25/10/2016

Μεταθέσεις κ στοιχείων από n στοιχεία

$$M(n,k) = \frac{n!}{(n-k)!}$$ Προσοχή στη διάταξη.

Συνδυασμός κ στοιχείων από n στοιχεία

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$ όχι διάταξη

Εφαρμογή

$$(a+b)^n = \sum_{i=0}^{n} \overset{\text{συνδυασμοί}}{\binom{n}{i}} a^i b^{n-i}$$

$$(a-b)^n = (a+(-b))^n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} a^i b^{n-i}$$

$$2^n = (1+1)^n = \sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}$$

$$0 = (1-1)^n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots + (-1)^n \binom{n}{n}$$

Έστω $n=2t$: $\binom{n}{0} + \binom{n}{2} + \dots + \binom{n}{n} = \binom{n}{1} + \binom{n}{3} + \dots + \binom{n}{n-1}$

Παρατήρηση : $\binom{p}{i}$, p πρώτος $0 \le i \le p$

$\binom{p}{0} = 1 = \binom{p}{p}$ $\quad 0 < i < p \Rightarrow \binom{p}{i} = \frac{p!}{i!\,(p-i)!} = p \cdot A.$

Ευκλείδης: Υπάρχουν άπειροι πρώτοι.

Πρωταρχική Ανάλυση:

$n \in \mathbb{N}^*$ $n > 1$ Μοναδικά

$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ ώστε $p_1 < p_2 < \dots < p_m$ και $k_i > 0$

(*) **Θεώρημα Gauss**

Ένα κανονικό n-γωνο κατασκευάζεται γεωμετρικά (με κανόνα και διαβήτη) αν και μόνο αν οι περιττοί πρώτοι διαιρέτες του n είναι διακεκριμένοι πρώτοι τύπου Fermat.

→ **Πρώτοι του Fermat**

$F_k = 2^{2^k} + 1$, αν είναι πρώτος

Οι μοναδικοί πρώτοι γνωστοί τύπου Fermat

$F_0 = 3$ $F_1 = 5$ $F_2 = 17$ $F_3 = 257$ $F_4 = 65537$

$F_5 = 4.294.967.297 = 641 \cdot 6700417$

Σύμφωνα με τον Gauss δεν υπάρχει κανονικό 7-γωνο.

→ **Πρώτοι του Mersenne**

Αν ο αριθμός $2^p - 1$ είναι πρώτος για p πρώτος, θα καλείται πρώτος του Mersenne

Μπορεί ο $2^{ab} - 1$ να είναι πρώτος;

Λύση: Όχι: διότι $2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \dots + 1\right)$

γινόμενο

(*) Να βρεθεί ο μικρότερος πρώτος p ώστε 2^p-1 όχι πρώτος.

Πρόταση

Υπάρχουν άπειροι πρώτοι μορφής $4k+3$ και $4k+1$

Απόδειξη

Ας υποθέσουμε ότι έχουμε πεπερασμένο πλήθος πρώτων αριθμών μορφής

$4k+3$: $\underset{p_1=3}{4k_1+3}, \underset{p_2}{4k_2+3}, \ldots, \underset{p_n}{4k_n+3}$

Ο φυσικός

$4p_2p_3\ldots p_n+3$ → πρώτος αδύνατον απο την υπόθεση
ή
→ $\boxed{\text{σύνθετος}}$ (=) διαιρείται τουλάχιστον απο 2 πρώτους.

Υποθέτουμε ότι ο ένας από αυτούς είναι κάποιος από $p_1, \ldots, p_n$

Αν $\left.\begin{array}{l} p_1=3 \mid 4p_1p_2\ldots p_n+3 \\ 3\mid 3 \end{array}\right\} \Rightarrow 3\mid 4p_2\ldots p_n \Rightarrow$
$\Rightarrow 3\mid 4$ ή $3\mid p_i$ αδύνατο

άρα, το $3 \nmid 4p_2\ldots p_n+3$

Αν $\left.\begin{array}{l} p_i \mid 4p_2\ldots p_n+3 \\ p_i \mid p_i \Rightarrow p_i\mid 4p_2 \end{array}\right\}$ $p_i \mid 3$ αδύνατο γιατί p_i πρώτος και μεγαλύτερος του 3.

Άρα, ο $4p_2 \cdots p_n + 3$ διαιρείται μόνο από πρώτους μορφής $4k+1$

$$4p_2 \cdots p_n + 3 = (4l_1+1)(4l_2+1)\cdots(4l_m+1)$$
$$4p_2 \cdots p_n + \cancel{3}_{2} = 4 \cdot A \cancel{+1}$$

$$4p_2 \cdots p_n - 4A = -2$$
$$4(p_2 \cdots p_n - A) = -2 \quad \text{αδύνατο}$$
γιατί $4 \times (\text{κάτι}) =$ δεν κάνει -2

Μ.Κ.Δ. Ε.Κ.Π.

Έστω $a, b \in \mathbb{Z}$ με $a^2+b^2 > 0$ (όχι $a = b = 0$)

Γνωρίζουμε ότι κάθε ακέραιος έχει πεπερασμένο πλήθος διαιρετών.

Άρα, και το πλήθος των κοινών διαιρετών θα είναι πεπερασμένο μεταξύ a και b.

<u>Ορισμός</u>

Έστω $a, b \in \mathbb{Z}$ με $a^2+b^2 > 0$. Ο Μέγιστος Κοινός Διαιρέτης των a και b συμβολίζεται με (a,b) και είναι ο θετικός ακέραιος δ ώστε:

1) $\delta | a$ και $\delta | b$
2) Αν $\gamma | a$ και $\gamma | b \Rightarrow \gamma | \delta$

Άρα $(a,b) = \delta$ είναι μέγιστος με αυτήν την ιδιότητα.

<u>π.χ</u> $(14, -35) = (14, 35) = (-14, -35) = 7$.

Ορισμός

Έστω $a, b \in \mathbb{Z}^*$. Το Ελάχιστο Κοινό Πολλαπλάσιο των a και b συμβολίζεται με $[a,b] = \varepsilon$ και έχει τις εξής ιδιότητες:

1) a και $b | \varepsilon$
2) Αν $a|m$ και $b|m \Rightarrow \varepsilon \leq m$

Π.χ. $[10, 130] = [-10, 130] = [10, -130] = 130$

$[-6, 20] = 60$

Π.χ $a = 2 \cdot 3^5 \cdot 11^4 \cdot 17$
$b = 3^4 \cdot 11^3 \cdot 13^2 \cdot 17^5$

$(a,b) = 3^4 \cdot 11^3 \cdot 17$
$[a,b] = 2 \cdot 3^5 \cdot 11^4 \cdot 13^2 \cdot 17^5$

Θεώρημα

Έστω $a, b \in \mathbb{Z}^*$.

1) Τα κοινά πολλαπλάσια των a και b είναι ακριβώς τα πολλαπλάσια του $[a,b] = \varepsilon$
2) Οι κοινοί διαιρέτες των a και b είναι ακριβώς οι διαιρέτες του $(a,b) = \delta$

Έστω $\varepsilon = [a,b] =$ ΕΚΠ (*)
Έστω m κοινό πολλαπλάσιο (**) των a και b με $\varepsilon \nmid m \Rightarrow$
$\Rightarrow m = \pi\varepsilon + \upsilon$ με $0 < \upsilon < \varepsilon$

$\upsilon = m - \pi\varepsilon$.

Άρα, $a, b | \varepsilon$ λόγω (*) και $a, b | m$ λόγω (**).
Δηλαδή, $a, b | \upsilon$ και $\upsilon < \varepsilon$.

αδύνατον

2) $\delta = (\alpha, \beta)$ και υποθέτουμε ότι $\exists\ \gamma$ με $\gamma | \alpha$ και $\gamma | \beta$

Θέλουμε $\gamma | \delta \Leftrightarrow \delta = \gamma \gamma'$

Υποθέτουμε ότι $\gamma \nmid \delta$. Σίγουρα υπάρχει πρώτος $p | \gamma$ και $p \nmid \delta$.

$\delta = (\alpha, \beta) \Rightarrow \delta | \alpha$ και $\delta | \beta$

$\alpha = \delta \cdot \alpha'$ και $\beta = \delta \cdot \beta'$.

$$\left.\begin{array}{l} p | \gamma,\ \gamma | \alpha \Rightarrow p | \alpha = \delta \cdot \alpha' \\ p \nmid \delta \end{array}\right\} \Rightarrow p | \alpha' \quad (+++)$$

Το ίδιο $p | \beta'$ $(++++)$

$(+++)$ και $(++++)$ $\Rightarrow \alpha = \delta p \alpha''$ και $\beta = \delta p \beta''$

Έχουμε $\delta p | \alpha$ και $\delta p | \beta$ Αδύνατο γιατί ο Μ.Κ.Δ είναι μόνο ο δ.

Το άτοπο δίνει ότι $\nexists\ p$ πρώτος ώστε $p | \gamma$ και $p \nmid \delta$

Δηλαδή $\gamma | \delta$.

Πόρισμα

Έστω $a, b \in \mathbb{Z}^*$

$$[a,b] = \frac{|a||b|}{(a,b)}$$

Απόδειξη

Θεωρούμε $a, b \in \mathbb{N}$.

$a = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$ $\quad p_1 < p_2 < \dots < p_\ell$ $\quad k_i > 0$

$b = q_1^{m_1} q_2^{m_2} \cdots q_n^{m_n}$ $\quad q_1 < q_2 < \dots < q_n$ $\quad m_i > 0$

(όταν δεν συνδέονται καθόλου έχουμε πχ $[2^k, 3^\ell] = 2^k \cdot 3^\ell$
$(2^k, 3^\ell) = 1$.)

Το ξαναγράφουμε χρησιμοποιώντας όλους τους πρώτους.
Όσοι δεν χρειάζονται στη μηδενική

$r_1 = 2 < r_2 = 3 < r_3 = 5 < \dots <$ μεγαλύτερος πρώτος

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

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

$(a,b) = r_1^{\varepsilon_1} \cdot r_2^{\varepsilon_2} \cdots r_t^{\varepsilon_t}$ $\quad \varepsilon_i = \min(a_i, a_i')$

$[a,b] = r_1^{\varepsilon_1'} \cdot r_2^{\varepsilon_2'} \cdots r_t^{\varepsilon_t'}$ $\quad \varepsilon_i' = \max(a_i, a_i')$

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

αν $a_i \le a_i' \Rightarrow \varepsilon_i = a_i$ 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

$$= a \cdot b$$