01-11-16

• **Μέγιστος Κοινός Διαιρέτης**

Έστω $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$

• Ορισμός: Αν υπάρχει $k = 1, 2, \dots, n : \alpha_k \neq 0$, τότε ο (ΜΚΔ) των $\alpha_1, \dots, \alpha_n$ είναι ένας θετικός ακέραιος $d = (\alpha_1, \dots, \alpha_n) = \text{ΜΚΔ}(\alpha_1, \dots, \alpha_n)$

1) $d | \alpha_1, d | \alpha_2, \dots, d | \alpha_n$ και

2) Αν $\delta | \alpha_1, \dots, \delta | \alpha_n$ τότε: $\delta \leq d$

(*) Αν $\alpha_1, \alpha_2, \dots, \alpha_n$ είναι 0 τότε θέτουμε $d = 0$

• Θεώρημα: Έστω $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$ και τουλάχιστον ένας απ' αυτούς είναι μη-μηδενικός

Αν $d = (\alpha_1, \alpha_2, \dots, \alpha_n)$ τότε υπάρχουν $k_1, k_2, \dots, k_n \in \mathbb{Z}$

$d = k_1\alpha_1 + k_2\alpha_2 + \dots + k_n\alpha_n$ (ακέραιος γραμμικός συνδυασμός των $\alpha_1, \dots, \alpha_n$)

Απόδειξη: Θεωρούμε το σύνολο $S = \{x_1\alpha_1 + \dots + x_n\alpha_n \mid x_i \in \mathbb{Z}, 1 \leq i \leq n\}$

$S \subseteq \mathbb{Z}$

• 1ο Βήμα: $S \neq \emptyset$, διότι $\forall i = 1, \dots, n$, $\alpha_i \in S$

$[\alpha_i = 0 \cdot \alpha_1 + 0 \cdot \alpha_2 + \dots + 1 \cdot \alpha_i + 0 \cdot \alpha_{i+1} + \dots + 0 \cdot \alpha_n] \in S$

• 2ο Βήμα: $S \cap \mathbb{N} \neq \emptyset$ διότι υπάρχει $k=1,\dots,n$: $a_k \neq 0$ και τότε

• Αν $a_k > 0 \Rightarrow a_k \in S \cap \mathbb{N}$

• Αν $a_k < 0 \Rightarrow -a_k > 0$ και $-a_k = (0 \cdot a_1 + \dots - 1 \cdot a_k + \dots + 0 \cdot a_n) \in S$

$\Rightarrow -a_k \in S \cap \mathbb{N}$

• 3ο Βήμα: Επειδή $S \cap \mathbb{N} \neq \emptyset$, απ' την (ΑΚΔ) έπεται ότι το $S \cap \mathbb{N}$ έχει ελάχιστο στοιχείο $d = \min(S \cap \mathbb{N})$

ΘΔΟ: $d = (a_1, a_2, \dots, a_n)$

• 4ο Βήμα: $d \in S \cap \mathbb{N} \Rightarrow \exists k_1, \dots, k_n \in \mathbb{Z} : d = k_1 a_1 + \dots + k_n a_n$ (1)

Θα δείξουμε ότι $S = \{d \cdot q \in \mathbb{Z} \mid q \in \mathbb{Z}\}$

• Αν $q \in \mathbb{Z}$, τότε επειδή $d = k_1 a_1 + \dots + k_n a_n \Rightarrow$

$\Rightarrow dq = (k_1 q) a_1 + \dots + (k_n q) a_n \in S$

Άρα, $\{dq \in \mathbb{Z} \mid q \in \mathbb{Z}\} \subseteq S$ (2)

Από την Ευκλείδεια Διαίρεση του m με το d, θα έχουμε $m = dq + r$, $d, r \in \mathbb{Z}$ και $0 \leq r < d$

Αν $r \neq 0$, τότε $r = m - dq = (j_1 a_1 + \dots + j_n a_n - (k_1 q) a_1 - \dots - (k_n q) a_n)$

$= (j_1 - k_1 q) a_1 + \dots + (j_n - k_n q) a_n$. Άρα, επειδή $r > 0$

έπεται ότι $r \in S \cap \mathbb{N}$. Άτοπο, διότι $r < d$ και $d = \min S \cap \mathbb{N}$

Άρα, $r=0 \Rightarrow m=dq \in \{dq \in Z \mid q \in Z\} \Rightarrow$

$\Rightarrow S \subseteq \{dq \mid q \in Z\}$ (3)

Από τις σχέσεις (2), (3) έπεται ότι $S=\{dq \in Z \mid q \in Z\}$

5ο Βήμα: Γνωρίζουμε ότι τα $a_1, a_2, \dots, a_n \in S$

Όμως $S=\{dq \in Z \mid q \in Z\} \Rightarrow d \mid a_1, \dots, d \mid a_n$

Έστω $\delta \mid a_1, \delta \mid a_2, \dots, \delta \mid a_n$. Τότε

$\delta \mid k_1 a_1, \dots, \delta \mid k_n a_n \Rightarrow \delta \mid k_1 a_1 + \dots + k_n a_n \Rightarrow$

$\boxed{\delta \mid d} \Rightarrow \delta \leq d$ Άρα, $d=(a_1, \dots, a_n)$

• Πόρισμα: Έστω $a_1, a_2, \dots, a_n \in Z$ και υπάρχει $k=1, \dots, n$ $a_k \neq 0$

Τότε αν $d \in N$, ο $d=(a_1, \dots, a_n) \Leftrightarrow$

1) $d \mid a_1, \dots, d \mid a_n$

2) $\delta \mid a_1, \dots, \delta \mid a_n \Rightarrow \delta \mid d$

• Πόρισμα: Έστω ότι $a_1, a_2, \dots, a_n \in Z$ και υπάρχει $k=1, \dots, n$, $a_k \neq 0$

Αν $d \in N$ έτσι ώστε 1) $d \mid a_1, \dots, a_n$
2) $d=k_1 a_1 + \dots + k_n a_n$, $k_i \in Z$

Τότε $d=(a_1, \dots, a_n)$

(*) Οι αποδείξεις των πορισμάτων είναι άμεσες συνέπειες του θεωρήματος.

• **Ορισμός**: Αν $a_1, a_2, ..., a_n \in \mathbb{Z}$, τότε:

1) Οι $a_1, a_2, ..., a_n$ καλούνται πρώτοι μεταξύ τους $\Leftrightarrow$

$\Leftrightarrow (a_1, a_2, ..., a_n) = 1$

2) Οι $a_1, a_2, ..., a_n$ καλούνται πρώτοι μεταξύ τους ανά δύο $\Leftrightarrow$

$\Leftrightarrow$ Αν $1 \le i \neq j \le n : (a_i, a_j) = 1$

Παράδειγμα: $a_1 = 6$, $a_2 = 14$, $a_3 = 21$

Τότε $(6, 14, 21) = 1$, όμως $(6, 14) = 2 \neq 1$

• Πόρισμα: Αν $d = (a_1, a_2, ..., a_n)$ τότε:

$d = 1 = (a_1, ..., a_n) \Leftrightarrow \exists\, k_1, ..., k_n \in \mathbb{Z} : 1 = k_1 a_1 + ... + k_n a_n$

Απόδειξη: $(\Rightarrow)$ προκύπτει απ' το Θεώρημα

$(\Leftarrow)$ $\left.\begin{array}{l} 1 = k_1 a_1 + ... + k_n a_n \\ 1 | a_1, ..., 1 | a_n \end{array}\right\} \xRightarrow{\text{Πόρισμα}} 1 = (a_1, ..., a_n)$

Παράδειγμα: $\forall \kappa \in \mathbb{Z} : (2\kappa+1, 9\kappa+4) = 1$

$9(2\kappa+1) - 2(9\kappa+4) = 18\kappa + 9 - 18\kappa + 8 = 1$

Απ' το πόρισμα προκύπτει το ζητούμενο

Θέσαμε $d = (2\kappa+1, 9\kappa+4) \Rightarrow \begin{cases} d \mid 2\kappa+1 \\ d \mid 9\kappa+4 \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} d \mid 9(2\kappa+1) \Rightarrow d \mid 18\kappa+9 \\ d \mid 2(9\kappa+4) \Rightarrow d \mid 18\kappa+8 \end{cases} \Rightarrow d \mid 18\kappa+9-18\kappa-8$

$\Rightarrow d \mid 1$, άρα $d = 1$

• **Θεώρημα:** Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$, υπάρχει $\kappa = 1, \dots, n : a_\kappa \neq 0$

Τότε: 1) $(a_1, a_2, \dots, a_n) = (|a_1|, |a_2|, \dots, |a_n|)$

2) Αν $\lambda \neq 0$, τότε: $(\lambda a_1, \lambda a_2, \dots, \lambda a_n) = |\lambda| (a_1, \dots, a_n)$

3) Αν $\kappa_1, \kappa_2, \dots, \kappa_n \in \mathbb{Z} : (a_1, \dots, a_n) = (a_1, a_2, \dots, a_n, \kappa_1 a_1 + \dots + \kappa_n a_n)$

4) $(a_1, a_2, \dots, a_n) = d$, τότε: $\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = 1$

Απόδειξη: 1) Επειδή $x|a \iff x| |a|$ η ισότητα 1 προκύπτει άμεσα.

2) Αν $\lambda > 0$ τότε έστω $d = (a_1, a_2, \ldots, a_n)$ και

$\delta = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n)$

ΘΔΟ: $\delta = \lambda d$, θα έχουμε:

$d = (a_1, \ldots, a_n) \Rightarrow \exists k_1, \ldots, k_n \in \mathbb{Z} : d = k_1 a_1 + \ldots + k_n a_n$

$$\left.\begin{array}{l} \Rightarrow \lambda d = k_1(\lambda a_1) + \ldots + k_n(\lambda a_n) \ (*) \\ d|a_1, \ldots, d|a_n \Rightarrow \lambda d | \lambda a_1, \ldots, \lambda d | \lambda a_n \ (**) \end{array}\right\} \Rightarrow$$

$\Rightarrow \lambda d = (\lambda a_1, \ldots, \lambda a_n) = \delta$

Για $\lambda < 0$ (αφήνεται ως άσκηση - Αποδεικνύεται ανάλογα)

3) Έστω $d = (a_1, a_2, \ldots, a_n)$ και $\delta = (a_1, \ldots, a_n, k_1 a_1 + \ldots + k_n a_n)$

$d|a_1, \ldots, d|a_n \Rightarrow d|k_1 a_1, \ldots, d|k_n a_n \Rightarrow$

$$\left.\begin{array}{l} \left.\begin{array}{l} \Rightarrow d | k_1 a_1 + \ldots + k_n a_n \\ d|a_1, \ldots, d|a_n \end{array}\right\} \Rightarrow d|\delta \ (1) \\ \delta | a_i, \ 1 \le i \le n \Rightarrow \delta | d \ (2) \end{array}\right\} \Rightarrow \text{Απ' τις 1, 2 προκύπτει } \delta = d$$

4) $d | a_i \ , \ 1 \leq i \leq n \Rightarrow \frac{a_i}{d} \in \mathbb{Z} \ , \ 1 \leq i \leq n$

Τότε $d = (a_1, a_2, \dots, a_n) = \left(d \cdot \frac{a_1}{d}, d \frac{a_2}{d}, \dots, d \frac{a_n}{d} \right)$

$= d \left(\frac{a_1}{d}, \dots, \frac{a_n}{d} \right) \Rightarrow \left(\frac{a_1}{d}, \dots, \frac{a_n}{d} \right) = 1$

Άσκηση: $(\alpha, b) = 1 \Rightarrow (\alpha + b, \alpha - b) = ?$

Έστω $d = (\alpha + b, \alpha - b) \Rightarrow \left. \begin{cases} d | \alpha + b \\ d | \alpha - b \end{cases} \xrightarrow[(-)]{(+)} \begin{matrix} d | 2\alpha \\ d | 2b \end{matrix} \right\} \Rightarrow$

$\Rightarrow d | (2\alpha, 2b) \Rightarrow (2\alpha, 2b) = 2(\alpha, b) = 2$

Άρα, $d | 2 \Rightarrow d = 1$ ή $d = 2$

~> Αν α, b: άρτιοι $\Rightarrow$ Άτοπο διότι $(\alpha, b) = 1$

~> Αν α, b: περιττοί $\Rightarrow \alpha + b, \alpha - b$: άρτιοι, άρα $\begin{matrix} 2 | \alpha + b \\ 2 | \alpha - b \end{matrix}$

$\Rightarrow 2 | d \Rightarrow 2 \leq d$, άρα $d = 2$

• Αν α: περιττός (αντ. άρτιος), b: άρτιος (αντ. περιττός)

$d = 1$