

19/03/15.

Μέγιστος Κοινός Διαπέρων

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

- Αν $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$ τότε: $\forall m \in \mathbb{Z} : m|\alpha_1 = 0, \dots, m|\alpha_n = 0$

Άρα το πλήθος των θετικών κοινών διαπέρων είναι άπειρο
Οπότε ο μέγιστος κοινός διαπέρων των $\alpha_1, \dots, \alpha_n$
με $\alpha_1 = \dots = \alpha_n = 0$ είναι το 0.

- Υποθέτουμε ότι: $\exists i=1, \dots, n : \alpha_i \neq 0$. Τότε το σύνολο S των θετικών διαπέρων των $\alpha_1, \dots, \alpha_n$ είναι $\neq \emptyset$: $S = \{m \in \mathbb{N} \mid m|\alpha_1, \dots, m|\alpha_n\}$
κοινών διότι $1 \in S$.

Επίσης το S είναι πεπερασμένο διότι: αν $m \in S \Rightarrow$
 $\Rightarrow m|\alpha_i \Rightarrow m|\alpha_i \Rightarrow m \leq |\alpha_i| \Rightarrow 1 \leq m \leq |\alpha_i|$

Ορίσμος: Έστω $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$.

① Αν $\alpha_1 = \dots = \alpha_n = 0$ τότε ο Μέγιστος Κοινός Διαπέρων αυτών συμβολίζεται με: $(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$.

② Αν $\exists i=1, \dots, n : \alpha_i \neq 0$, τότε ο Μέγιστος Κοινός Διαπέρων των $\alpha_1, \dots, \alpha_n$ ορίζεται να είναι το max στοιχείο του S & συμβολίζεται με: $(\alpha_1, \dots, \alpha_n)$

Έστω $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ κ' $\exists i=1, \dots, n : \alpha_i \neq 0$.

Τότε: $d = (\alpha_1, \dots, \alpha_n) \Leftrightarrow d \in \mathbb{N}$ κ' $d|\alpha_1, \dots, d|\alpha_n$
κ' αν $\delta|\alpha_1, \dots, \delta|\alpha_n$ τότε $\Rightarrow \delta \leq d$

Θεώρημα: Έστω $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ κ' $\exists i=1, \dots, n : \alpha_i \neq 0$. Τότε
αν $d = (\alpha_1, \dots, \alpha_n)$, τότε $\exists k_1, \dots, k_n \in \mathbb{Z} : \boxed{d = k_1\alpha_1 + \dots + k_n\alpha_n}$

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

Επειδή $\forall i=1, \dots, n : \alpha_i = 0 \cdot \alpha_1 + \dots + 0 \cdot \alpha_{i-1} + 1 \cdot \alpha_i + \dots + 0 \cdot \alpha_n \Rightarrow$

$\Rightarrow \forall i=1, \dots, n : \alpha_i \in S$. Επειδή τουλάχιστον ένα από τα $\alpha_i \neq 0$
 $\alpha_i \in S \Rightarrow$ το S θα περιέχει k' μη μηδενικά στοιχεία
 Επειδή κάθε $\alpha_i \in S \Rightarrow -\alpha_i \in S$ διότι:

$$-\alpha_i = 0 \cdot \alpha_1 + \dots + 0 \cdot \alpha_{i-1} + (-1) \cdot \alpha_i + \dots + 0 \cdot \alpha_n$$

$\Rightarrow S$ περιέχει πάντα k' -θετικούς ακεραίους $\Rightarrow$

$\Rightarrow S \cap \mathbb{N} \neq \emptyset$. Άρα από (ΑΚΔ) το S έχει μιν, έστω d
 $d = \min(S \cap \mathbb{N})$.

Αρκεί νδο $d = (\alpha_1, \dots, \alpha_n)$.

Έστω $m \in S \Rightarrow \exists \xi_1, \dots, \xi_n \in \mathbb{Z} : \xi_1 \alpha_1 + \dots + \xi_n \alpha_n = m$.

Από την Ευκλείδεια διαίρεση του m με το d θα έχουμε:
 $m = d \cdot q + r, 0 \leq r < d$

$$\text{Τότε } r = m - d \cdot q = \xi_1 \alpha_1 + \dots + \xi_n \alpha_n - d \cdot q$$

Όμως $d = \min(S \cap \mathbb{N}) \Rightarrow \exists k_1, \dots, k_n \in \mathbb{Z} : d = k_1 \alpha_1 + \dots + k_n \alpha_n$

$$\Rightarrow r = \xi_1 \alpha_1 + \dots + \xi_n \alpha_n - (q k_1 \alpha_1 + \dots + q k_n \alpha_n) =$$

$$= (\xi_1 - q k_1) \alpha_1 + \dots + (\xi_n - q k_n) \alpha_n \in S$$

Επειδή $0 \leq r < d$, αν $r \neq 0 \Rightarrow r \in (S \cap \mathbb{N})$ και τότε θα έχουμε

Απονο διότι $r < d \neq d = \min(S \cap \mathbb{N})$

Οπότε $r=0 \Rightarrow m = d \cdot q$.

Άρα $\forall m \in S : d | m$. Διαίρεται επειδή $\alpha_1, \dots, \alpha_n \in S$, θα έχουμε
 ότι $d | \alpha_1, \dots, d | \alpha_n$ ①

Έστω ότι $\delta \in \mathbb{N}$ κ' $\delta | \alpha_1, \dots, \delta | \alpha_n$. Πρέπει νδο $\delta \leq d \Rightarrow$

$$\Rightarrow \delta | k_1 \alpha_1 + \dots + k_n \alpha_n \rightarrow \delta | (k_1 \alpha_1 + \dots + k_n \alpha_n) = d \Rightarrow$$

$$\Rightarrow \boxed{\delta \leq d} \text{ ②}$$

Από ①, ② $\Rightarrow d = (\alpha_1, \dots, \alpha_n)$.

Πρόταση: Έστω $\alpha_1, \dots, \alpha_n \in \mathbb{Z}, \exists i=1, \dots, n, \alpha_i \neq 0$. Τότε

$$d = (\alpha_1, \dots, \alpha_n) \Leftrightarrow d \in \mathbb{N}, d | \alpha_1, \dots, d | \alpha_n$$

$$\text{αν } \delta | \alpha_1, \dots, \delta | \alpha_n \Rightarrow \delta | d$$

Απόδειξη: $(\Rightarrow)$ Αν $d = (\alpha_1, \dots, \alpha_n)$ κ' αν $\delta | \alpha_1, \dots, \delta | \alpha_n$ τότε
 από το Παράδειγμα $\Rightarrow \exists k_1, \dots, k_n \in \mathbb{Z} : d = k_1 \alpha_1 + \dots + k_n \alpha_n$

$$(\Leftarrow) \text{ Av } d \in \mathbb{N} \quad k' \mid d \mid \alpha_1, \dots, d \mid \alpha_n \quad k' \mid \delta \mid d_1, \dots, \delta \mid d_n \Rightarrow \delta \mid d \Rightarrow \\ \Rightarrow \delta \leq d \Rightarrow \boxed{d = (\alpha_1, \dots, \alpha_n)}.$$

Definition: Es sei $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$, $\exists i=1, \dots, n : \alpha_i \neq 0$ & ist
 $(d \in \mathbb{N}) \quad d = (\alpha_1, \dots, \alpha_n) (=) d \mid \alpha_1, \dots, d \mid \alpha_n \quad k' \cdot d = k_1 \alpha_1 + \dots + k_n \alpha_n$ & a.k. $k_1, \dots, k_n \in \mathbb{Z}$

($\Leftarrow$) Έστω ότι $\delta/\alpha_1, \dots, \delta/\alpha_n \Rightarrow \delta/k_1\alpha_1, \dots, \delta/k_n\alpha_n \Rightarrow$
 $\Rightarrow \delta/(k_1\alpha_1 + \dots + k_n\alpha_n) = d \Rightarrow$ από το προηγούμενο
 πρόβλημα έχουμε το ζητούμενο $\delta \eta \Rightarrow d = (\alpha_1, \dots, \alpha_n)$.

Παράδειγμα ① : Έστω ότι $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ κ' $\exists i, j = 1, \dots, n$
 $i \neq j$ κ' $\gcd(\alpha_i, \alpha_j) = 1$. Έστω ότι
 $d = (\alpha_1, \dots, \alpha_n) \Rightarrow d \mid \alpha_i, d \mid \alpha_j$. Τότε $d \mid (\alpha_i, \alpha_j) = 1 \} \Rightarrow$
 $d \in \mathbb{N}$
 $\Rightarrow \boxed{d=1}$. Άρα $(\alpha_1, \dots, \alpha_n) = 1$

- Το αντίστροφο του ② $\Delta EN_{16\chi\psi\epsilon\tau} : (6, 14, 21) = 1$

ANNA : $(6, 14) = 2$
 $(6, 21) = 3$
 $(14, 21) = 7$ } $\Rightarrow$ 0×1
 $npwzoi$
 $ttzaxjzovs$
 $avx 2$

1836 12714 13721

Πρόταση : Αν $d_1, \dots, d_n \in \mathbb{Z}$, τότε $(d_1, \dots, d_n) = 1 \Leftrightarrow$
 $(\Rightarrow) \exists k_1, \dots, k_n : k_1 d_1 + \dots + k_n d_n = 1$

Απόδειξη : $(\Rightarrow)$ έχει αποδειχθεί πριν.
 $(\Leftarrow) \left. \begin{array}{l} d_1, \dots, d_n \neq 0 \\ 1 = k_1 d_1 + \dots + k_n d_n \end{array} \right\} \Rightarrow$

Πομπή $(d_1, \dots, d_n) = 1$.

Παράδειγμα ① : ~~$(9k+7, 4k+3)$~~ , ($k = \text{ωχόν αριθμός}$)
 $(2k+1, 9k+4) = 1$

$$\begin{aligned} \text{Έστω } d = (2k+1, 9k+4) &\Rightarrow d \mid 2k+1, d \mid 9k+4 \Rightarrow \\ &\Rightarrow \begin{cases} d \mid 9(2k+1) = 18k+9 \\ d \mid 2(9k+4) = 18k+8 \end{cases} \Rightarrow d \mid 18k+9 - 18k-8 = 1 \\ &\Rightarrow \boxed{d \mid 1} \Rightarrow \boxed{d=1} \end{aligned}$$

Ενισχύει : $9(2k+1) - 2(9k+4) = 1 \Rightarrow 1 = (2k+1, 9k+4)$
 ΠΡΟΤΑΣΗ

Παράδειγμα ② : Αν $a, b \in \mathbb{Z}$ κ' $(a, b) = 1$ τότε:
 $(9a+7b, 4a+3b) = 1$

Έστω ότι $d = (9a+7b, 4a+3b) \Rightarrow$

$$\Rightarrow \begin{cases} d \mid 9a+7b \\ d \mid 4a+3b \end{cases} \Rightarrow \begin{cases} d \mid 4(9a+7b) \\ d \mid 9(4a+3b) \end{cases} \Rightarrow$$

$$\Rightarrow d \mid 36a + 28b - 36a - 27 \Rightarrow \boxed{d \mid b} \text{ ①}$$

$$\begin{aligned} \text{Ενισχύει } \begin{cases} d \mid 3(9a+7b) \\ d \mid 7(4a+3b) \end{cases} &\Rightarrow d \mid 27a + 21b - 28 - 21b \Rightarrow \\ &\Rightarrow d \mid -a \Rightarrow \boxed{d \mid a} \text{ ②} \end{aligned}$$

$$\text{Από ①②} \Rightarrow \begin{cases} d \mid (a, b) = 1 \\ d \in \mathbb{N} \end{cases} \Rightarrow \boxed{d=1}$$

Θεώρημα: Έστω $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ όχι όλοι ίσοι. Τότε:

① $(\alpha_1, \dots, \alpha_n) = (|\alpha_1|, \dots, |\alpha_n|)$

② $\forall \lambda \neq 0$, τότε: $(\lambda \alpha_1, \dots, \lambda \alpha_n) = |\lambda| (\alpha_1, \dots, \alpha_n)$

③ $\forall \gamma = \alpha_1 x_1 + \dots + \alpha_n x_n \Rightarrow (\alpha_1, \dots, \alpha_n, \gamma) = (\alpha_1, \dots, \alpha_n)$
 $x_i \in \mathbb{Z} \quad \forall i=1, \dots, n$

④ $(\alpha_1, \dots, \alpha_n) = d \Leftrightarrow \left(\frac{\alpha_1}{d}, \dots, \frac{\alpha_n}{d}\right) = 1$.

Απόδειξη: ① Έστω $d = (\alpha_1, \dots, \alpha_n)$ & $d' = (|\alpha_1|, \dots, |\alpha_n|)$

$$\left. \begin{aligned} \text{Το } d|\alpha_1, \dots, d|\alpha_n &\Rightarrow d||\alpha_1|, \dots, d||\alpha_n| \Rightarrow \boxed{d|d'} \text{ ①} \\ \text{Το } d'|\alpha_1, \dots, d'|\alpha_n &\Rightarrow d'|\alpha_1, \dots, d'|\alpha_n \Rightarrow \boxed{d'|d} \text{ ②} \end{aligned} \right\} \Rightarrow$$

$$\Rightarrow \boxed{d=d'}$$

② • $\lambda > 0$. Έστω $d = (\alpha_1, \dots, \alpha_n) \Rightarrow d|\alpha_1, \dots, d|\alpha_n \Rightarrow$
 $\Rightarrow \lambda d|\lambda \alpha_1, \dots, \lambda d|\lambda \alpha_n \Rightarrow \lambda d|(\lambda \alpha_1, \dots, \lambda \alpha_n) = \delta$
 $d = (\alpha_1, \dots, \alpha_n) \Rightarrow \exists k_1, \dots, k_n \in \mathbb{Z} : d = k_1 \alpha_1 + \dots + k_n \alpha_n \Rightarrow$
 $\Rightarrow \lambda d = \lambda k_1 \alpha_1 + \dots + \lambda k_n \alpha_n$
 $\delta = (\lambda \alpha_1, \dots, \lambda \alpha_n) \Rightarrow \delta|\lambda k_1 \alpha_1, \dots, \delta|\lambda k_n \alpha_n \Rightarrow$
 $\Rightarrow \delta|\lambda k_1 d, \dots, \delta|\lambda k_n d \Rightarrow \delta|(\lambda k_1 d + \dots + \lambda k_n d) = \lambda d$
 $\left. \begin{aligned} \text{Άρα } \delta|\lambda d \\ \text{Άρα } \lambda d|\delta \end{aligned} \right\} \Rightarrow \boxed{\delta = \lambda d}$

• $\forall \lambda < 0 \Rightarrow$ δουλεύει ανάλογα.

③ $d = (\alpha_1, \dots, \alpha_n)$ & $\delta = (\alpha_1, \dots, \alpha_n, \gamma)$. Θ.δ.ο. $d = \delta$
 $d|\alpha_1, \dots, d|\alpha_n \Rightarrow d|\alpha_1 x_1, \dots, d|\alpha_n x_n \Rightarrow d|\alpha_1 x_1 + \dots + \alpha_n x_n = \gamma$
 $\left. \begin{aligned} \text{Άρα } d|\gamma \end{aligned} \right\} \Rightarrow \boxed{d|\delta} \text{ ①}$
 $\left. \begin{aligned} \text{Προφανώς } \delta|\alpha_1, \dots, \delta|\alpha_n \end{aligned} \right\} \Rightarrow \boxed{\delta|d} \text{ ②} \Rightarrow \boxed{\delta = d}$

④ $(\Rightarrow) d = (\alpha_1, \dots, \alpha_n) \Rightarrow d|\alpha_1, \dots, d|\alpha_n \Rightarrow \frac{\alpha_1}{d}, \dots, \frac{\alpha_n}{d} \in \mathbb{Z}$

$d = \alpha_1 k_1 + \dots + \alpha_n k_n$, για $k_1, \dots, k_n \in \mathbb{Z} \Rightarrow$

$$1 = k_1 \cdot \frac{\alpha_1}{d} + \dots + k_n \cdot \frac{\alpha_n}{d} \Rightarrow \left(\frac{\alpha_1}{d}, \dots, \frac{\alpha_n}{d} \right) = 1$$

$$(\Leftrightarrow) \exists \text{gcd} \left(\frac{\alpha_1}{d}, \dots, \frac{\alpha_n}{d} \right) = 1 \Rightarrow \frac{\alpha_1}{d}, \dots, \frac{\alpha_n}{d} \in \mathbb{Z} \Rightarrow$$

$$\Rightarrow d \mid \alpha_1, \dots, d \mid \alpha_n$$

$$\Rightarrow \exists \lambda_1, \dots, \lambda_n \in \mathbb{Z} : \lambda_1 \cdot \frac{\alpha_1}{d} + \dots + \lambda_n \cdot \frac{\alpha_n}{d} = 1 \Rightarrow \lambda_1 \alpha_1 + \dots + \lambda_n \alpha_n = d$$

$$\Rightarrow d = (\alpha_1, \dots, \alpha_n)$$

Πρόταση: Αν $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$, τότε $(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_k, (\alpha_{k+1}, \dots, \alpha_n))$

$$\forall k \in \mathbb{N} : 1 \leq k \leq n-2$$

Απόδειξη: Έστω $d = (\alpha_1, \dots, \alpha_n) \mid k' \mid \delta = (\alpha_{k+1}, \dots, \alpha_n)$
 $k' \mid d' = (\alpha_1, \dots, \alpha_k, \delta)$

$$\text{Θ.δ.ο. } d = d'$$

$$\text{Είναι: } d = (\alpha_1, \dots, \alpha_n) \Rightarrow d \mid \alpha_1, \dots, d \mid \alpha_k, \underbrace{d \mid \alpha_{k+1}, \dots, d \mid \alpha_n}_{d \mid \delta = (\alpha_{k+1}, \dots, \alpha_n)}$$

$$\text{Άρα } d \mid \alpha_1, \dots, d \mid \alpha_k, d \mid \delta \Rightarrow \boxed{d \mid d'} \text{ ①}$$

$$d' = (\alpha_1, \dots, \alpha_k, \delta) \Rightarrow \left\{ \begin{array}{l} d' \mid \alpha_1, \dots, d' \mid \alpha_k \\ d' \mid \delta \text{ ή } k' \delta \mid \alpha_{k+1}, \dots, \alpha_n \end{array} \right\} \Rightarrow$$

$$\Rightarrow d' \mid \alpha_1, \dots, d' \mid \alpha_k, d' \mid \alpha_{k+1}, \dots, d' \mid \alpha_n \Rightarrow$$

$$\Rightarrow \boxed{d' \mid d} \text{ ②}$$

$$\text{Από ①, ②} \Rightarrow \boxed{d = d'}$$

Περικύβημα: Αν σ : μερική τάξη των αριθμών $1, 2, \dots, n$, τότε:
 $(\alpha_1, \dots, \alpha_n) = (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$

Θεώρημα (Λήμμα του Ευκλείδη): Έστω $a, b, c \in \mathbb{Z}$ κ'έστω
 $a | bc$. Αν $(a, b) = 1$ τότε $a | c$.
 (Αντίστροφα $(a, c) = 1 \Rightarrow a | b$).

Απόδειξη: $a | b \cdot c \Rightarrow \exists z \in \mathbb{Z} : bc = a \cdot z$ ①
 $(a, b) = 1 \Rightarrow \exists (x, y) \in \mathbb{Z}^2 : ax + by = 1$ ②

$$c = c \cdot 1 \stackrel{②}{=} c(ax + by) = cax + bcy \stackrel{①}{=} c \cdot ax + azy = a(cx + zy). \text{ Άρα } a | c$$

Παρατήρηση: Έστω P πρώτος. Τότε $\forall a \in \mathbb{Z} : (P, a) = \begin{cases} 1 \Leftrightarrow P \nmid a \\ P \Leftrightarrow P | a \end{cases}$

Αν $P | a \cdot b$. Έστω $P \nmid a \Rightarrow (P, a) = 1$.
 Από το Θεώρημα $\Rightarrow P | b$

Θεώρημα: Έστω $a, b \in \mathbb{N}$ κ'έστω ότι: $a = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$
 κ' $b = p_1^{b_1} \cdot \dots \cdot p_k^{b_k}$, όπου $a_i \geq 0, b_i \geq 0, 1 \leq i \leq k$.
 $(a, b) = p_1^{c_1} \cdot \dots \cdot p_k^{c_k}$, όπου $c_i = \min\{a_i, b_i\}, \forall i = 1, \dots, k$.

Απόδειξη: Έστω $d = p_1^{c_1} \cdot \dots \cdot p_k^{c_k}$ όπου $c_i = \min\{a_i, b_i\}, \forall i = 1, \dots, k$
 $\forall i = 1, \dots, k : c_i = \min\{a_i, b_i\} \leq a_i, b_i \Rightarrow$
 $\Rightarrow d | a \text{ κ' } d | b$ ①

Αν $a = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$
 τότε $d | a \Rightarrow d = p_1^{c_1} \cdot \dots \cdot p_k^{c_k}$
 $0 \leq c_i \leq a_i, 1 \leq i \leq k$

Έστω $\delta | a$ κ' $\delta | b$
 Όπου $\delta = p_1^{\delta_1} \cdot \dots \cdot p_k^{\delta_k}$

Τότε $\delta | a \Rightarrow \delta_i \leq a_i$
 $\delta | b \Rightarrow \delta_i \leq b_i$
 $\forall i = 1, \dots, k$

$$\Rightarrow \delta_i \leq \min\{a_i, b_i\} = c_i$$

$$\text{Επειδή } d = p_1^{c_1} \cdot \dots \cdot p_k^{c_k} \Rightarrow \delta | d$$
 ②

$$\text{Από ①, ②} \Rightarrow (a, b) = d$$

Γενίκευση (Θεώρημα): Έστω $a_1, \dots, a_k$ ($k \geq 2$) θετικοί διαφορετικοί
 Τότε $\forall j = 1, \dots, k : a_j = p_1^{a_{j1}} \cdot \dots \cdot p_r^{a_{jr}}$ και τότε
 $(a_1, \dots, a_k) = p_1^{b_1} \cdot \dots \cdot p_k^{b_k}$ όπου $b_i = \min\{a_{i1}, \dots, a_{ik}\} \quad \forall i = 1, \dots, k$