

Όλες οι μεταθέσεις είναι $\frac{n!}{(n-k)!}$

Ένας συνδυασμός μας δίνει $k!$ μεταθέσεις.

Άρα το πλήθος των συνδυασμών είναι $\frac{n!}{k!}$

$$\frac{(n-k)!}{k!} = \frac{n!}{(n-k)! \cdot k!} = \binom{n}{k}$$

Θεώρημα: Κάθε $n \geq 1$ φυσικός, έχει έναν πρώτο διαμέρη.

Θεώρημα (Ευκλείδης): Υπάρχουν άπειροι πρώτοι.

Απόδειξη: Έστω ότι υπάρχουν πεπερασμένοι πρώτοι

$p_1, p_2, \dots, p_k$.

Υποθέτουμε: Τον: $p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Αν δείξαμε ότι είναι πρώτος, θα είχαμε άτονο.

Υποθέτουμε ότι δεν είναι. Άρα είναι σύνθετος.

Άρα διαμερίζεται από πρώτο p_i .

$$p_i / p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$$

$$p_i / p_i \Rightarrow p_i / p_1 \cdot p_2 \cdot \dots \cdot p_k$$

$$\text{Άρα ο } p_i \text{ διαμερίζει } p_1 \cdot \dots \cdot p_{k+1} - p_1 \cdot \dots \cdot p_k = 1 \Rightarrow p_i / 1$$

Άτονο

Θεώρημα: Κάθε φυσικός $a > 1$ σύνθετος, έχει τουλάχιστον ένα πρώτο διαμέρη $\leq \sqrt{a}$.

Απόδειξη: Έστω $a = bc$ με $1 < b, c < a$.

Έστω $c \leq b$ (το εντάξαμε).

$$c^2 \leq b \cdot c = a \Rightarrow$$

$$c \leq \sqrt{a}$$

Πρόταση: $[a, b] = \frac{|a| \cdot |b|}{(a, b)}$, or $ab \neq 0$

$$H' a, b = |a| |b|.$$

Απόδειξη: $|a| \cdot |b| = p_1^{k_1+m_1} \dots p_l^{k_l+m_l}$

Επίσης έχουμε $(a, b)(a, b) = p_1^{k_1+m_1} \dots p_l^{k_l+m_l}$.

$$k_i + m_i = \min(k_i, m_i) + \max(k_i, m_i)$$

Αν $k_i \leq m_i \Rightarrow \min(k_i, m_i) = k_i$ και $\max(k_i, m_i) = m_i$.

Αρα ισχύει.

Πρόταση: Έστω $a, b \in \mathbb{Z}^*$. Τότε τα κοινά πολλαπλασια των a και b , είναι τα πολλαπλασια του $[a, b] = \frac{ab}{(a, b)}$.

Οι κοινοί διαιρετές των a και b είναι οι διαιρετές του $(a, b) \cdot n$.

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

Απόδειξη. Με την αρχή της κοινής διαίρεσης

$$S = \{ |ax + by|, ax + by \in \mathbb{N}^+ \text{ και } x, y \in \mathbb{Z}^* \}$$

Το S έχει ελάχιστο στοιχείο το n . Δηλαδή $\exists x_0 \text{ και } y_0$ ώστε $n = ax_0 + by_0$.

$$\delta / a \text{ και } b \Rightarrow \delta / ax_0 \text{ και } by_0 \Rightarrow \delta / n. (*)$$

Έστω ότι $a = nq + u$ με $0 < u < n$
ή $u < a$

$$v = a - un$$

$$\text{αφού } \delta | a \text{ και } \delta | n \Rightarrow \delta | a \text{ και } \delta | un \Rightarrow \delta | v$$

$$v = a - un = a - ax_0 - by_0 = a(1 - x_0) - by_0$$

$v \in S$ και η μικρότερο και $v \in n$. Αδυνατά. Αρα $n | a$.

Με τον ίδιο τρόπο, $n | b$. Αρα $n | \delta$.

(*) Τελικά $\delta = n$. Αρα υπάρχουν αριθμοί x_0 και y_0 μη μηδενικοί ώστε

$$\delta = ax_0 + by_0$$

Η πρόταση δεν μας λέει πώς να βρούμε τα x_0 και y_0 .

ΙΔΙΟΤΗΤΕΣ ΕΚΔ ΚΑΙ ΝΚΔ

$$a, b \in \mathbb{Z}^*$$

$$1) (a, b) = (|a|, |b|)$$

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

$$\text{Αν } (a, b) = |a| \Rightarrow b \text{ πολλαπλασιάζει το } |a|$$

$$\text{Αν } [a, b] = |b| \Rightarrow a \text{ πολλαπλασιάζει το } |b|$$

$$\text{Αν } (a, b) = [a, b] \Rightarrow |a| = |b|$$

$$2)^* (ga, gb) = |g|(a, b)$$

$$[ga, gb] = |g|[a, b]$$

$$3)^* \text{Αν } g | (a, b) \Rightarrow \left(\frac{a}{g}, \frac{b}{g} \right) = \frac{(a, b)}{|g|} \quad \text{και}$$

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

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

$$5) \text{ Αν } \gamma | a \cdot b \text{ τότε } \gamma | (a, \gamma)(b, \gamma) \Rightarrow \gamma | (a, \gamma) \cdot b \text{ ή } \gamma | (b, \gamma)$$

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

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

$$8) \text{ Αν } (a, b) = 1 \text{ και } a/\gamma, b/\gamma \Rightarrow a \cdot b/\gamma$$

$$9)^* (a, b)^n = (a^n, b^n)$$

$$10)^* a/b \Leftrightarrow a^n/b^n$$

$$\delta = (a, b) \Rightarrow \exists x, y \in \mathbb{Z}^* \text{ με } \delta = ax + by$$

Πως θα βρούμε το δ ?

ΛΗΜΜΑ $\rightarrow$ Έστω $a, b \in \mathbb{Z}^*$

Αν u είναι το υπόλοιπο της διαίρεσης a δια b : $a = bn + u$

με $0 \leq u < |b|$ τότε $(a, b) = (b, u)$

$$\text{Απόδειξη: } (a, b) = (bn + u, b) = (bn + u - bn, b) = (u, b)$$

Από Λήμμα (4) $\nearrow$

Εύρεση του ΜΚΔ (a, b) με τον αλγόριθμο του Ευκλείδη.

Θέσουμε να βρούμε τον (a_0, a_1) με $a_0 \geq a_1 > 0$.

$$a_0 = a_1 \cdot n_1 + a_2 \text{ με } a_2 \geq 0 \text{ και } a_2 < a_1$$

$$(a_0, a_1) = (a_1, a_2)$$

$$a_1 = a_2 n_2 + a_3 \text{ με } 0 \leq a_3 < a_2$$

$$(a_0, a_1) = (a_1, a_2) = (a_2, a_3)$$

Συνεχίζοντας με αυτόν τον τρόπο, θα έχουμε ότι:

$$a_0 \geq a_1 > a_2 > a_3 > \dots > a_{k+1} > 0$$

Αρα, θα έχουμε:

$$a_{k-1} = a_k n_k + a_{k+1} \text{ και } a_{k+1} = 0$$

Αρα a_{k-1} διαιρείται από a_k .

$$(a_0, a_1) = (a_1, a_2) = \dots = (a_{k-1}, a_k) = a_k$$

$\uparrow$ ιδιότητα (1)

$$\text{π.χ. } (2015, 130) = 65 = 2015x + 130y$$

$$\begin{matrix} 2015 & = & 130 \cdot 15 & + & 65 \\ a_0 & & a_1 & & a_2 \end{matrix}$$

$$\begin{array}{r} 2015 \overline{) 130} \\ \underline{715} \\ 585 \\ \underline{585} \\ 0 \end{array}$$

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

$$(2015, 130) = (130, 65) = 65$$

$$2015 = 130 \cdot 15 + 65 \Rightarrow 65 = 2015 \overset{x=1}{\cdot 1} - 130 \cdot \overset{y=-15}{15}$$

$$130 = 65 \cdot 2$$

$$65 = 1 \cdot 2015 + (-15) \cdot 130$$

$$n.x. (1985, 132) = (132, 5) = (5, 2) = 1$$

$$\begin{array}{r|l} 1985 & 132 \\ 0662 & 15 \\ \hline 005 & \end{array}$$

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

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

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

$$5 = 2 \cdot 2 + (1) \quad (1 = \text{MKA})$$

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

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

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

$$53 \cdot 15 = 795$$

$$= (1985 - 132 \cdot 15) 53 - 132 \cdot 2 = 1985 \cdot 53 - 132 \cdot 797$$

$$x = 53 \text{ και } y = -797$$

$$17.x. (n^2+1, (n+1)^2+1) = (n^2+1, (n+1)^2+1 - (n^2+1))$$

$$= (n^2+1, 2n+1) = \cancel{(n^2+1 - n(2n+1), 2n+1)}$$

$$\cancel{(2-n, 2n+1)} = 2(n^2+1) - n(2n+1) = 2 - n =$$

$$= (2-n, 2n+1) = (4-2n+2n+1, 2n+1) = (5, 2n+1) = 1 \text{ ή } 5$$

γιατί μόνο αυτοί διαρούν το 5.

$$(5, 2 \cdot 1 + 1) = (5, 3) = 1 \quad (5, 2 \cdot 2 + 1) = 5$$