

Εύρεση: Διαιρείς το n με τους πρώτους $\leq \sqrt{n}$

και αν διαιρείται γραφείς τη δύναμήν εις την οποία διαιρείται και να μην διαιρείται από άλλη μεγαλύτερη

$$n = 2^3 \cdot 3 \cdot 5^2 \cdot 11^{100}$$

$$2 | n$$

$$2 | n/2$$

$$2 | n/4$$

$$2 | n/8$$

Ποιος είναι μεγαλύτερος;

$$n' = 2^3 \cdot 5^2 \cdot 11^{100}$$

$$m = 2 \cdot 3^3 \cdot 7^2 \cdot 17$$

Καλό είναι να χρησιμοποιήσουμε τους ίδιους πρώτους

$$n' = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^{100} \cdot 17^0$$

$$m = 2 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 17$$

ΜΚΔ - ΕΚΠ

Πρόβλημα:

Μας δίνουν κανονικούς αριθμούς και μας ζητούν να βρούμε όλους τους διαυρέτες και όλα τα πολλαπλασιαστικά

Τα πολλαπλασιαστικά του m στο προηγούμενο π.χ

$$m = 2 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 17$$

Τα ελάχιστα κοινά πολλαπλασιαστικά του n' με το m στο προηγούμενο παράδειγμα είναι:

αν έχουμε τα σύνολα

$$\{a \cdot 2 \cdot 3^2 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 17 \mid a \in \mathbb{Z}^*\} \text{ και } \{b \cdot 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^{100} \cdot 17^0 \mid b \in \mathbb{Z}^*\}$$

το σύνολο των ΕΚΠ των δυο συνόλων περιγράφεται ως εξής:

$$\{x \cdot \text{ΕΚΠ}[n, m] \mid x \in \mathbb{Z}^* \text{ και } x \leq \text{από τα κοινά πολλαπλασιαστικά}\}$$

Οεδομένους τους κοινούς διαυρέτες των n και m . Αυτό το σύνολο είναι γενεραστικό.

Επειδή το 1 είναι ο μικρότερος κοινός διαυρέτης, αρκεί να βρούμε τον μέγιστο κοινό διαυρέτη.

ΟΡΙΣΜΟΣ:

Εστω $a, b \in \mathbb{Z}^*$. Ο ΜΚΔ των a, b συμβολίζεται με (a, b) και είναι ο θετικός αλγεαίος δ ώστε

1) $\delta \mid a$ και $\delta \mid b$

2) Αν $\gamma \mid a$ και $\gamma \mid b$ τότε $\gamma \mid \delta$

Δηλ ο δ είναι ο μεγαλύτερος

π.χ.

$$(14, 35) = 7, \quad (-14, 35) = 7, \quad (14, -35) = 7, \quad (-14, -35) = 7.$$

ηx

$$(u^2+1, (u+1)^2+1) = \delta$$

$$\left. \begin{array}{l} \delta \mid u^2+1 \\ \delta \mid (u^2+1)+1 \end{array} \right\} \left. \begin{array}{l} \delta \mid u^2+1 \\ \delta \mid u^2+2u+2 \end{array} \right\} \delta \mid [u^2+2u+2 - u^2-1] \Rightarrow$$

$$\Rightarrow \delta \mid 2u+1$$

$$\text{Άρα, } \left. \begin{array}{l} \delta \mid 2u+1 \\ \delta \mid u^2+1 \end{array} \right\} \left. \begin{array}{l} \delta \mid (2u+1)^2 \\ \delta \mid 4(u^2+1) \end{array} \right\} \delta \mid [(2u+1)^2 - 4(u^2+1)] \Rightarrow$$

$$\Rightarrow \delta \mid 4u-3$$

$$\text{Άρα, } \left. \begin{array}{l} \delta \mid 4u-3 \\ \delta \mid 2(2u+1) \end{array} \right\} \delta \mid [4u+2 - 4u+3] \Rightarrow \delta \mid 5$$

$$\text{Άρα } \delta = 1 \text{ ή } \delta = 5$$

ΟΡΙΣΜΟΣ: Έστω $a, b \in \mathbb{Z}^*$. Το ΕΚΚ των a, b συμβολίζεται με $[a, b]$ και είναι ο ελάχιστος ε , ώστε:

- 1) $a \mid \varepsilon$ και $b \mid \varepsilon$
- 2) Αν $a \mid \gamma$ και $b \mid \gamma$, τότε $\varepsilon \mid \gamma$

Πx

$$[10, 13] = 130, [10, -13] = 130$$

$$[10, 26] = 130$$

Παρατήρηση!

δινομένων ημερών

$$[10, 13] = [2 \cdot 5, 13] = 2 \cdot 5 \cdot 13 = 130$$

$$[10, 26] = [2 \cdot 5, 2 \cdot 13] = 2 \cdot 5 \cdot 13 = 130$$

ΘΕΩΡΗΜΑ:

Έστω $a, b \in \mathbb{Z}^*$

- 1) Τα κοινά πολλαπλασιαστικά των a, b είναι ακριβώς τα πολλαπλασιαστικά του $[a, b]$
- 2) Οι κοινοί διαιρέτες των a, b είναι ακριβώς οι διαιρέτες του (a, b)

ΑΠΟΔΕΙΞΗ

1) Έστω γ ένα κοινό πολλαπλασιαστικό των a, b

~~Ή~~ $\gamma = a \cdot a'$ και $\gamma = b \cdot b'$

Υποθέτουμε ότι γ όχι πολλαπλασιαστικό του $[a, b] = \varepsilon$

Άρα, $\gamma = \varepsilon\eta + \upsilon$, $0 < \upsilon < \varepsilon$

$$\begin{array}{l} a/\gamma \\ a/\varepsilon \end{array} \left\{ \begin{array}{l} \Rightarrow a/\varepsilon\eta + \upsilon - \varepsilon\eta = \upsilon \\ \end{array} \right.$$

το ίδιο για το b
δηλαδή b/υ

$$a/\gamma = \varepsilon\eta + \upsilon$$

$$a/\varepsilon\eta$$

Άρα, το υ είναι κοινό πολλαπλασιαστικό των a, b και $\upsilon < \varepsilon = [a, b]$

Άρα, ε/γ

2) Έστω $\delta = (a, b)$ και για ενώ γ/δ

θέλουμε γ/δ . Υποθέτουμε ότι $\gamma \nmid \delta$

Άρα, $\exists$ πρώτος p ώστε p/γ και $p \nmid \delta$

$a = \delta a'$ και $b = \delta b'$ και επίσης

$\delta \nmid \gamma$ πρώτος q ώστε q/a' και b'

γιατί τότε ο δq θα διαιρούσε τα a & b

$$\begin{array}{l} p/\gamma \Rightarrow p/a \text{ και } p \nmid \delta \\ \Rightarrow p/b \end{array} \left| \begin{array}{l} a = \delta a' \\ b = \delta b' \end{array} \right.$$

$$\begin{array}{l} p/a = \delta a' \\ p \nmid \delta \end{array} \left\{ \Rightarrow p/a' \text{ και } \right. \quad \left. \begin{array}{l} p/b = \delta b' \\ p \nmid \delta \end{array} \right\} \Rightarrow p/b'$$

Βρίσκουμε λοιπόν πρώτο p ώστε $p|a'$ και $p|b'$

Αρα, $\delta p|a$ και β αδύνατον γιατί ο α μέγιστος

$\delta = (a, \beta)$, $\alpha = \delta a'$ και $\beta = \delta b'$ ώστε a' και b'

έχουν μόνο α $\perp$ σαν κοινό διαιρέτη

Παύ αν είχαν έναν πρώτο p διαιρέτη, τότε

$\delta p = (a, \beta)$ Αδύνατον

ΠΡΟΤΙΕΝΑ:

Εστω $a, b \in \mathbb{Z}^*$ τότε $[a, b] = \frac{|a| \cdot |b|}{(a, b)} \Leftrightarrow |a| \cdot |b| = [a, b] \cdot (a, b)$

ΑΠΟΔΕΙΞΗ

Γράψουμε τους a, b σαν γινόμενα των ανελύκων

χρησιμοποιώντας κοινούς πρώτους όπου κανονισ

δων χρειάζεται και είναι υψηλότερος στη ιεραρχία

$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$, $1 \leq p_1 < \dots < p_r$ πρώτοι

$b = p_1^{k'_1} \cdot p_2^{k'_2} \cdot \dots \cdot p_r^{k'_r}$, $0 \leq k_i$, k_i φυσικοί

Τότε τον τυχαίο $p_i^{k_i}$ και $p_i^{k'_i}$

$\min(k_i, k'_i)$ και $\max(k_i, k'_i)$

Αν $\min(k_i, k'_i) = k'_i \Rightarrow \max(k_i, k'_i) = k_i$

Αρα, $p_i^{k_i} \cdot p_i^{k'_i} = p_i^{\min(k_i, k'_i)} \cdot p_i^{\max(k_i, k'_i)}$

Εστω $\delta = p_1^{\min(k_1, k'_1)} \cdot \dots \cdot p_r^{\min(k_r, k'_r)}$

και $\varepsilon = p_1^{\max(k_1, k'_1)} \cdot \dots \cdot p_r^{\max(k_r, k'_r)}$

Επειδή, $p_i^{k_i} \geq p_i^{\min(k_i, k'_i)} \Rightarrow \delta | a$ και β

$p_i^{k_i} \geq \dots$

$p_i^{k_i} \leq p_i^{\max(k_i, k'_i)} \Rightarrow a$ και β / ε

$p_i^{k_i} \leq \dots$

Αρκεί να το δ $\max$ και το ε $\min$.

Αν δ όχι $\max$ τότε θα υπήρχε πρώτος p_j ώστε

το $p_j | (a, b)$ και $p_j \nmid \delta$. Τότε, το

$p_j^{\min(k_j, k'_j)} | \delta$ και $p_j \nmid \delta$ και $p_j | a$ και β

Αν $\min(k_i, k_i') = 0$

Τότε αν $k_i = 0 \Rightarrow p_i | a$ Αποδο

Επίσης, θεωρούμε ελάχιστο

Εστω ε' ώστε a/ε' και b/ε' και $\varepsilon' < \varepsilon$

Αφού ο a/ε' & $b/\varepsilon' \Rightarrow p_i^{\max(k_i, k_i')} | \varepsilon'$, $\forall i$.

Αφού $p_i^{\max(k_i, k_i')} | \varepsilon'$ τότε για όλα τα i

και $p_i \neq p_j$ πρώτοι θα έχουμε:

$$p_1^{\max(k_1, k_1')} \dots p_r^{\max(k_r, k_r')} | \varepsilon' \Rightarrow$$

$\Rightarrow \varepsilon | \varepsilon'$ και $\varepsilon' < \varepsilon$ Αδυνατούν.

$$|a| \cdot |b| = (p_1^{k_1} \dots p_r^{k_r}) \cdot (p_1^{k_1'} \dots p_r^{k_r'})$$

$\forall i$: $\min(k_i, k_i')$ θα είναι ένας από τους δύο

και ο άλλος θα είναι $\max(k_i, k_i')$; Άρα:

$$(p_1^{k_1} \dots p_r^{k_r}) / (p_1^{k_1'} \dots p_r^{k_r'}) = \delta, \varepsilon$$

Προσοχή: αυτό δεν σημαίνει ότι $\delta = p_1^{k_1} \dots p_r^{k_r}$

Θεώρημα (Bezout)

Εστω $a, b \in \mathbb{Z}^*$

Τότε υπάρχουν αριθμοί x, y ώστε $(a, b) = x \cdot a + y \cdot b$

(δηλ. ο ΜΚΔ γράφεται ως γραμ. συνδυασμός των a, b)

Απόδειξη

Θεωρούμε σύνολο $S = \{ax + by \in \mathbb{N}^* \mid x, y \in \mathbb{Z}\}$

Εστω $b \neq 0$ τότε:

$$ax < \begin{cases} a < 0, x < 0 \\ a > 0, x > 0 \end{cases}$$

Αντίστοιχο

Με την αρχή της ναυαγής διατάξης, το S έχει ελάχιστο

$\min S = u$ όπου $(a, b) = \delta$ και $\delta = u$

Για το u $\exists x_0, y_0$ ώστε $u = ax_0 + by_0$

θεωρούμε $u | a$ και $u | b$

Εστω ότι $u \nmid a \rightarrow a = u\pi + v$, $0 < v < u$

$$0 < v = a - u\pi = a - (ax_0 + by_0)\pi =$$

$$= a - x_0 \cdot a\pi - b y_0 \pi = a(1 - x_0\pi) + b(-y_0\pi) \in S$$

$u \leq v \leq u$ Αδύνατον

Αρα, το u/a και για τον ίδιο λόγο u/b

Αρα, ο u/d (γιατί οι κοινοί διαιρέτες των a, b διαιρούν το ΜΚΔ)

Αλλά d/a και $b \Rightarrow d/ax_0$ & $by_0 \Rightarrow d/y$

Τελικά u/d και $d/y \Rightarrow d=u$

Ορισμός: Έστω $a, b \in \mathbb{Z}^*$. Θα λέμε ότι οι a, b είναι πρώτοι μεταξύ τους ή πρώτοι προς αλλήλους αν $(a, b) = 1$

Πχ

Αν έχουμε δύο αριθμούς με 120 ψυχία ομαθεύει και είναι γινόμενα δύο πρώτων συνιστωσών με 63 ψυχία ομαθεύει, τότε ο υπολογιστής θα δει 40×10^3 χρόνια για να βρει το ΜΚΔ. Με το θεώρημα Bezout θα το βρούμε άμεσα.

Ιδιότητες ΜΚΔ και ΕΚΠ

Έστω $a, b \in \mathbb{N}^*$

1) $(a, b) = a \Leftrightarrow b = a \cdot x \Leftrightarrow [a, b] = b$

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

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

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

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

5) Αν $\gamma | a \cdot b$, τότε το $\gamma | (a, r) \cdot (b, r) \Rightarrow$

$\Rightarrow \gamma | (a, r) \cdot b$ ή $\gamma | a \cdot (b, r)$

Αν $\gamma | a \cdot b$ και $(a, r) = 1 \Rightarrow \gamma | b$

6) $(a, b \cdot r) = (a, (a, b) \cdot r)$

$$7) \text{ Αν } (a, \beta) = 1 \text{ και } \gamma | a \Rightarrow (\beta, \gamma) = 1$$

$$8) \text{ Αν } (a, \beta) = 1 \text{ και } a, \beta | \gamma \text{ τότε } a \cdot \beta | \gamma$$

$$9) \text{ Αν } (a, \beta) = 1, \text{ τότε } (a\beta, \gamma) = (a, \beta) \cdot (a, \gamma).$$

$$\text{και } [a\beta, \gamma] = [a, \beta] \cdot [\beta, \gamma]$$

$$10) \text{ Αν } (a, \beta) = 1 \text{ και } \gamma | a \cdot \beta \text{ με } \gamma > 0$$

$$\text{τότε } \exists! \delta_1 \text{ και } \delta_2 \text{ ώστε } \gamma = \delta_1 \cdot \delta_2 \text{ και } \delta_1 | a \text{ \& } \delta_2 | \beta.$$

ΛΗΜΜΑ:

Έστω $a, b \in \mathbb{Z}$ με $b \neq 0$

Αν $a = bn + u$ με $0 \leq u < |b|$, τότε ο ΜΚΔ

$$(a, b) = (b, u), \quad u = a - bn.$$

Απόδειξη

Είναι η (4) ιδιότητα

ΕΥΚΛΕΙΔΕΙΟΣ ΑΛΓΟΡΙΘΜΟΣ

Θεωρούμε $(a, b) =$

$(a, b) = (|a|, |b|)$. Αρα θεωρώ ότι οι αριθμοί μου

είναι φυσικοί. Κάποιοι είναι μεγαλύτεροι

$$a = a_0 > b = a_1$$

$$(a_0, a_1) \quad a_0 = a_1 \pi_1 + u_1, \quad 0 \leq u_1 < a_1$$

Σύμφωνα με την ιδιότητα 4 η το ίδιο

$$(a_0, a_1) = (a_1, u_1) = (u_1, u_2) = (u_2, u_3) = \dots = (u_k, u_{k+1})$$

$$a_0 = a_1 \pi_1 + u_1, \quad 0 \leq u_1 < a_1$$

$$a_1 = u_1 \pi_2 + u_2, \quad 0 \leq u_2 < u_1$$

$$u_1 = u_2 \pi_3 + u_3, \quad 0 \leq u_3 < u_2$$

$$\vdots$$

$$u_k = u_{k+1} \pi_{k+1} + u_{k+2}, \quad u_{k+2} = 0 \text{ ή } 1$$

$$\text{Όταν έχουμε } (u_k, u_{k+1}) = (u_{k+1} \pi_{k+1}, u_{k+1}) = u_{k+1}$$

nx 1

$$(2015, 130) = (130, 65) = (2 \cdot 65, 65) = 65$$

$$2015 = 130 \cdot 15 + 65$$

$$130 = 65 \cdot 2 + 0$$

nx 2

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

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

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

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

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