

26/03/15

ΕΥΚΛΕΙΔΕΙΟΣ ΑΛΓΟΡΙΘΜΟΣ

Έστω $a, b \in \mathbb{Z}$ και έστω $b \neq 0$.

ΠΡΟΒΛΗΜΑ: Πώς μπορούμε να βρούμε τον ΜΚΔ $d = (a, b) =$;

ΛΗΜΜΑ: Έστω $a, b \in \mathbb{Z}$ $b \neq 0$. Τότε αν'υπν ευκλείδεια διαίρεση

$$\exists! (q, r) \in \mathbb{Z}^2: a = b \cdot q + r, q \in \mathbb{Z}, 0 \leq r < |b|$$

Τότε $(a, b) = (b, r)$

Απόδειξη: Έστω $d = (a, b)$ κ' $\delta = (b, r)$.

$$d = (a, b) \Rightarrow \left\{ \begin{array}{l} d \mid a \\ d \mid b \Rightarrow d \mid 9 \cdot b \end{array} \right\} \Rightarrow d \mid b \cdot 9 - a = r \Rightarrow \boxed{d \mid r}$$

$$\text{Άρα } \boxed{d \mid (b, r) = \delta} \quad (1)$$

$$\delta = (b, r) \Rightarrow \left\{ \begin{array}{l} \delta \mid b \\ \delta \mid r \end{array} \right\} \Rightarrow \delta \mid b \cdot 9 \Rightarrow \delta \mid (b \cdot 9 - r) = a \Rightarrow \boxed{\delta \mid a}$$

$$\text{Άρα } \boxed{\delta \mid d} \quad (2)$$

$$\Rightarrow (1), (2) \Rightarrow \boxed{\delta = d}$$

Έστω $a, b \in \mathbb{Z}$ κ' $b \neq 0$. Επειδή $(a, b) = (|a|, |b|)$

Αρα χωρίς βλάβη ως γενικότητας μπορούμε να υποθέσουμε
ότι $a, b \geq 0$, κ' επίσης μπορούμε να υποθέσουμε ότι $a \geq b > 0$.

Τότε $a = b \cdot q + r$, $0 \leq r < b$.

Θέτουμε $a = r_0$, $b = r_1$, $q = q_1$, $r = r_2$.

Τότε $r_0 = r_1 \cdot q_1 + r_2$ με $0 \leq r_2 < r_1$

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

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

$\vdots$

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

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

$\vdots$

Επειδή: ~~απειροστική~~

$\dots < r_{n+1} < r_n < r_{n-1} < \dots < r_3 < r_2 < r_1$

Επειδή $r_i \in \mathbb{N} \Rightarrow \exists k \in \mathbb{N} : r_k = 0$.

Χωρίς βλάβη ως γενικότητας έστω $k = n+1$.

Τότε $r_{n+1} = 0$

Από το "ΛΗΜΜΑ": $d_{\text{opp}}(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \dots =$
 $= (r_{n-1}, r_n) = r_n$ διότι από τη

σχέση $r_{n-1} = r_n \cdot q_n$ (χρ' $r_{n+1} = 0$) $\Rightarrow$ το r_n διαιρεί τον $r_{n-1} \Rightarrow$
 $\Rightarrow (r_{n-1}, r_n) = r_n$

Επειδή το r_n είναι το τελευταίο μη-μηδενικό υπόλοιπο $\Rightarrow$
 $\Rightarrow$ ο ΜΚΔ 2 ακεραίων αριθμών είναι το τελευταίο
μη-μηδενικό υπόλοιπο στις διαδοχικές ευκλείδειες διαίρεσεις
~~των~~ των αριθμών.



Έστω $a, b \in \mathbb{Z}$, $b \neq 0$ κ' $d = (a, b)$. Τότε $\exists x, y \in \mathbb{Z}$:

$$d = ax + by$$

ΠΡΟΒΛΗΜΑ: Πώς βρίσκουμε 2 x, y ;

$$d = r_{\text{max}} = r_{n-2} - r_{n-1} \cdot q_{n-1} =$$

$$= r_{n-2} - q_{n-1} (r_{n-3} - r_{n-2} \cdot q_{n-2}) =$$

$$= (1 + q_{n-1} \cdot q_{n-2}) r_{n-2} - q_{n-1} \cdot r_{n-3} = \dots =$$

$$= r_0 \cdot x + r_1 \cdot y, \quad r_0 = a, r_1 = b$$

Παράδειγμα: ~~Παράδειγμα~~ $d = (1985, 132) = x \cdot 1985 + y \cdot 132$
 (*) Τα x, y δεν είναι υποχρεωτικό να είναι

$\overbrace{1985}^{r_0} = \overbrace{132}^{r_1} \cdot \overbrace{15}^{q_1} + \overbrace{5}^{r_2}$ (τονάδικα!)

$\overbrace{132}^{r_1} = \overbrace{5}^{r_2} \cdot \overbrace{26}^{q_2} + \overbrace{2}^{r_3}$

$\overbrace{5}^{r_2} = \overbrace{2}^{r_3} \cdot \overbrace{2}^{q_3} + \overbrace{1}^{r_4}$ → ΜΚΔ!

$\overbrace{2}^{r_3} = \overbrace{2}^{q_4} \cdot \overbrace{1}^{r_4} + \overbrace{0}^{r_5}$

Άρα $d = (1985, 132) = 1$.
 $d = 1 = 5 - 2 \cdot 2 =$
 $= 5 - 2 \cdot (132 - 5 \cdot 26) =$
 $= -2 \cdot 132 + 5 \cdot 53 =$
 $= (1985 - 15 \cdot 132) - 132 \cdot 2 =$
 $= \underbrace{1985}_{\alpha} - \underbrace{53}_{\chi} + \underbrace{132}_{\beta} \underbrace{(-2)}_{\gamma}$

Θεώρημα Lame: Ο αριθμός των διαμέτρων οι οποίες αναρρώνει για την εύρεση του ΜΚΔ 2 αριθμών με χρήση του Ευκλείδειου Αλγόριθμο $\leq 5k$ (όπου $k = 20$ η μέγιστος των ψηφίων του μικρότερου από τους 2.)

$\frac{\log 10}{\log \phi}$, όπου $\phi = \frac{1+\sqrt{5}}{2}$ περίπου ~ 4.785 .

Παράδειγμα: Θεωρούμε την ακολουθία Fibonacci: $F_1=1, F_2=1, F_3=2$
 και $F_n = F_{n-1} + F_{n-2}, \forall n \geq 3$.

Τότε $(F_{n+2}, F_{n+1}) = 1 \quad \forall n \geq 0$.

Πόση: Έστω $d = (F_{n+2}, F_{n+1}) \Rightarrow \begin{cases} d \mid F_{n+2} = F_{n+1} + F_n \\ d \mid F_{n+1} \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} d \mid F_n \\ d \mid F_{n+1} \end{cases} \Rightarrow \dots \Rightarrow \begin{cases} d \mid F_2 \\ d \mid F_1 \end{cases} \Rightarrow \boxed{d=1}$

$F_{n+2} = 1 \cdot F_{n+1} + F_n$
 $F_{n+1} = 1 \cdot F_n + F_{n-1}$
 $\vdots$



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

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

Οι διακρίσεις που αναζητούμε είναι ακριβώς $n < 5n$.

Έστω ότι $d_1, \dots, d_n$ με $d_i \neq 0, \forall i=1, \dots, n$.

$$\begin{aligned} d &= (d_1, \dots, d_n) = \left(\frac{(d_1, d_2)}{d_1}, d_3, \dots, d_n \right) = \\ &= \left(\frac{(d_1, d_3)}{d_2}, d_4, \dots, d_n \right) = \dots = (d_{n-2}, d_n). \end{aligned}$$

Παράδειγμα : $d_1 = 112, d_2 = 96, d_3 = 24$.

$$\begin{aligned} &\quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\ &\quad \quad \quad (24) \neq \quad 3 \cdot (23) \quad 3 \cdot (23) \leftarrow \\ &(112, 96, 24) = (16, 24) = 8 \end{aligned}$$

Αν $d = d_1 x_1 + \dots + d_n x_n$
όπου $x_i \in \mathbb{Z}$

Ελάχιστο Κοινό Πολλαπλάσιο (ΕΚΠ)

Έστω $d_1, \dots, d_n \in \mathbb{Z}$. Τότε ο αριθμός $m \in \mathbb{Z}$ είναι κοινό πολλαπλάσιο των $d_1, \dots, d_n$ ($\Rightarrow d_i | m, \dots, d_n | m$)

Αν κάποιο $d_i = 0, \forall i=1, \dots, n$ τότε $m = d_i \cdot x = 0 \cdot x = 0$
(εξαρτημένη περίπτωση).

Από δω και εφεξής υποθέτουμε ότι $d_i \neq 0, \forall i=1, \dots, n$.

Πορίσμα : Το ελάχιστο κοινό πολλαπλάσιο (ΕΚΠ) των $d_1, \dots, d_n$ είναι ένας θετικός ακέραιος m :

- ① m : κοινό πολλαπλάσιο των $d_1, \dots, d_n$ δηλ $d_i | m, \dots, d_n | m$
- ② l : $-||-$: $d_i | l, \dots, d_n | l \Rightarrow \boxed{l \geq m}$.

Υπάρχει ΕΚΔ των $d_1, \dots, d_n$:

$$\text{Έστω } S = \{k \in \mathbb{N} \mid d_1 \mid k, \dots, d_n \mid k\}$$

Τότε $S \neq \emptyset$ διότι ο αριθμός $|d_1 d_2 \dots d_n| \in S$
Από ~~από~~ (ΑΚΛ) $\Rightarrow S$ έχει ελάχιστο στοιχείο m .
κ' προφανώς το m είναι το (ΕΚΔ) των $d_1, \dots, d_n$.

Συμμεταβολή: $\text{ΕΚΔ}(d_1, \dots, d_n) = [d_1, \dots, d_n]$

$\longleftrightarrow$

Βασικές ιδιότητες ΕΚΔ $d_1, \dots, d_n \in \mathbb{Z} \setminus \{0\}$.

$$(1) \quad m = [d_1, \dots, d_n] \Leftrightarrow \begin{cases} d_1 \mid m, \dots, d_n \mid m \\ d_1 \mid l, \dots, d_n \mid l \end{cases} \Rightarrow \frac{m \mid l}{\Rightarrow m \leq l}$$

($\Leftarrow$) η ανισότητα είναι άφρον διότι αν $m \mid l \Rightarrow m \leq l$.

($\Rightarrow$) Έστω $m = [d_1, \dots, d_n]$ κ' έστω $d_1 \mid l, \dots, d_n \mid l \Rightarrow$
 $\Rightarrow m \leq l$. Εφαρμόζοντας διαίρεση του l

με το m : $l = m \cdot q + r, \quad 0 \leq r < m$

Τότε l, m είναι κοινά πολλαπλαζ των $d_1, \dots, d_n$

$$d_i \mid l, d_i \mid m, \forall i=1, \dots, n \Rightarrow d_i \mid l \quad \xrightarrow{d_i \mid m \cdot q} d_i \mid m \cdot q$$

$$\Rightarrow d_i \mid r, \forall i=1, \dots, n \Rightarrow r \in S \Rightarrow r \in S$$

$$r < m = [d_1, \dots, d_n] = \min S \Rightarrow$$

$$\Rightarrow \text{Από } r=0 \Rightarrow \boxed{r=0}$$

(2) Αν $d_1, \dots, d_n \in \mathbb{Z} \setminus \{0\}, \lambda \in \mathbb{Z} \setminus \{0\}$. Τότε

$$(a) \quad [d_1, \dots, d_n] = [|d_1|, \dots, |d_n|]$$

$$(b) \quad [\lambda d_1, \dots, \lambda d_n] = |\lambda| [d_1, \dots, d_n]$$

$$(c) \quad [d_1, \dots, d_n] = m \Rightarrow \left(\frac{m}{d_1}, \dots, \frac{m}{d_n} \right) = 1$$

$$(d) \quad \text{Θέτουμε } d(\frac{m}{d_1}, \dots, \frac{m}{d_n}) \Rightarrow d \mid \frac{m}{d_1}, \dots, d \mid \frac{m}{d_n} \Rightarrow$$

$$\Rightarrow \exists c_1, \dots, c_n \in \mathbb{Z} : \frac{m}{d_1} = d \cdot c_1, \dots, \frac{m}{d_n} = d \cdot c_n \Rightarrow$$

$$\Rightarrow m = d c_1 d_1, \dots, m = d c_n d_n \Rightarrow$$

$$\Rightarrow \text{to nu eivai koivo no2/610} \Rightarrow \text{Toke } [d, d_1, \dots, d_n] \mid m \Rightarrow$$

$$\Rightarrow d [d_1, \dots, d_n] \mid m \Rightarrow d \cdot m \mid m \Rightarrow$$

$$\Rightarrow d m \leq m \Rightarrow d \leq 1 \Rightarrow \boxed{d=1}$$

$m \in \mathbb{N} \quad d \in \mathbb{N}$

③ Av $m > 2$, tote: $[d_1, \dots, d_n] = [d_1, \dots, d_r, [d_{r+1}, \dots, d_n]]$

④ Av $(d_i, d_j) = 1 \quad 1 \leq i \neq j \leq n$, tote $[d_i, d_j] = |d_i \cdot d_j|$
 $\text{Enn } [d_1, \dots, d_n] = |d_1 \cdot \dots \cdot d_n|$

$\longleftarrow$

④ Essee $a, b, c \in \mathbb{N}$ k' $(b, c) = 1$. Tote av $b \mid a$ k' $c \mid a \Rightarrow$
 $\Rightarrow b \cdot c \mid a$

$$\begin{array}{l} a = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \\ b = p_1^{b_1} \cdot \dots \cdot p_k^{b_k} \\ c = p_1^{r_1} \cdot \dots \cdot p_k^{r_k} \end{array} \quad \left| \quad d_i, b_i, r_i \geq 0, \forall i=1, \dots, k. \right.$$

$$bc = p_1^{b_1+r_1} \cdot \dots \cdot p_k^{b_k+r_k} \mid a = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \Rightarrow b_i + r_i \leq \alpha_i \quad \forall i=1, \dots, k$$

$$1 = (b, c) = p_1^{\min\{b_1, r_1\}} \cdot \dots \cdot p_k^{\min\{b_k, r_k\}} \Rightarrow$$

$$\Rightarrow \min\{b_i, r_i\} = 0, \forall i=1, \dots, k.$$

Av $\min\{b_i, r_i\} = \underset{=0}{b_i} \Rightarrow b_i + r_i = r_i \leq \alpha_i$ siota $c \mid a$

$\min\{b_i, r_i\} = r_i \Rightarrow b_i + r_i = b_i \leq \alpha_i$ siota $b \mid a$

$$\Rightarrow \boxed{b_i + r_i \leq \alpha_i, \forall i=1, \dots, k.}$$

Θεωρημα: Av $a, b \in \mathbb{Z} \setminus \{0\}$. Tote $(a, b) [a, b] = |a \cdot b|$

Απόδειξη: ① $\forall \text{noD. ou } (a, b) = 1$. Tote d.d.o.
 $[a, b] = |a \cdot b|$

Essee $m = [a, b] \Rightarrow a \mid m$ k' $b \mid m \Rightarrow \boxed{|a \cdot b| \mid m} \quad (*)$
 $(a, b) = 1$

Οπως $a \mid m$ k' $b \mid m$
 $\text{και } m \mid ab \Rightarrow \boxed{m \mid |a \cdot b|} \quad (b)$

Από $(a)(b)$ έχουμε ότι $|ab| = m$.

② (Πρώτη Παρατήρηση) : Έστω $d = (a, b) \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1 \Rightarrow$

$$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) \cdot \left[\frac{a}{d}, \frac{b}{d}\right] = \left|\frac{a \cdot b}{d^2}\right| \Rightarrow$$

$$\Rightarrow d \left(\frac{a}{d}, \frac{b}{d}\right) \cdot d \cdot \left[\frac{a}{d}, \frac{b}{d}\right] = d^2 \cdot \frac{|ab|}{d^2} \Rightarrow$$

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

$$\Rightarrow \boxed{(a, b) \cdot [a, b] = |a \cdot b|}$$

—

Θεώρημα : Έστω $a, b \in \mathbb{N}$. Έστω $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$
 $b = p_1^{\beta_1} \dots p_k^{\beta_k}$

όπου $\alpha_i, \beta_i \geq 0 \quad \forall i=1, \dots, k$.

Τότε $[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} \dots p_k^{\max\{\alpha_k, \beta_k\}}$

Απόδειξη : $(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_k^{\min\{\alpha_k, \beta_k\}}$
 $\text{έστω } a \cdot b = p_1^{\alpha_1 + \beta_1} \dots p_k^{\alpha_k + \beta_k}$

$[a, b] = p_1^{\gamma_1} \dots p_k^{\gamma_k}$. Ο.δ.ο. $\gamma_i = \max\{\alpha_i, \beta_i\}, \forall i=1, \dots, k$.

Είναι : $(a, b) \cdot [a, b] = a \cdot b \Rightarrow$

$$\Rightarrow p_1^{\min\{\alpha_1, \beta_1\}} \dots p_k^{\min\{\alpha_k, \beta_k\}} \cdot p_1^{\gamma_1} \dots p_k^{\gamma_k} = p_1^{\alpha_1 + \beta_1} \dots p_k^{\alpha_k + \beta_k} \Rightarrow$$

$$\Rightarrow p_1^{\gamma_1 + \min\{\alpha_1, \beta_1\}} \dots p_k^{\gamma_k + \min\{\alpha_k, \beta_k\}} = p_1^{\alpha_1 + \beta_1} \dots p_k^{\alpha_k + \beta_k}$$

Αρκεί να δείξουμε : $\gamma_i = \alpha_i + \beta_i - \min\{\alpha_i, \beta_i\} = \max\{\alpha_i, \beta_i\}, \quad 1 \leq i \leq k$

Όπως $\max\{\alpha_i, \beta_i\} \begin{cases} \rightarrow = \alpha_i \Rightarrow \min\{\alpha_i, \beta_i\} = \beta_i \text{ τότε} \\ \rightarrow = \beta_i \Rightarrow \min\{\alpha_i, \beta_i\} = \alpha_i \end{cases}$

$$\begin{cases} \max\{\alpha_i, \beta_i\} = \alpha_i + \beta_i - \min\{\alpha_i, \beta_i\} \\ \rightarrow = \beta_i \Rightarrow \min\{\alpha_i, \beta_i\} = \alpha_i + \beta_i - \beta_i = \alpha_i \end{cases}$$

Άρα $\forall i=1, \dots, k : \max\{\alpha_i, \beta_i\} = \alpha_i + \beta_i - \min\{\alpha_i, \beta_i\} = \gamma_i$

$\forall i=1, \dots, k$ ισχύει το ζητούμενο, $\gamma_i = \max\{\alpha_i, \beta_i\}$

Der 16x05 n geraden von pro-education Beispiel
8n) $(\alpha_1, \alpha_2, \alpha_3) \cdot [\alpha_1, \alpha_2, \alpha_3] \neq \alpha_1 \cdot \alpha_2 \cdot \alpha_3$.