Επειδή $\varepsilon_i = \min(a_i, a_i')$ και
$\varepsilon_i' = \max(a_i, a_i')$ έχουμε

αν $a_i \leq a_i' \Rightarrow \varepsilon_i = a_i$ και $\varepsilon_i' = a_i'$

$$[a,b](a,b) = p_1^{\varepsilon_1'} \cdot p_2^{\varepsilon_2'} \cdots p_t^{\varepsilon_t'} \cdot p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} =$$

$$= p_1^{a_1} \cdots p_t^{a_t} \cdot p_1^{a_1'} \cdots p_t^{a_t'}$$ από το

$$= a \cdot b.$$

1/11/2016

ΜΚΔ $a, b \in \mathbb{Z}$ με $a^2+b^2 > 0$
$(a,b) = \delta \in \mathbb{N}$ ώστε $\delta | a$ και b (***)
ΕΚΠ αν $\gamma | a$ και b
$\gamma | \delta$

$a, b \in \mathbb{Z}^*$ $[a,b] = \varepsilon$ ώστε
$a, b | \varepsilon$ και
αν $a, b | m \Rightarrow \varepsilon \leq m$

Τα κοινά πολλαπλάσια των a και b είναι ακριβώς τα πολλαπλάσια του $[a,b]$.
Οι κοινοί διαιρέτες των a και b είναι οι διαιρέτες του (a,b)

$$a \cdot b = [a,b](a,b)$$

Θεώρημα

Αν $a, b \in \mathbb{Z}^*$ και $\delta = (a,b)$ τότε υπάρχουν ακέραιοι x και y ώστε $\boxed{\delta = ax + by}$.

Απόδειξη

Ορίζουμε το σύνολο

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}$$

$S \cap \mathbb{N}^* \subseteq \mathbb{N} \Rightarrow$ έχει ελάχιστο στοιχείο.

Το ελάχιστο στοιχείο $n = ax_0 + by_0$ (+) για κάποια x_0 και y_0 θα δείξουμε ότι είναι το δ.

Υποθέτουμε ότι $n \nmid a \Rightarrow a = n\pi + u$, $0 < u < a$ $\Rightarrow u = a - n \cdot \pi \overset{+}{\Rightarrow}$

$\Rightarrow u = a - (ax_0 + by_0)\pi =$

$= a(1 - x_0\pi) - by_0 n \in S$

και $u > 0$

άρα $u < n$ ελάχιστο

αδύνατο

άρα $n \mid a$ και με τον ίδιο τρόπο $n \mid b \xRightarrow{(+++)} n \mid \delta$

$$\left.\begin{array}{l} \delta \mid a \Rightarrow \delta \mid a \cdot x_0 \\ \delta \mid b \Rightarrow \delta \mid by_0 \end{array}\right\} \Rightarrow \delta \mid ax_0 + by_0 = n$$

$\Rightarrow n = \delta$

Πως θα τον βρούμε;;

Θεώρημα

Έστω $a, b > 1$

Τότε $a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$ με $p_1 < p_2 < \dots < p_n$ πρώτοι και $k_i > 0$

$b = q_1^{m_1} \cdot q_2^{m_2} \cdots q_l^{m_l}$ με $q_1 < q_2 < \dots < q_l$ πρώτοι και $m_i > 0$

Επίσης μπορούν να γραφούν χρησιμοποιώντας κοινούς πρώτους με μηδενικούς εκθέτες αν χρειάζονται ως εξής: Θεωρούμε όλους τους πρώτους μέχρι τον μεγαλύτερο που υπάρχει στον a ή b.

$a = r_1^{a_1} r_2^{a_2} \cdots r_t^{a_t}$ $\quad r_1 < r_2 < \dots < r_t$ πρώτοι

$b = r_1^{a_1'} \cdot r_2^{a_2'} \cdots r_t^{a_t'}$ $\quad a_i, a_i' \geq 0$

$(a,b) = r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_t^{\gamma_t}$ με $\gamma_i = \min(a_i, a_i')$

$[a,b] = r_1^{\gamma_1'} \cdot r_2^{\gamma_2'} \cdots r_t^{\gamma_t'}$ με $\gamma_i' = \max(a_i, a_i')$

π.χ. $a = 2^3 5^7 \cdot 11 \cdot 13^9 \cdot 23 = 2^3\, 3^0\, 5^7\, 7^0\, 11^1\, 13^9\, 17^0\, 19^0\, 23^1$

$b = 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 17^5 = 2^0\, 3^2\, 5^6\, 7^3\, 11^2\, 13^0\, 17^5\, 19^0\, 23^0$

$(a,b) = 2^0 \cdot 3^0 \cdot 5^6\, 7^0 \cdot 11^1 \cdot 13^0\, 17^0\, 19^0\, 23^0 \Leftrightarrow \boxed{(a,b) = 5^6 \cdot 11}$

κοινοί πρώτοι στη μικρότερη δύναμη

$[a,b] = 2^3 \cdot 3^2 \cdot 5^7 \cdot 7^3 \cdot 11^2 \cdot 13^9 \cdot 17^5 \cdot \cancel{19^0} \cdot 23^1$

κοινοί και μη κοινοί στη μεγαλύτερη δύναμη.

(Να μπορώ να τις αποδείξω, τουλάχιστον τις αρχικές.)

Ιδιότητες ΜΚΔ ΕΚΠ

Αρχικά $a, b \in \mathbb{Z}^*$

1) $(a,b) = (|a|, |b|)$ $\quad [a,b] = [|a|, |b|]$

Αρκεί λοιπόν να τους βρίσκουμε για φυσικούς

αν $(a,b) = |a|$ τότε $b = a\cdot\gamma \Leftrightarrow [a,b] = |b|$

2) $(\gamma a, \gamma b) = |\gamma| (a,b)$

$[\gamma a, \gamma b] = |\gamma| [a,b]$

3) Αν $\gamma | (a,b)$ τότε $\left(\frac{a}{\gamma}, \frac{b}{\gamma}\right) = \frac{(a,b)}{|\gamma|}$

Αν $\gamma = (a,b)$ τότε $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \frac{(a,b)}{(a,b)} = 1$

4) $(a,b) = (a, b+\kappa a)$ $\quad \kappa \in \mathbb{Z}$

5) Αν $\underset{6}{\gamma} | \underset{2}{a}\underset{3}{b} \Rightarrow \underset{6}{\gamma} | \underset{(2,6)}{(a,\gamma)} \underset{(3,6)}{(b,\gamma)} \Rightarrow \gamma | (a,\gamma) b$ και $\gamma | a (b,\gamma)$

Αν $\gamma | ab$ και $(\gamma, a) = 1$ τότε $\gamma | b$

6) $(a, b\gamma) = (a, (a,b)\gamma)$

7) Αν $(a,b) = 1$ και $\gamma | a$ τότε $(\gamma, b) = 1$

8) Αν $(a,b) = 1$ και $\underset{6|6}{a|\gamma}$, $\underset{3|6}{b|\gamma}$ τότε $ab|\gamma$

$\not\Leftarrow$ $\quad 6\cdot 3 \nmid 6$ γιατί 6,3 δεν είναι πρώτοι μεταξύ τους.

9) Αν $(a,b) = 1$ τότε $(a, b, \gamma) = (a,\gamma)(b,\gamma)$

$[a,b,\gamma] = [a,\gamma][b,\gamma]$

$(16, 24) = (24, 16)$

$24 = 16 \cdot 1 + 8 \Rightarrow 8 = 24 - 16 \cdot 1$

$\boxed{16} = 8 \cdot 2 + 0$

$112 - 96 = 16 = 8 \cdot 2$

$24 = 16 \cdot 1 + 8 \Rightarrow 8 = 24 - 16 \Rightarrow$

$\Rightarrow 8 = 24 - (112 - 96) = -\underset{x}{112} + \underset{y}{96} + \underset{z}{24}$

άρα $x = -1$, $y = 1$ και $z = 1$.

Να βρεθεί $(1985, 132) = x1985 + y132$

$$1 = 5 - 2\cdot 2 = 5 - (132 - 5\cdot 26)\cdot 2 =$$
$$= 5 - 132\cdot 2 + 5\cdot 52 =$$
$$= -132\cdot 2 + 5\cdot 53 =$$
$$= -132\cdot 2 + (1985 - 132\cdot 15)\cdot 53 =$$
$$= -132\cdot 2 + 1985\cdot 53 - 132\cdot 15\cdot 53$$
$$= 1985\cdot 53 - 132(2 + 15\cdot 53)$$

$x = 53$ και $y = -(2 + 5\cdot 53)$

Να βρεθούν ακέραιοι x, y ώστε $1 = 1985x + 132y$

$$540 \,|\, \underline{66}$$
$$12 \,|\, 8$$

$(540, 66) = 540x + 66y$

$540 = 66\cdot 8 + 12 \rightarrow 12 = 540 - 8\cdot 66$

$66 = 12\cdot 5 + 6 \rightarrow 6 = 66 - 12\cdot 5$

$12 = 2\cdot 6$

$$= 66 - 5(540 - 8\cdot 66) =$$
$$= 66 - 5\cdot 540 + 40\cdot 66$$
$$= 41\cdot 66 - 5\cdot 540$$

$x = -5 \quad y = 41$

$(540, 66) = 6$

Πως ο υπολογιστής υπολογίζει τον ΜΚΔ; $a > b > u$

Με τον Ευκλείδιο αλγόριθμο

<u>Λήμμα</u>

Έστω $\alpha, b \in \mathbb{Z}$ με $b \neq 0$. Αν u είναι το υπόλοιπο της διαίρεσης $a = bn + u$ με $0 \leq u \leq |b|$ τότε $(a,b) = (b,u)$

<u>Απόδειξη</u>

Θεωρούμε ότι $a, b \in \mathbb{N}$ με $b \geq 1$ $\quad (a,b) = (|\alpha|, |b|)$

Έστω $\delta = (\alpha, b)$ και $\delta' = (b,u)$. Πρέπει $\delta = \delta'$

$$\left.\begin{array}{l} \delta \mid a \\ \delta \mid b \Rightarrow \delta \mid n \cdot b \end{array}\right\} \Rightarrow \begin{array}{l} \delta \mid a - \pi b = u \\ \delta \mid b \text{ και } \delta \mid u \Rightarrow \delta \mid (b,u) = \delta' \ (+) \text{ Θέλουμε } \delta' = \delta \end{array}$$

$$\left.\begin{array}{l} \delta' \mid b \Rightarrow \delta' \mid bn \\ \delta' \mid u \ ; \ \delta' \mid u \end{array}\right\} \Rightarrow \delta' \mid bn + u = a$$

$$\left.\begin{array}{l} \delta' \mid a \\ \delta' \mid b \end{array}\right\} \Rightarrow \delta' \mid (\alpha, b) = \delta \ (++)$$

Από $(+)$ και $(++)$ $\Rightarrow \delta = \delta'$

<u>Π.χ</u> Να βρεθεί $(1985, 132)$

$$\begin{array}{ll} 1985 = 132 \cdot 15 + 5 & \Rightarrow (1985, 132) = (132, 5) \\ 132 = 5 \cdot 26 + 2 & \Rightarrow (132, 5) = (5, 2) \\ 5 = 2 \cdot 2 + \boxed{1} & \Rightarrow (5, 2) = (2, 1) = 1 \\ 2 = 1 \cdot 2 + 0 & \end{array}$$

άρα $(1985, 132) = (132, 5) = (5, 2) = (2, 1) = 1$.

Αλγόριθμος του Ευκλείδη

Εύρεση του ΜΚΔ (a,b)

$a = b\pi_0 + \upsilon_0 \to$ είναι $\upsilon_0 = 0 \Rightarrow (a,b) = b$
$\searrow$ όχι $0 < \upsilon_0 < |b| = b$

$b = \upsilon_0 \pi_1 + \upsilon_1 \to$ είναι $\upsilon_1 = 0 \Rightarrow (b, \upsilon_0) = \upsilon_0$
$\searrow$ όχι $0 < \upsilon_1 < \upsilon_0$

$\upsilon_0 = \upsilon_1 \pi_2 + \upsilon_2 \to \upsilon_2 = 0 \quad (\upsilon_0, \upsilon_1) = \upsilon_1$
$\searrow$ όχι $0 < \upsilon_2 < \upsilon_1 < \upsilon_0 < b$

Επειδή η ακολουθία
$b \to \upsilon_0 \to \upsilon_1 \to \upsilon_2 \to \dots$ είναι γνησίως φθίνουσα
θα έχουμε ότι κάποτε θα γίνει μηδέν

$\upsilon_\kappa = \upsilon_{\kappa+1}\pi_{\kappa+2} \Rightarrow (\upsilon_\kappa, \upsilon_{\kappa+1}) = \upsilon_{\kappa+1}$

Σύμφωνα με το προηγούμενο λήμμα έχουμε ότι
$(a,b) = (b, \upsilon_0) = (\upsilon_0, \upsilon_1) = (\upsilon_1, \upsilon_2) = \dots = (\upsilon_\kappa, \upsilon_{\kappa+1}) = \upsilon_{\kappa+1}$

π.χ. Να βρεθούν οι ακέραιοι x, y και z με
$(112, 96, 24) = 112x + 96y + 24z$

$((112, 96), 24) = (112, 96, 24)$

$(112, 96)$
$112 = 96 \cdot 1 + 16$
$96 = 16 \cdot 6 + 0 \Rightarrow (96, 16) = (112, 96) = 16$

$(112, 96) = \boxed{16} = 112 - 96$