

Ευκλείδειος Αλγόριθμος • για την εύρεση του ΜΚΔ δύο αριθμών

Έστω $a, b \in \mathbb{Z}$, $b \neq 0$. Τότε: $a = bq + r$, όπου $0 \leq r < |b|$ και

$$(a, b) = (b, r)$$

Μπορείτε να υποθέσετε ότι $a, b > 0$. Θέτουμε: $r_0 = a$ $r_1 = b$

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

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

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

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

$$r_{n-1} = r_n q_n + \underbrace{r_{n+1}}_0$$

$$\text{Τότε } 0 < r_n < r_{n-1} < r_{n-2} < \dots < r_1$$

$$\text{Τότε: } (a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \dots$$
$$= \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n q_n, r_n)$$
$$= r_n(q_n, 1) = r_n$$

Άρα, ο ΜΚΔ των a, b συμπίπτει με το τελευταίο μη-μηδενικό υπόλοιπο στα Ευκλείδεια Αλγόριθμο. Αν $d = (a, b)$, τότε $\exists x, y \in \mathbb{Z}$: $d = ax + by$. Πρόβλημα: Πώς βρίσκουμε τα x, y ?

Παράδειγμα 1: $d = (39, 24)$

$$\begin{array}{llll} 39 & = & 24 \cdot 1 & + & 15 \\ r_0 & & r_1 q_1 & & r_2 \end{array}$$

$$\begin{array}{llll} 24 & = & 15 \cdot 1 & + & 9 \\ r_1 & & r_2 q_2 & & r_3 \end{array}$$

$$\begin{array}{llll} 15 & = & 9 \cdot 1 & + & 6 \\ r_2 & & r_3 q_3 & & r_4 \end{array}$$

$$\begin{array}{llll} 9 & = & 6 \cdot 1 & + & 3 \\ r_3 & & r_4 q_4 & & r_5 \end{array}$$

$$\begin{array}{llll} 6 & = & 3 \cdot 2 & + & 0 \\ r_4 & & r_5 q_5 & & r_6 \end{array}$$

$$\text{Άρα, ο ΜΚΔ } (39, 24) = 3$$

$$\text{Ψάχνουμε } x, y \in \mathbb{Z}: 3 = 39x + 24y$$

Αν τις διαδοχικές Ευκλείδειες Διακρίσεις, θα είχαμε

$$3 = 9 - 6 = 9 - (15 - 9) = -15 + 2 \cdot 9 = -15 + 2 \cdot (24 - 15) =$$
$$= -3 \cdot 15 + 2 \cdot 24 = -3(39 - 24) + 2 \cdot 24 = \underbrace{-3}_{x} 39 + \underbrace{5}_{y} 24$$

$$\text{Τότε: } 3 = \underbrace{(-3)}_{x} 39 + 24 \underbrace{(5)}_{y}$$

②

Παράδειγμα 2

$$d = (1985, 132)$$

$$1985 = 132 \cdot 15 + 5$$

$r_0 \quad r_1 \quad q_1 \quad r_2$

$$132 = 5 \cdot 26 + 2$$

$r_1 \quad r_2 \quad q_2 \quad r_3$

$$5 = 2 \cdot 2 + 1$$

$r_2 \quad r_3 \quad q_3 \quad r_4$

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

$r_3 \quad r_4 \quad q_4 \quad r_5$

$$\text{Άρα, } (1985, 132) = 1$$

$$\Psiάχνουμε $x, y \in \mathbb{Z}$: $1 = 1985 \cdot x + 132 \cdot y$$$

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

$$= -2 \cdot 132 + 53 \cdot 5 = \underline{53 \cdot 1985 - 797 \cdot 132}$$

$$= 1985 \cdot \underline{53} + 132 \cdot \underline{(-797)}$$

$$\text{Άρα, } 1 = \underline{53} \cdot 1985 - \underline{797} \cdot 132$$

Παρατήρηση: Το ζεύγος $x, y \in \mathbb{Z}$: $1985x + 132y = 1$, ΔΕΝ είναι μοναδικό, διότι για παράδειγμα: $x = 53 + 132 \cdot t$
 $y = -797 - 1985 \cdot t$, $t \in \mathbb{Z}$
 τότε: $1985x + 132y = 1$

Θεώρημα: [LAME]: Αν $a, b \in \mathbb{Z}$, όπου $a \geq b > 0$. Ο αριθμός των Ευκλείδειων Διαυρέσεων που απαιτούνται για την εύρεση του ΜΚΔ των a, b είναι μικρότερος ή ίσος από 5 φορές το πηλίκος των ψηφίων του μικρότερου από τους a, b

Παράδειγμα 3 (Ακ. Fibonacci): Θα περιγράψουμε τον Ευκλείδειο Αλγόριθμο για την εύρεση του ΜΚΔ: (f_{n+2}, f_{n+1})

$$f_{n+2} = f_{n+1} \cdot 1 + f_n$$

$r_0 \quad r_1 \quad q_1 \quad r_2$

$$f_{n+1} = f_n \cdot 1 + f_{n-1}$$

$r_1 \quad r_2 \quad q_2 \quad r_3$

$$f_4 = f_3 \cdot 1 + f_2$$

$$f_3 = f_2 \cdot 1 + f_1 = 2 \cdot f_1 + 0$$

Τότε: $(f_{n+2}, f_{n+1}) = f_2 = 1$ και το πηλίκος των απαιτούμενων Διαυρέσεων στον Ευκλείδειο Αλγόριθμο είναι ακριβώς η

Οσον Ευκλείδειο Αλγόριθμο

③

Ελάχιστο Κοινό Πολλαπλάσιο

Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Ο αριθμός $l \in \mathbb{Z}$ καλείται κοινό πολλαπλάσιο των $a_1, a_2, \dots, a_n \iff a_1 | l, a_2 | l, \dots, a_n | l$. Αν κάποιος $a_i = 0$, τότε επειδή $a_i | l \implies l = 0$. Τότε, ορίζουμε το ελάχιστο κοινό πολλαπλάσιο των $a_1, \dots, a_n$ να είναι το 0.

Από τώρα και στο εξής, θα υποθέτουμε ότι οι $a_i \neq 0, 1 \leq i \leq n$.

Θεωρούμε το σύνολο $S = \{l \in \mathbb{N} \mid l: \text{κοινό πολλαπλάσιο των } a_1, \dots, a_n\} \subseteq \mathbb{N}$. Τότε το $S \neq \emptyset$, διότι ο θετικός ακέραιος $|a_1 a_2 \dots a_n| \in S$. Αν' την $(AKA)_{\mathbb{N}}^S$ S έχει ελάχιστο στοιχείο $m = \epsilon_{KN}(a_1, a_2, \dots, a_n) = [a_1, a_2, \dots, a_n]$, το οποίο καλείται ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \dots, a_n$.

Επομένως: $m = [a_1, a_2, \dots, a_n] \iff$ ① $a_1 | m, \dots, a_n | m$
 ② $a_1 | l, \dots, a_n | l \implies \boxed{m \leq l}$

Θεώρημα: (Ιδιότητες $\in K\mathbb{N}$). Έστω $a_1, \dots, a_n \in \mathbb{Z}$, όπου $a_i \neq 0, 1 \leq i \leq n$.

1) $m = [a_1, a_2, \dots, a_n] \iff$ ① $a_1 | m, \dots, a_n | m$
 ② $a_1 | l, \dots, a_n | l \implies m | l$

2) $[a_1, a_2, \dots, a_n] = [|a_1|, |a_2|, \dots, |a_n|]$

3) $[ka_1, ka_2, \dots, ka_n] = |k| [a_1, a_2, \dots, a_n]$

4) Αν $m = [a_1, a_2, \dots, a_n] \implies a_1 | m, a_2 | m, \dots, a_n | m \implies \frac{m}{a_1}, \dots, \frac{m}{a_n}$ και τότε
 $(\frac{m}{a_1}, \dots, \frac{m}{a_n}) = 1$

5) $[a_1, \dots, a_n] = [a_1, \dots, a_k, [a_{k+1}, \dots, a_n]]$

6) Αν $(a_i, a_j) = 1, \forall i \neq j, 1 \leq i, j \leq n$, τότε: $[a_1, a_2, \dots, a_n] = |a_1 a_2 \dots a_n|$

Αποδείξεις: 1, 2, 3, 5, 6 $\rightarrow$ Αποδεικνύονται όμοια με τις διατάξεις του ΗΜ

Απόδειξη:

$$4) m = [a_1, a_2, \dots, a_n] \Rightarrow a_1 | m, \dots, a_n | m \Rightarrow \frac{m}{a_1}, \dots, \frac{m}{a_n} \in \mathbb{Z} \text{ κι έστω } d = \left(\frac{m}{a_1}, \dots, \frac{m}{a_n}\right)$$

$$\text{Τότε: } d \mid \frac{m}{a_1}, \dots, d \mid \frac{m}{a_n} \Rightarrow \exists c_1, \dots, c_n \in \mathbb{Z} : \frac{m}{a_1} = dc_1, \dots, \frac{m}{a_n} = dc_n \Rightarrow$$

$$\Rightarrow m = da_1, c_1 = da_2 c_2 = \dots = da_n c_n \Rightarrow da_1 | m, \dots, da_n | m \xrightarrow{\text{Θ1)}} [da_1, \dots, da_n] | m$$

$$\xrightarrow{3)} d[a_1, \dots, a_n] | m \Rightarrow dm | m \Rightarrow dm \leq m \Rightarrow \boxed{d=1}$$

Θεώρημα: Αν $a, b \in \mathbb{Z}, a, b \neq 0$, τότε: $[a, b] \cdot (a, b) = |ab|$

Απόδειξη: Επειδή $[a, b] = [|a|, |b|]$ και $(a, b) = (|a|, |b|)$ και μπορούμε να υποθέσουμε ότι $a, b \in \mathbb{N}$. Θέτουμε $d = (a, b)$.

Τότε: $d|a, d|b \Rightarrow d|a \cdot b \Rightarrow \frac{ab}{d} \in \mathbb{Z}$. Θέτουμε $m = \frac{ab}{d}$.

$$\text{Θ5.2: } m = [a, b]$$

① $a|m$, διότι: $m = \frac{ab}{d} = a \cdot \frac{b}{d}$ και $\frac{b}{d} \in \mathbb{Z}$, διότι $d|b$. Ανάλογα $b|m$, καθώς $m = \frac{ab}{d} = b \cdot \frac{a}{d}$ και $\frac{a}{d} \in \mathbb{Z}$, διότι $d|a$.

$$\text{② Έστω } \left. \begin{matrix} a|l \\ b|l \end{matrix} \right\} \xrightarrow{\text{Θ4.5.2}} \underline{m|l} \xrightarrow{\text{Θ5.2}} \frac{ab}{d} | l \iff \frac{l}{\frac{ab}{d}} \in \mathbb{Z} \iff \frac{l \cdot d}{ab} \in \mathbb{Z}$$

$$\text{Επειδή, } d = (a, b) \Rightarrow \exists x, y \in \mathbb{Z} : d = ax + by. \text{ Άρα } \frac{ld}{ab} = \frac{l(ax+by)}{ab} =$$

$$= \frac{la}{ab}x + \frac{lb}{ab}y = \frac{lx}{b} + \frac{ly}{a}. \text{ Τότε επειδή } \left. \begin{matrix} a|l \\ b|l \end{matrix} \right\} \Rightarrow \frac{l}{a} \in \mathbb{Z} \wedge \frac{l}{b} \in \mathbb{Z} \Rightarrow \frac{lx}{b} + \frac{ly}{a} \in \mathbb{Z} \text{ (ως 2 φορές ακέραια)}$$

$$\text{Άρα } \frac{ld}{ab} \in \mathbb{Z}, \text{ οπότε } m = \frac{ab}{d} = [a, b]$$

Θεώρημα: Αν $a, b \in \mathbb{N}$ και: $a = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}, b = p_1^{b_1} \cdot \dots \cdot p_k^{b_k}, a_i, b_i \geq 0$

$$\text{Τότε } [a, b] = p_1^{\max\{a_1, b_1\}} \cdot \dots \cdot p_k^{\max\{a_k, b_k\}}$$