09-11-16

• <u>Αλγόριθμος του Ευκλείδη</u>

Έστω $\alpha, b \in \mathbb{Z}$ κι έστω $\alpha, b \neq 0$. Ο αλγόριθμος του Ευκλείδη αφορά τη μέθοδο εύρεσης του ΜΚΔ(α, b) των α, b.

~ **Λήμμα:** Έστω $\alpha, b \in \mathbb{Z}$, $b \neq 0$ κι έστω οι μοναδικοί ακέραιοι q, r: $\alpha = bq + r$, $0 \leq r < |b|$

Τότε: $(\alpha, b) = (b, r)$, αν $r \neq 0$

Αν $r = 0$, τότε $(\alpha, b) = |b|$

Απόδειξη: Έστω $d = (\alpha, b)$ και $\delta = (b, r)$

Ν.δ.ο.: $d = \delta$

$$(1): d = (\alpha, b) \Rightarrow \begin{cases} d \mid \alpha \\ d \mid b \end{cases} \Rightarrow \begin{cases} d \mid \alpha \\ d \mid bq \end{cases} \Rightarrow d \mid \alpha - bq \Rightarrow$$

$$\Rightarrow \begin{cases} d \mid r \\ d \mid b \end{cases} \Rightarrow d \mid (b, r). \text{ Άρα, } d \mid \delta$$

$$(2): \delta = (b, r) \Rightarrow \begin{cases} \delta \mid b \\ \delta \mid r \end{cases} \Rightarrow \begin{cases} \delta \mid bq \\ \delta \mid r \end{cases} \Rightarrow \delta \mid bq + r \Rightarrow$$

$$\Rightarrow \begin{cases} \delta \mid \alpha \\ \delta \mid b \end{cases} \Rightarrow \delta \mid (\alpha, b) \Rightarrow \delta \mid d. \text{ Από } (1), (2) \Rightarrow \boxed{\delta = d}$$

Έστω $\alpha, b \in \mathbb{Z}$, $\alpha \neq 0 \neq b$. Για την εύρεση του (α, b) αρκεί να περιοριστούμε στην περίπτωση: $\alpha, b > 0$

{διότι: $(\alpha, b) = (|\alpha|, |b|)$.

Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $\alpha \geq b > 0$

Συμβολίζουμε $\alpha = r_0$, $b = r_1$

$r_0 = r_1 q_1 + r_2$, όπου $0 \leq r_2 < r_1$

$(*)$ $(r_0, r_1) = (r_1, r_2)$

$r_1 = r_2 q_2 + r_3$, όπου $0 \leq r_3 < r_2$

$(**)$ $(r_1, r_2) = (r_2, r_3)$

$r_2 = r_3 q_3 + r_4$, όπου $0 \leq r_4 < r_3$

$(***)$ $(r_2, r_3) = (r_3, r_4)$

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

$r_{n-1} = r_n q_n + r_{n+1}$, όπου $0 \leq r_{n+1} < r_n$

$\hookrightarrow r_1 > r_2 > r_3 > \ldots > r_{n-2} > r_{n-1} > r_n > \ldots$

Η παραπάνω είναι γνησίως φθίνουσα ακολουθία φυσικών αριθμών κι έπεται ότι:

$\exists k : r_k = 0$. Έστω ότι $k = n+1 \Rightarrow r_{n+1} = 0$

$(\alpha, b) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$

Άρα ο ΜΚΔ των α, b είναι το τελευταίο μη-μηδενικό υπόλοιπο στις διαδοχικές Ευκλείδειες Διαιρέσεις.

↳ Η παραπάνω διαδικασία είναι αλγοριθμική ↵

Παράδειγμα: $d=(1985, 132)$

$$1985 = 132 \cdot 15 + 5$$
$$(r_0) = r_1 \, q_1 + r_2$$

$$132 = 5 \cdot 26 + 2$$
$$(r_1) = r_2 \, q_2 + r_3$$

$$5 = 2 \cdot 2 + 1 \longrightarrow \text{ΜΚΔ}(1985, 132) = 1$$
$$(r_2) = r_3 \, q_3 + r_4$$

$$2 = 2 \cdot 1 + 0$$

Αν $d=(\alpha, b)$ τότε $\exists \; x, y \in \mathbb{Z}: d = \alpha x + by$

⊛ Πρόβλημα: Πώς βρίσκουμε τα x, y?

$$1 = 5 - 2 \cdot 2 = 5 - 2(132 - 5 \cdot 26) = -2 \cdot 132 + 53 \cdot 5 =$$

$$= -2 \cdot 132 + 53(1985 - 15 \cdot 132) = \underbrace{53}_{x} \cdot 1985 \underbrace{-797}_{y} \cdot 132$$

$$\Rightarrow 1 = 53 \cdot 1985 + (-797) \cdot 132$$

$$d = x \cdot \alpha + y \cdot b$$

Θεώρημα Lame: Ο αριθμός των διαιρέσεων που απαιτούνται στον αλγόριθμο του Ευκλείδη για την εύρεση του ΜΚΔ δύο αριθμών είναι μικρότερος ή ίσος από: 5·(πλήθος δεκαδικών ψηφίων του μικρότερου απ' τους δύο αριθμούς.

* Το 5 μπορεί να αντικατασταθεί απ' τον αριθμό

$\frac{\log 10}{\log \varphi} \simeq 4{,}785$, όπου $\varphi = \frac{1+\sqrt{5}}{2}$

↳ Επίσης ένα εναλλακτικό φράγμα είναι: $\frac{\log b}{\log \varphi} + 1$

όπου b: ο μικρότερος απ' τους 2 αριθμούς

* Άσκηση: Αν $\{F_n\}_{n \geq 1}$ = η ακολουθία Fibonacci

τότε $\forall n \geq 1 : (F_n, F_{n+1}) = 1$

Νδο: Το πλήθος των Ευκλείδειων Διαιρέσεων που απαιτούνται για την εύρεση του ΜΚΔ είναι ακριβώς n

Υπόδειξη: $F_{n+1} = F_n + F_{n-1}$

$F_n = F_{n-1} + F_{n-2}$

$\vdots$

• <u>Ελάχιστο Κοινό Πολλαπλάσιο</u>

Αν $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$. Ένας αριθμός k είναι κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \dots, \alpha_n \iff$

$k = \alpha_1 x_1, \dots, k = \alpha_n x_n, \quad x_1, x_2, \dots, x_n \in \mathbb{Z}$

$\iff \alpha_1 | k, \dots, \alpha_n | k$

Αν κάποια $\alpha_i = 0$, τότε κάθε κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \dots, \alpha_n$ θα είναι 0.

Συνεπώς, από τώρα και στο εξής θα υποθέτουμε ότι: $\alpha_1, \dots, \alpha_n \neq 0$

Ορισμός: Το ελάχιστο κοινό πολλαπλάσιο των $\alpha_1, \alpha_2, \dots, \alpha_n$ είναι ένας θετικός ακέραιος m, έτσι ώστε:

1) Αν $\alpha_1 | l, \dots, \alpha_n | l \Rightarrow m \leq l$

Έστω $S = \{k \in \mathbb{N} \mid k$: ακέραιο πολ/σιο των $\alpha_i, 1 \leq i \leq n\}$

$S \subseteq \mathbb{N}$ και $S \neq \emptyset$ διότι $|\alpha_1 \alpha_2 \cdots \alpha_n| \in S$

Από την (ΑΚΔ) $\Rightarrow \exists \min S$ και τότε προφανώς

$\min S =$ ελάχιστο κοινό πολ/σιο των $\alpha_1, \dots, \alpha_n$

Το (ΕΚΠ) των $\alpha_1, \dots, \alpha_n$ συμβολίζεται ως: $[\alpha_1, \dots, \alpha_n]$

Πρόταση: Έστω $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z} \setminus \{0\}$. Τότε

1) $m = [\alpha_1, \alpha_2, \dots, \alpha_n] \iff$ α) $\alpha_1 | m, \dots, \alpha_n | m$

β) Αν $\alpha_1 | \ell, \dots, \alpha_n | \ell \Rightarrow m | \ell$

{Η απόδειξη αφήνεται ως Άσκηση}

2) Αν $\lambda \in \mathbb{Z}$ τότε:

i) $[\alpha_1, \dots, \alpha_n] = [|\alpha_1|, \dots, |\alpha_n|]$

ii) $[\lambda\alpha_1, \dots, \lambda\alpha_n] = |\lambda| [\alpha_1, \dots, \alpha_n]$

iii) Αν $m = [\alpha_1, \dots, \alpha_n]$, τότε: $\left(\frac{m}{\alpha_1}, \dots, \frac{m}{\alpha_n}\right) = 1$

3) Αν $(\alpha_i, \alpha_j) = 1$, $1 \leq i \neq j \leq n$, τότε

$[\alpha_1, \dots, \alpha_n] = |\alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_n|$

4) Αν $n \geq 2$ και $1 \leq k \leq n-2$ τότε:

$[\alpha_1, \dots, \alpha_n] = [\alpha_1, \dots, \alpha_{k-1}, [\alpha_k, \dots, \alpha_n]]$

- Θεώρημα: Αν $\alpha, b \in \mathbb{Z} \setminus \{0\}$ τότε ισχύει:

$$(\alpha, b) \cdot [\alpha, b] = |\alpha \cdot b|$$

Απόδειξη: Επειδή $(\alpha, b) = (|\alpha|, |b|)$ και $[\alpha, b] = [|\alpha|, |b|]$

μπορούμε να υποθέσουμε ότι: $\alpha > 0$ και $b > 0$

1η Περίπτωση: Έστω ότι $(\alpha, b) = 1$. ΘΔο $[\alpha, b] = \alpha \cdot b$

Έστω ότι $m = [\alpha, b]$. Τότε: $\left.\begin{array}{l} \alpha \mid m \\ b \mid m \\ (\alpha, b) = 1 \end{array}\right\} \Rightarrow \alpha \cdot b \mid m \quad (1)$

Επειδή $\alpha \cdot b$ είναι κοινό πολλ/σιο των α, b θα έχουμε ότι: $m \mid \alpha b \quad (2)$

Από τις (1), (2) $\Longrightarrow m = [\alpha, b] = \alpha \cdot b$

2η Περίπτωση: Έστω $(\alpha, b) = d > 1$. ΘΔο: $(\alpha, b) \cdot [\alpha, b] = \alpha \cdot b$

$(\alpha, b) = d \Rightarrow \left(\frac{\alpha}{d}, \frac{b}{d}\right) = 1$. Τότε, θα έχουμε την 1η Περίπτωση, δηλαδή:

$$\left(\frac{\alpha}{d}, \frac{b}{d}\right) \cdot \left[\frac{\alpha}{d}, \frac{b}{d}\right] = 1 \cdot \frac{\alpha}{d} \cdot \frac{b}{d} \Rightarrow$$

$$\Rightarrow d\left(\frac{\alpha}{d}, \frac{b}{d}\right) d\left[\frac{\alpha}{d}, \frac{b}{d}\right] = d \cdot \frac{\alpha}{d} \cdot d\,\frac{b}{d} \Longrightarrow$$

$$\Rightarrow \left(d\,\frac{\alpha}{d}, d\,\frac{b}{d}\right)\left[d\,\frac{\alpha}{d}, d\,\frac{b}{d}\right] = \alpha \cdot b \Rightarrow$$

$$\Rightarrow (\alpha, b)[\alpha, b] = \alpha \cdot b$$

Έστω α, b. Τότε μπορούμε να γράψουμε

$\alpha = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $p_1, \ldots, p_k$, $i \neq j \Rightarrow p_i \neq p_j$

$\alpha_1, \ldots, a_k \geq 0$

$\beta_1, \ldots, \beta_k \geq 0$

$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$, $\gamma_i = \min\{\alpha_i, \beta_i\}$, $1 \leq i \leq k$

<u>Θεώρημα:</u> $[\alpha, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$, $\delta_i = \max\{\alpha_i, \beta_i\}$
$1 \leq i \leq k$

<u>Απόδειξη:</u> Θα έχουμε: $(\alpha, b)[\alpha, b] = \alpha \cdot b \Rightarrow$

$\Rightarrow p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k} \cdot [a,b] = p_1^{\alpha_1 + \beta_1} \cdots p_k^{\alpha_k + \beta_k} \Rightarrow$

$\Rightarrow [a,b] = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}$, $x_i = \alpha_i + \beta_i - \gamma_i =$
$= \alpha_i + \beta_i - \min\{\alpha_i, \beta_i\} =$
$= \max\{a_i, \beta_i\}$

Άρα, $[a,b] = p_1^{\max\{a_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}$