Diszkrét matematika 1.

5. előadás

Fancsali Szabolcs (Ligeti Péter diái alapján)

nudniq@cs.elte.hu
www.cs.elte.hu/∼nudniq

Kombinatorika

Alapproblémák

- sorbarendezések
- kiválasztások
- leszámlálások

Miket használunk

- négy alapművelet
  - összadás – esetszétválasztás
  - kivonás – „összes-rossz”
  - szorzás – független választás
  - osztás – „tehén-szabály”
- skatulya-elv
- bijekció

Permutációk

Példa

Egy elsős informatikus hallgatónak 15 vizsgát kell letennie. Hány különböző sorrendben teheti ezt meg?

Definíció

Az $1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$ szorzatot n faktoriálisnak nevezzük. Jele $n!$, továbbá $0! = 1$

Állítás

n különböző elem összes lehetséges sorrendjeinek száma $n!$ (Ezt az n elem (ismétlés nélküli) permutációinak nevezzük.)

Tétel (Stirling formula)

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

Permutációk

Példa

A fent említett hallgató 1 vizsgát 1esre, 2 vizsgát 2esre, ..., 5 vizsgát 5ösre teljesített. Hányféle sorrendben írhatja le a jegyeket?

Állítás

k_1 darab első típusú elem, k_2 darab második típusú elem, ..., k_n darab n-ik típusú elem lehetséges sorrendjeinek száma

$$\frac{(k_1 + k_2 + \cdots + k_n)!}{k_1! \cdot k_2! \cdot \ldots \cdot k_n!}$$

(Ezt az elemek ismétléses permutációinak nevezzük.)

Variációk

Példa

Az egyetemen összesen 15 különböző óra van. Ebből 6ot szeretnénk hétfőre tenni. Hányféle lehet a hétfői órarend?

Állítás

n különböző elemből minden lehetséges sorrendben k elem kiválasztásainak száma

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

(Ezt az elemek k-ad osztályú variációinak nevezzük.)

Variációk

Példa

Egy 48 fős dimat évfolyam hallgatói összesen hányféleképpen kaphatnak osztályzatot?

Állítás

n elemből képezhető k tagú sorozatok száma n^k.
*(Ezt az elemek k-ad osztályú ismétlés variáció*inak *nevezzük.)*

Kombinációk

Példa

A 14 dimat előadásról 3szor lehet hiányozni. Hányféleképpen lehet ezt megtenni?

Állítás

Egy n elemű halmaz k elemű részhalmazainak száma

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

(Ezt az elemek k-ad osztályú kombinációinak nevezzük.)

Binomiális együtthatók

Tétel

Az $\binom{n}{k}$ binomiális együtthatókra teljesülnek az alábbi azonosságok:

$$\binom{n}{k} = \binom{n}{n-k};$$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k};$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Kombinációk

Példa

A büfében 5-féle süteményt árulnak. 15 darabot hányféleképpen lehet megvenni?

Állítás

n elemből k kiválasztásainak száma, ha egy elem többször is szerepelhet és a sorrend nem számít

$$\binom{n+k-1}{k}$$

(Ezt az elemek k-ad osztályú ismétléses kombinációinak nevezzük.)

Binomiális tétel

Binomiális tétel

$\forall x, y \in \mathbb{R}, n \in \mathbb{N}^+$ esetén

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Következmény

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

*inomiális tétel

Binomiális tétel

$\forall x, y \in \mathbb{R}, n \in \mathbb{N}^+$ esetén

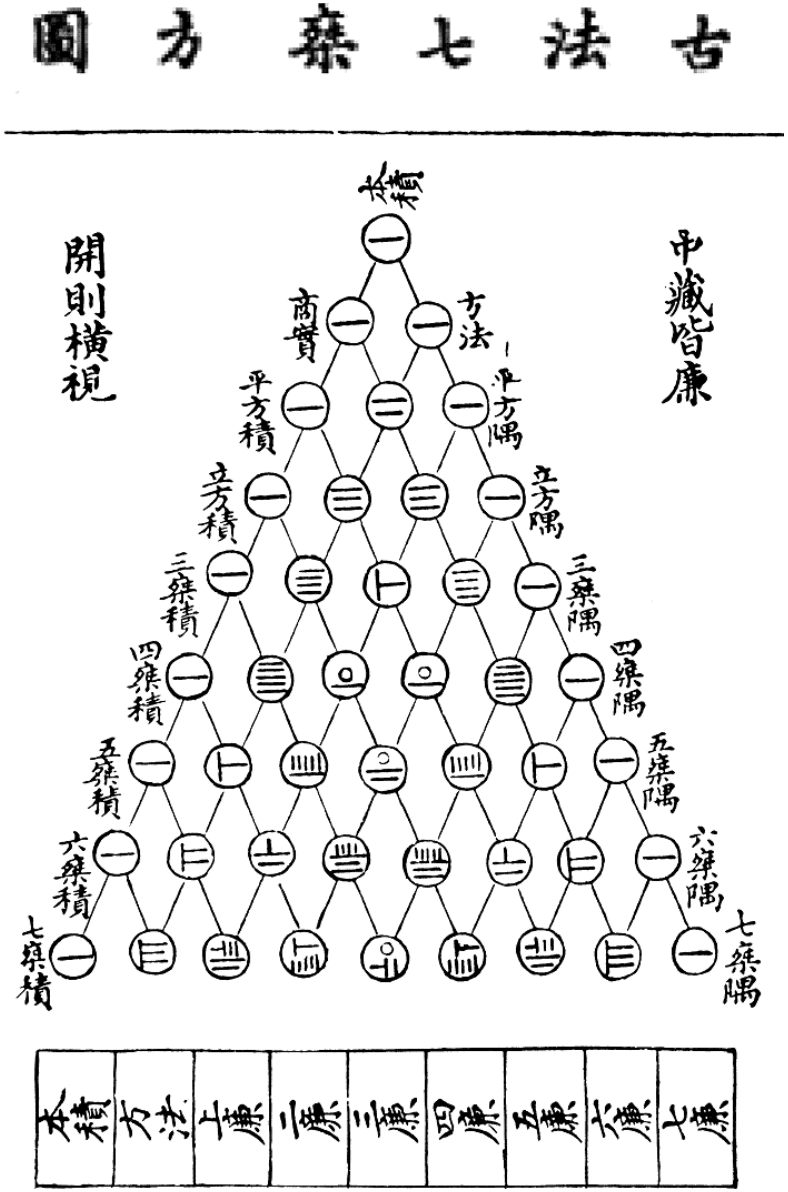
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Polinomiális tétel

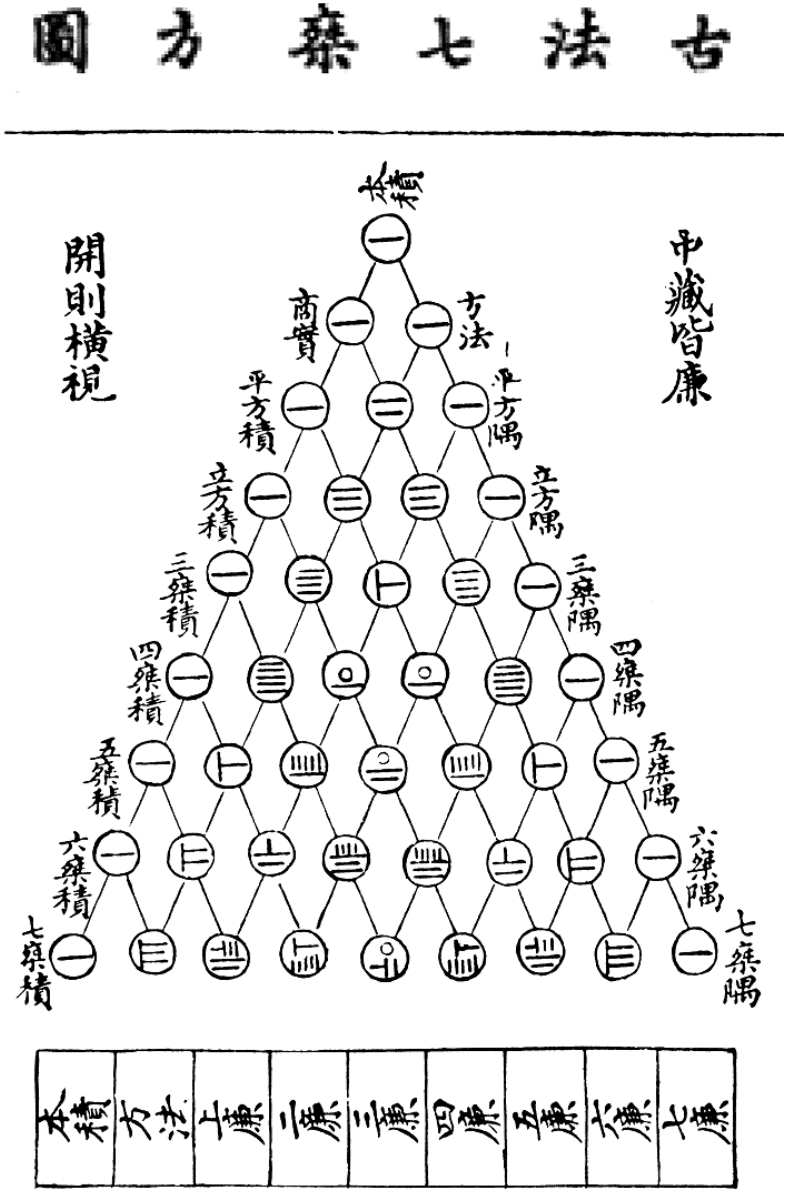
$\forall x_1, x_2, \ldots, x_r \in \mathbb{R}, n, r \in \mathbb{N}^+$ esetén

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{i_1+i_2+\cdots+i_r=n} \frac{n!}{i_1! \cdot i_2! \cdot \ldots \cdot i_r!} x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_r^{i_r}.$$

Pascal-háromszög



Pascal-háromszög



Pascal-háromszög

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$
$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$
$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$
$$\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6}$$
$$\dots$$

$$1$$
$$1\quad 1$$
$$1\quad 2\quad 1$$
$$1\quad 3\quad 3\quad 1$$
$$1\quad 4\quad 6\quad 4\quad 1$$
$$1\quad 5\quad 10\quad 10\quad 5\quad 1$$
$$1\quad 6\quad 15\quad 20\quad 15\quad 6\quad 1$$
$$1\quad 7\quad 21\quad 35\quad 35\quad 21\quad 7\quad 1$$
$$1\quad 8\quad 28\quad 56\quad 70\quad 56\quad 28\quad 8\quad 1$$
$$\dots$$

Azonosságok a Pascal-△-ben

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

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

$$\sum_{k=0}^{n} \binom{n}{k}^2 = ?$$

$$\sum_{i=0}^{k} \binom{n+i}{i} = ?$$

Szita módszer

Példa

Hány olyan 100nál kisebb pozitív egész van, ami nem osztható 2, 3 és 5 egyikével sem?

Állítás

Legyenek $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots$$

Fibonacci-számok

Példa

Egy lépcsőnek n foka van. Hányféleképpen mehetünk fel rajta, ha egy lépésben egy vagy két fokot lépünk?

Definíció

Az F_i számokat Fibonacci-számoknak nevezzük, ahol $F_0 = 0, F_1 = 1$, valamint $n \geq 1$ esetén

$$F_{n+1} = F_n + F_{n-1}$$

Azonosságok

- $F_0 + F_1 + \cdots + F_n = ?$
- Pascal-háromszög?
- és még rengeteg érdekesség...

Fibonacci-számok

Definíció

Az F_i számokat Fibonacci-számoknak nevezzük, ahol $F_0 = 0, F_1 = 1$, valamint $n \geq 1$ esetén

$$F_{n+1} = F_n + F_{n-1}$$

Tétel

Az F_n Fibonacci-számra fennáll az alábbi azonosság:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Születésnap paradoxon

Példa

Annak az esélye, hogy lesz két ember, akinek ugyanazon napon van a születésnapja:

- 367 embernél 100%
- 23 embernél több, mint 50%
- 58 embernél már több, mint 99%...

Tétel (Születésnap paradoxon)

Válasszunk n véletlen értéket az $\{1, \ldots, d\}$ számok közül. Ekkor annak az esélye, hogy lesz közöttük két egyforma $\approx 1 - e^{-\frac{n(n-1)}{2d}}$. (NemBiz.)

Alkalmazás: kriptográfiai hash-függvények

Motiváció

Tetszőleges hosszúságú üzenetnek egy fix hosszú „lenyomatát” képezzünk, ami eléggé „szétszórja” az üzeneteket.

Definíció

Egy $H : \{0,1\}^* \mapsto \{0,1\}^k$ *függvényt hash-függvénynek nevezünk, ahol* $k = 128, 160, 256, \ldots$ *fix érték.*
Egy ütközés $H(.)$*-ban egy* $x \neq y \in \{0,1\}^*$ *pár, amire* $H(x) = H(y)$.

Hash-függvény ütközések

- kriptográfiai hash-függvény egyik fő kritériuma, hogy nehéz legyen ütközést találni benne (számítási értelemben)
- skatulya-elv $\Rightarrow 2^k + 1$ üzenetből biztosan lesz ütközés
- születésnap paradoxon: $\Rightarrow 2^{k/2}$ üzenetből legalább 50% eséllyel lesz ütközés...