

5-3-15
5^η Διάλεξη

Μεταθέσεις - Συμβολισμοί

Μια k -μετάθεση από ένα σύνολο n στοιχείων είναι μια διατεταγμένη συλλογή από k στοιχεία από το σύνολό μας.

$M(n, k)$ = αριθμός όλων των k -μεταθέσεων από το σύνολο με τα n στοιχεία.

ΠΡΟΤΑΣΗ: Αν $1 \leq k \leq n$, τότε $M(n, k) = \frac{n!}{(n-k)!}$

Πχ. Πόσες τριάδες σχηματίζουμε από 5 στοιχεία?

1) Μας ενδιαφέρει η σειρά. Άρα είναι 3-μεταθέσεις. $M(5, 3) = \frac{5!}{(5-3)!} = \frac{5!}{2!}$

2) Δεν μας ενδιαφέρει η σειρά.

Αντίστοιχα $\{\square, +, 0\} = \{+, \square, 0\} = \{0, \square, +\} = \dots$

Άρα ζητάμε όλα τα υποσύνολα του συνόλου με 5 στοιχεία τα οποία έχουν ακριβώς 3 στοιχεία. Αυτό ονομάζεται συνδυασμός 3 στοιχείων από τα 5. Αντίστοιχα είναι "σαν" το $M(5, 3)$, χωρίς να μας ενδιαφέρει η σειρά $\{\square, +, 0\}$. Πόσες διατάξεις δημιουργούνται: Ανά ζητάμε τον αριθμό των 3-διατάξεων από 3 στοιχεία,

$$M(3, 3) = \frac{3!}{(3-3)!} = 3!$$

$(\square + 0) \neq (\square 0 +) \neq (+ \square 0) \neq (+ 0 \square) \neq (0 \square +) \neq (0 + \square)$
Σαν σύνολα είναι το ίδιο σύνολο $\{\square, +, 0\}$.

Άρα ο αριθμός που ζητάμε θα είναι $\frac{M(5, 3)}{3!} = \frac{5!}{(5-3)! 3!}$

Αυτός ο αριθμός δίνει τους ενδ. 3 στοιχείων από τα 5.

ΟΡΙΣΜΟΣ: Έστω $1 \leq k \leq n$. Ένας k -αριθμός στο A είναι ένα υποσύνολο A με n -στοχεία είναι ένα υποσύνολο του A το οποίο περιέχει ακριβώς k στοιχεία. $\binom{n}{k}$ θα συμβολίσαμε το πλήθος όλων των k -αριθμών στο n -στοχεία.

ΙΠΟΘΕΣΗ.

$$\text{Αν } 1 \leq k \leq n, \text{ τότε } \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{(n-k)!k!}$$

Απόδειξη = αλγώριθμος.

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

$\binom{n}{i}$ καθορίζεται συμπεριλαμβανομένων των a και b .

Απόδ. Με επαγωγή.

$$\boxed{\text{Βασικές}} \quad \binom{n}{0} = 1, \quad \binom{n}{k} = \binom{n}{n-k}, \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

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

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(n-1-k+1)!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!}$$

$$= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} = \frac{(n-1)!}{(n-k)!(k-1)!} \cdot \frac{k}{k} + \frac{(n-1)!}{(n-1-k)!k!} \cdot \frac{(n-k)}{(n-k)}$$

$$\frac{(k+n-k)}{(n-k)k} = \frac{(n-1)!n}{(n-k)k} = \frac{(n-1)!n}{(n-1-k)!(n-k)(k-1)!k} = \binom{n}{k}$$

Το $\binom{n}{i}$ είναι ο αριθμός των i -αριθμών με τους οποίους a εμφανίζεται i φορές και b εμφανίζεται $n-i$ φορές. $(a+b)^n = (a+b)(a+b)\dots(a+b) = (a+b)^n$.

Απόδειξη με επαγωγή.

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

$$n=2 \quad (a+b)^2 = a^2 + 2ab + b^2 = \sum_{i=0}^2 \binom{2}{i} a^i b^{2-i} \quad \text{Ισχύει!}$$

Υποθέτουμε ότι ισχύει για k :
 $(a+b)^k = \sum_{i=0}^k \binom{k}{i} a^i b^{k-i}$

Θα το δείξουμε για $(a+b)^{k+1}$

$$\begin{aligned} (a+b)^{k+1} &= (a+b)^k (a+b) = \left(\sum_{i=0}^k \binom{k}{i} a^i b^{k-i} \right) (a+b) = \\ &= \sum_{i=0}^k \binom{k}{i} a^{i+1} b^{k-i} + \sum_{i=0}^k \binom{k}{i} a^i b^{k-i+1} = \text{Συνθέτουμε} \\ &\quad \text{τους κοινούς όρους} \end{aligned}$$

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

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

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

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

Θεώρημα Κάθε φυσικός $n > 1$ έχει πρώτο διαμετέρι.

Απόδειξη

Για $n=2$ ισχύει.

Υποθέτουμε ότι ισχύει για όλους τους φυσικούς από $k+1$. Ι.Π. (Ισχύει για όλους τους $n > 1$).

Αν $k+1$ είναι πρώτος ισχύει. Αν δεν είναι, τότε θα 'ναι σύνθετος $k+1=ab$ με $1 < a, b < k+1$.

Από την υπόθεση της επαγωγής το a έχει πρώτο διαμετέρι, έστω p .
 $a=pa'$ και $k+1=ab=pa'b$. Άρα $p \mid k+1$.

Θεώρημα Το γινόμενο των πρώτων είναι άπειρο.

Απόδ.

Υποθέτουμε ότι το γινόμενο των πρώτων αριθμών είναι
πεπερασμένο: $1 < p_1 < p_2 < \dots < p_k$.

Θέλουμε να κατασκευάσουμε πρώτο διαφανές αριθμό.

Έστω $a = p_1 p_2 \dots p_k + 1$. Αν δεν είναι πρώτος, θα πρέπει να
υπάρξει πρώτος p_i ο οποίος θα τον διαιρεί:

$$p_i | a$$

$$p_i | p_i \Rightarrow p_i | (p_i p_i) p_k \} \Rightarrow p_i | a - p_1 \dots p_k \quad \left(\begin{array}{l} \text{Εάν όλοι αυτοί} \\ \text{είναι μεγαλύτεροι} \\ \text{από 1, αδύνατον} \end{array} \right)$$

Άρα ο a είναι πρώτος $\neq p_1 \dots p_k$ αδύνατον.

Το γινόμενο των πρώτων είναι άπειρο.

$$a|b \Leftrightarrow \exists c: b = a \cdot c$$

Δείγμα

Κάθε σύνθετος αριθμός $a > 1$ έχει ταλάνιστρον ένα πρώτο διαφανές
 $\leq \sqrt{a}$

Απόδειξη.

Από a σύνθετος $a = bc$ με $1 < b, c < a \Rightarrow$ υποθέτουμε ότι $c \leq b$
 $c^2 \leq bc = a \Rightarrow c \leq \sqrt{a}$

Παραίτητο ότι κάθε αριθμός > 1 έχει πρώτο διαφανές. Άρα ο c
έχει πρώτο διαφανές τον p . Αν $p | c$ και $c | a$. Άρα $p | a$ κ' $p \leq c \leq \sqrt{a}$

Πρόταση.

Έστω $a > 1$. Αν ο a δεν διαιρείται από κανένα πρώτο μικρότερο ή
ίσο του $\sqrt{a}$, τότε ο a είναι πρώτος.

Απόδ.

Αν δεν ήταν πρώτος $a = bc$ τότε θα είχε πρώτο διαφανές $\leq \sqrt{a}$ από
το προηγούμενο. Αλλά αυτό αποκλείεται από την υπόθεση.

Πρόβλημα: Να βρεθούν όλοι οι πρώτοι μικρότεροι ή ίσοι του $a > 1$
 για $a = 100$

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
									100

Βρες όλους τους πρώτους μέχρι το $\sqrt{a}$.
 $10 = \sqrt{100} \rightarrow 2, 3, 5, 7$.

$\{2, \dots, 100\} - (\{πολλαπλα του 2\} \cup \{πολλαπλα του 3\} \cup \{πολλαπλα του 5\} \cup \{πολλαπλα του 7\})$.

$\cup \{2, 3, 5, 7\}$ δίνει όλους τους πρώτους μικρότερους του 100.

Αυτή η διαδικασία καλείται το Κρίσιμο του Ερατοσθένη και βασίζεται στο πρόσφυμνο τόπισμα.

Ζητάμε το εύρος των πρώτων μικρότερων ή ίσων του a .

Βρίσκουμε όλους τους πρώτους $\leq \sqrt{a}$.

Για κάθε έναν από αυτούς από το αρχικό εύρος $\{2, \dots, a\}$ αφαιρούμε τα πολλαπλά τους και προσθέτουμε τους πρώτους $\leq \sqrt{a}$.

Παράδειγμα: Αν ο p είναι πρώτος και $p|ab$ τότε $p|a$ ή $p|b$.

Απόδειξη

Με τον ορισμό της καλής διαίρεσης. Προθέτουμε ότι το a διαιρείται με p ή όχι. Αν $p|a$ τότε $a = kp$ και $ab = kp \cdot b$ οπότε $p|ab$. Αν $p \nmid a$ τότε $p \nmid ab$ οπότε $p|b$.

Αρα $\exists a, b \in \mathbb{N}^*$ με $p \nmid a, b$ και $p \nmid ab$ ούτε $p \nmid b$
 $p \nmid a \rightarrow a = p\pi_1 + u_1 \quad 0 < u_1 < p$
 $p \nmid b \rightarrow b = p\pi_2 + u_2 \quad 0 < u_2 < p$
 $u_1 u_2 = (a - p\pi_1)(b - p\pi_2) = ab - p(a\pi_2 + b\pi_1 - p\pi_1\pi_2)$

$p \nmid ab$ και $p \mid p(a\pi_2 + b\pi_1 - p\pi_1\pi_2)$. Αρα $p \mid u_1 u_2$
 $u_1 u_2 = pk$ και $0 < u_1 < p$ και $0 < u_2 < p$. Αρα $0 < u_1 u_2 = pk < p^2$
 $\Rightarrow k < p$

Έστω q τρίτος διαπρέτης του k (χωρίζεται).

$q \mid k$ και $k \mid pk = u_1 u_2$. Αρα $q \mid u_1 u_2$
 q τρίτος $\Rightarrow$

$q < p$ και op είναι ο μικρότερος τρίτος για τον οποίο δεν ισχύει το θεώρημα. Αρα το θεώρημα ισχύει για τον a .
 Αντ. $q \mid u_1$ ή $q \mid u_2$.

Αυτό ισχύει για κάθε τρίτο διαπρέτη του k .

$$k = q_1 q_2 \dots q_\ell$$

$u_1 u_2 = pk = p q_1 q_2 \dots q_\ell$ Επειδή $q_i < p$ το θεώρημα ισχύει.

Αρα $\frac{u_1 u_2}{q_1 \dots q_\ell} = p$. Τροσάρει κάθε q_i διαπρέι το u_1 ή u_2 .

$$\frac{u_1 u_2}{q_1 \dots q_\ell} = \boxed{\text{γινόμενο 2 παραγώντων} = p}$$

$$u_1' u_2' = p \Rightarrow \underline{\underline{u_1' = 1}}$$

Έστω $u_2' = p$. Τότε $p \mid u_2 = u_2' x$

Αρα $p \mid b = p\pi_2 + u_2$
 $p \mid p\pi_2$
 $p \mid u_2 \Rightarrow p \mid b$

Αλλά είπαμε υποθέσαμε ότι ο p δε διαπρέι το a , ούτε το b .

Άρα! Αρα δεν υπάρχει ελάχιστος τρίτος, ώστε να μην έχει αυτή την ιδιότητα.