u>Πράγματι:</u>

Αφού $e \in \Delta_\alpha \cap \Delta_b$ τότε $e|\alpha$ και $e|b$. Τότε από το **vi)** του Θεωρήματος 2 έχουμε αμέσως ότι $e|(\alpha x + by)$. Δηλ. $e|d$. Άρα $e \in \Delta_d$. Συνεπώς $\Delta_\alpha \cap \Delta_b \subseteq \Delta_d$.

ii) $\Rightarrow$ **i)**

A) Έστω $\alpha \in \mathbb{Z}^*$ ή $b \in \mathbb{Z}^*$. Τότε $(\alpha, b) = \max(\Delta_\alpha \cap \Delta_b)$. Άρα $(\alpha, b) \in \Delta_\alpha \cap \Delta_b$.

Από το **Γ)** της υπόθεσης έχουμε τώρα ότι $(\alpha, b) \in \Delta_d$. Δηλ. $(\alpha, b)|d$. Τότε από το **x)** του Θεωρήματος 2 έπεται ότι $|(\alpha, b)| \leq |d| \underset{\text{A)}}{=} d$. Όμως $(\alpha, b) \leq |(\alpha, b)|$. Επομένως $(\alpha, b) \leq d$.

Από το **B)** έχουμε ότι $d \in \Delta_\alpha \cap \Delta_b$. Επίσης $(\alpha, b) = \max(\Delta_\alpha \cap \Delta_b)$. Άρα $d \leq (\alpha, b)$. Συνεπώς $d = (\alpha, b)$.

B) Έστω $\alpha = b = 0$. Τότε $(\alpha, b) = 0$. Από το **Γ)** της υπόθεσης έχουμε ότι $\Delta_\alpha \cap \Delta_b \subseteq \Delta_d$. Όμως $\Delta_\alpha = \Delta_b = \mathbb{Z}$ (βλ. το **ii)** της Παρατήρησης 4). Άρα $\Delta_\alpha \cap \Delta_b = \mathbb{Z}$ και επομένως $\mathbb{Z} \subseteq \Delta_d$. Από αυτό έπεται αμέσως ότι $\Delta_d = \mathbb{Z}$. Τότε από το **ii)** της Παρατήρησης 4 έχουμε ότι $d = 0$. Συνεπώς $d = (\alpha, b)$.

Από **A)** και **B)** έπεται ότι $d = (\alpha, b)$. □

<u>Παρατήρηση 10:</u> Από το **ii)B)** του προηγούμενου Θεωρήματος και το **vi)** του Θεωρήματος 2 έπεται αμέσως ότι αν $d = (\alpha, b)$ τότε για κάθε $x, y \in \mathbb{Z}$ έχουμε ότι $d|(\alpha x + by)$. □

<u>Θεώρημα 11:</u> Έστω $\alpha, b, c, d \in \mathbb{Z}$.

i) $(\alpha, b) = (|\alpha|, |b|)$

ii) $(\alpha c, bc) = |c|(\alpha, b)$

iii) $(\alpha,b)=1 \Leftrightarrow 1=\alpha x+by$ για κάποια $x,y\in\mathbb{Z}$

iv) Αν $(\alpha,b)=d\neq 0$, τότε $\left(\frac{\alpha}{d},\frac{b}{d}\right)=1$.

v) Αν $d\neq 0$, $d\in\Delta_\alpha\cap\Delta_b$ και $\left(\frac{\alpha}{d},\frac{b}{d}\right)=1$, τότε $(\alpha,b)=|d|$.

vi) $(\alpha,1)=1$, $(\alpha,0)=|\alpha|$

<u>Απόδειξη:</u>

i) Άσκηση.

ii) Έστω $f=(\alpha,b)$ και $e=(\alpha c,bc)$. Θα δείξουμε ότι $e=|c|f$.

Αφού $f=(\alpha,b)$ τότε (Θεώρημα 8) υπάρχουν $x,y\in\mathbb{Z}$ τέτοια ώστε $f=\alpha x+by$. Επομένως $cf=\alpha cx+bcy$. Επίσης αφού $e=(\alpha c,bc)$, τότε (βλ. Παρατήρηση 10) έχουμε αμέσως ότι $e|(\alpha cx+bcy)$. Άρα $e|cf$.

Επίσης αφού $f=(\alpha,b)$ τότε (βλ. το **ii)Β)** του Θεωρήματος 9) έχουμε ότι $f|\alpha$ και $f|b$. Τότε από το **viii)** του Θεωρήματος 2 έπεται ότι $cf|\alpha c$ και $cf|bc$. Άρα (βλ. το **ii)Γ)** του Θεωρήματος 9) $cf|e$. Συνεπώς από το **xi)** του Θεωρήματος 2 έχουμε ότι

$$|e|=|cf|=|c||f| \underset{\left(\text{(ii)A) Θεώρ. 9)}\right)}{\overset{e,f\geq 0}{\Leftrightarrow}} e=|c|f$$

iii) ($\Rightarrow$) Άμεσο από το Θεώρημα 8.

($\Leftarrow$) Έστω ότι $1=\alpha x+by$, $x,y\in\mathbb{Z}$. Θα δείξουμε ότι $(\alpha,b)=1$. <u>Πράγματι:</u>

Έστω $h=(\alpha,b)$. Τότε (βλ. Παρατήρηση 10) έχουμε ότι $h|(\alpha x+by)$. Άρα $h|1$ και επομένως $h=-1$ ή $h=1$. Όμως $h\geq 0$ αφού $h=(\alpha,b)$ (βλ. το **i)Α)** του Θεωρήματος 9). Επομένως $h=1$.

iv) $d=(\alpha,b) \underset{\substack{d|\alpha,d|b \\ \text{αφού } d=(\alpha,b) \\ \left(\text{άρα } \frac{\alpha}{d},\frac{b}{d}\in\mathbb{Z}\right)}}{=} \left(d\frac{\alpha}{d},d\frac{b}{d}\right) \underset{\text{ii)}}{=} |d|\left(\frac{\alpha}{d},\frac{b}{d}\right) \underset{\substack{d\geq 0 \\ \text{αφού } d=(\alpha,b) \\ (\text{βλ. } \textbf{i)A)} \text{ Θεώρ. 9})}}{=} d\left(\frac{\alpha}{d},\frac{b}{d}\right) \underset{(d\neq 0)}{\Leftrightarrow} \left(\frac{\alpha}{d},\frac{b}{d}\right)=1$

v) $(\alpha,b) \underset{(d\neq 0)}{=} \left(d\frac{\alpha}{d},d\frac{b}{d}\right) \underset{\substack{\text{ii)} \\ \text{αφού } \frac{\alpha}{d},\frac{b}{d}\in\mathbb{Z} \\ \text{διότι } d\in\Delta_\alpha\cap\Delta_b \\ (\text{άρα } d|\alpha,d|b)}}{=} |d|\left(\frac{\alpha}{d},\frac{b}{d}\right) \underset{\left(\left(\frac{\alpha}{d},\frac{b}{d}\right)=1\right)}{=} |d|$

Άρα $(\alpha,b)=|d|$

vi) Άσκηση. □

<u>Θεώρημα 12 (Λήμμα Ευκλείδη):</u> Έστω $\alpha,b,c\in\mathbb{Z}$ με $\alpha|bc$ και $(\alpha,b)=1$. Τότε $\alpha|c$.

<u>Απόδειξη:</u>

Από το Θεώρημα 8 έχουμε ότι υπάρχουν $x,y\in\mathbb{Z}$ με $1=\alpha x+by$. Άρα $c=\alpha cx+bcy$. Όμως $\alpha|bc$. Άρα (βλ. **vii)** Θεωρήματος 2) $\alpha|bcy$. Επίσης προφανώς $\alpha|\alpha cx$. Άρα (βλ. **vi)** Θεωρήματος 2) $\alpha|(\alpha cx+bcy)$. Συνεπώς $\alpha|c$. □

<u>Θεώρημα 13 (Ευκλείδειος αλγόριθμος):</u> Έστω α, b θετικοί ακέραιοι με $b\nmid\alpha$. Έστω $r_0:=\alpha$ και $r_1:=b$. Εφαρμόζοντας συνεχώς την ταυτότητα της Ευκλείδειας Διαίρεσης προκύπτει ένα σύνολο από υπόλοιπα r_2, r_3, ..., r_n, r_{n+1} που ορίζονται διαδοχικά από τις εξής σχέσεις:

$$r_0=r_1q_1+r_2, \quad 0<r_2<r_1$$

$$r_1=r_2q_2+r_3, \quad 0<r_3<r_2$$

.

.

.

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n + r_{n+1}, \quad r_{n+1} = 0$$

Τότε $r_n = (\alpha, b)$ (δηλ. το τελευταίο μη μηδενικό υπόλοιπο σε αυτήν τη διαδικασία είναι ο (α, b)).

Απόδειξη: Άσκηση. □

ΑΣΚΗΣΕΙΣ

1. **i)** Έστω $\alpha, b \in \mathbb{Z}$ με α, b άρτιοι. Να δείξετε ότι οι ab, $\alpha + b$ είναι άρτιοι.

ii) Έστω $\alpha, b \in \mathbb{Z}$ με α, b περιττοί. Να δείξετε ότι ο ab είναι περιττός και ο $\alpha + b$ είναι άρτιος.

iii) Έστω $\alpha, b \in \mathbb{Z}$ με α άρτιος και b περιττός. Να δείξετε ότι ο ab είναι άρτιος (άρα το γινόμενο δύο διαδοχικών ακεραίων είναι άρτιος) και ο $\alpha + b$ είναι περιττός .

2. Έστω $\alpha \in \mathbb{Z}$. Να δείξετε ότι αν $3 | \alpha^2$ τότε $3 | \alpha$.

3. Να αποδείξετε ότι:

i) Αν $\alpha \in \mathbb{Z}$ και α είναι άρτιος αριθμός, τότε $\alpha^2 = 4\lambda$ για κάποιο $\lambda \in \mathbb{Z}$.

ii) Αν $\alpha \in \mathbb{Z}$ και α είναι περιττός αριθμός, τότε

Α) $\alpha^2 = 4\kappa + 1$ για κάποιο $\kappa \in \mathbb{Z}$.

Γ) $32 | (\alpha^2 + 3)(\alpha^2 + 7)$.

Β) $\alpha^2 = 8\lambda + 1$ για κάποιο $\lambda \in \mathbb{Z}$.

iii) Αν $\alpha, b \in \mathbb{Z}$ και α, b είναι περιττοί αριθμοί, τότε η εξίσωση $x^2 = \alpha^2 + b^2$ δεν έχει ακέραιες λύσεις.

4. Έστω α, b περιττοί ακέραιοι. Να αποδείξετε ότι

i) $\dfrac{\alpha^2+(\alpha+2)^2+(\alpha+4)^2+1}{12}\in\mathbb{Z}$

ii) $\dfrac{\alpha^2-b^2}{8}\in\mathbb{Z}$

iii) $\dfrac{\alpha^4+b^4-2}{16}\in\mathbb{Z}$

5. Για ποιες τιμές του ακεραίου κ ο αριθμός $\dfrac{3\kappa+4}{5}$ είναι ακέραιος.

6. Έστω α, b, γ περιττοί ακέραιοι. Να αποδείξετε ότι η εξίσωση $\alpha x^2+bx+\gamma=0$ δεν έχει ακέραιες λύσεις. Έχει ακέραιες λύσεις η εξίσωση $x^2+5^{2014}x+2013=0$;

7. **i)** Έστω $\alpha\in\mathbb{Z}$ με $\alpha\geq 2$ και $\alpha\neq 3$.

A) Δείξτε ότι υπάρχουν $\kappa,\lambda\in\mathbb{Z}$ τέτοιοι ώστε $\alpha=2\kappa+5\lambda$.

B) Δείξτε ότι υπάρχουν $\mu,\nu\in\mathbb{N}$ τέτοια ώστε $\alpha=2\mu+5\nu$.

Γ) Τα μηχανήματα ΑΤΜ των τραπεζών δίνουν χαρτονομίσματα των 20 € και των 50 €. Τα ποσά που μπορείτε να πάρετε είναι οποιοδήποτε πολλαπλάσιο του 10 μεγαλύτερο ή ίσο των 20 € και διάφορο των 30 €. Πως γίνεται αυτό;

8. Έστω $\alpha,b\in\mathbb{Z}$. Να δείξετε:

i) $\left.\begin{matrix}11|(\alpha+2)\\11|(35-b)\end{matrix}\right\}\Rightarrow 11|(\alpha+b)$

ii) $\left.\begin{matrix}3|\alpha\\3|b\end{matrix}\right\}\Leftrightarrow 3|(\alpha^2+b^2)$

9. Να αποδείξετε ότι

i) Το γινόμενο τριών διαδοχικών ακεραίων διαιρείται με το 6.

ii) $6|\alpha(\alpha+1)(2\alpha+1)$

iii) $6|(\alpha^3+3\alpha^2-4\alpha)$

10. Αν $\kappa \in \mathbb{Z}$ και $m,n \in \mathbb{N}^*$ με $m|n$, να αποδείξετε ότι $\left(\kappa^m - 1\right)\left|\left(\kappa^n - 1\right)\right.$.

11. Για κάθε $\nu \in \mathbb{N}$ να αποδείξετε ότι:

i) $3\left|\left(\nu^3 + 2\nu\right)\right.$

ii) $5\left|\left(3 \cdot 27^\nu + 2 \cdot 2^\nu\right)\right.$

iii) $14\left|\left(3^{4\nu+2} + 5^{2\nu+1}\right)\right.$

12. Για κάθε $\alpha \in \mathbb{Z}$, να αποδείξετε ότι $4 \not| \left(\alpha^2 + 2\right)$.

13. Να αποδείξετε ότι δεν υπάρχουν διαδοχικοί θετικοί ακέραιοι που να είναι και οι δύο τετράγωνα ακεραίων.

14. Αν $m,n \in \mathbb{Z}$ με $m|n$ και $m \neq \pm 1$, τότε $m \not| \left(n+1\right)$.