Diszkrét matematika 1. középszint

8. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼ nagy
Mérai László diái alapján

Komputeralgebra Tanszék

2017. ősz

Polinomiális tétel

Példa

Mennyi lesz?

$(x+y+z)^2 = x^2+y^2+z^2+2xy+2xz+2yz.$ $(x+y+z)^3 = \ldots$

Tétel

r, $n \in \mathbb{N}$ esetén

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

Bizonyítás

$(x_1+x_2+\ldots+x_r)^n =$
$(x_1+x_2+\ldots+x_r)(x_1+x_2+\ldots+x_r)\cdots(x_1+x_2+\ldots+x_r).$
Az $x_1^{i_1}x_2^{i_2}\ldots x_r^{i_r}$ együtthatója:

$$\binom{n}{i_1}\binom{n-i_1}{i_2}\binom{n-i_1-i_2}{i_3}\cdots\binom{n-i_1-i_2-\ldots-i_{r-1}}{i_r} =$$

$$\frac{n!}{i_1!(n-i_1)!}\frac{(n-i_1)!}{i_2!(n-i_1-i_2)!}\cdots\frac{(n-i_1-i_2-\ldots-i_{r-1})!}{i_r!(n-i_1-\ldots-i_{r-1}-i_r)!} = \frac{n!}{i_1!\cdot i_2!\cdots i_r!}$$

□

Polinomiális tétel

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

$(x + y + z)^3 = \ldots$

i_1	i_2	i_3	$\frac{3!}{i_1!i_2!i_3!}$	$(x+y+z)^3 =$
3	0	0	$\frac{3!}{3!0!0!} = 1$	x^3
2	1	0	$\frac{3!}{2!1!0!} = 3$	$+3x^2y$
2	0	1	$\frac{3!}{2!0!1!} = 3$	$+3x^2z$
1	2	0	$\frac{3!}{1!2!0!} = 3$	$+3xy^2$
1	1	1	$\frac{3!}{1!1!1!} = 6$	$+6xyz$
1	0	2	$\frac{3!}{1!0!2!} = 3$	$+3xz^2$
0	3	0	$\frac{3!}{0!3!0!} = 1$	$+y^3$
0	2	1	$\frac{3!}{0!2!1!} = 3$	$+3y^2z$
0	1	2	$\frac{3!}{0!1!2!} = 3$	$+3yz^2$
0	0	3	$\frac{3!}{0!0!3!} = 1$	$+z^3$

Skatulya-elv

Skatulya-elv

Ha n darab gyufásdobozunk és $n+1$ gyufaszálunk van, akkor akárhogyan rakjuk bele az összes gyufát a skatulyákba, valamelyikben legalább kettő gyufa lesz.

Példa

Nyolc ember közül van legalább kettő, aki a hét ugyanazon napján született.

Az $\mathcal{A} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ halmazból bárhogyan választunk ki ötöt, akkor lesz közülük kettő, melyek összege 9.

Tekintsük az $\{1, 8\}$, $\{2, 7\}$, $\{3, 6\}$, $\{4, 5\}$ halmazokat. Ekkor a kiválasztott öt elem közül lesz kettő, melyek azonos halmazban lesznek, így összegük 9.

Szita módszer

Hány olyan 1000-nél kisebb pozitív egész szám van, amely nem osztható sem 2-vel, sem 3-mal, sem 5-tel?

Az 1000-nél kisebb számok

összes	999	999
2-vel osztható	$\left\lfloor \frac{999}{2} \right\rfloor = 499$	-499
3-mal osztható	$\left\lfloor \frac{999}{3} \right\rfloor = 333$	-333
5-tel osztható	$\left\lfloor \frac{999}{5} \right\rfloor = 199$	-199
$2 \cdot 3$-mal osztható	$\left\lfloor \frac{999}{2 \cdot 3} \right\rfloor = 166$	$+166$
$2 \cdot 5$-tel osztható	$\left\lfloor \frac{999}{2 \cdot 5} \right\rfloor = 99$	$+99$
$3 \cdot 5$-tel osztható	$\left\lfloor \frac{999}{3 \cdot 5} \right\rfloor = 66$	$+66$
$2 \cdot 3 \cdot 5$-tel osztható	$\left\lfloor \frac{999}{2 \cdot 3 \cdot 5} \right\rfloor = 33$	-33
		$= 266$

Szita módszer

Tétel

Legyenek A_1, A_2, ..., A_n véges halmazok. Ekkor

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

Példa

Hány olyan 1000-nél kisebb szám van, amely nem osztható sem 2-vel, sem 3-mal, sem 5-tel?

Először: Hány olyan 1000-nél kisebb szám van, amely osztható 2-vel vagy 3-mal vagy 5-tel?

$A_1 = \{1 \le n \le 999 : 2|n\} \to |A_1| = \left\lfloor \frac{999}{2} \right\rfloor$;

$A_2 = \{1 \le n \le 999 : 3|n\} \to |A_2| = \left\lfloor \frac{999}{3} \right\rfloor$;

$A_3 = \{1 \le n \le 999 : 5|n\} \to |A_3| = \left\lfloor \frac{999}{5} \right\rfloor$.

Hasonlóan $|A_1 \cap A_2| = \left\lfloor \frac{999}{2\cdot 3} \right\rfloor$, $|A_1 \cap A_3| = \left\lfloor \frac{999}{2\cdot 5} \right\rfloor$, $|A_2 \cap A_3| = \left\lfloor \frac{999}{3\cdot 5} \right\rfloor$,

$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{999}{2\cdot 3\cdot 5} \right\rfloor$.

2-vel vagy 3-mal vagy 5-tel osztható számok száma:

$$\left\lfloor \frac{999}{2} \right\rfloor + \left\lfloor \frac{999}{3} \right\rfloor + \left\lfloor \frac{999}{5} \right\rfloor - \left\lfloor \frac{999}{2\cdot 3} \right\rfloor - \left\lfloor \frac{999}{2\cdot 5} \right\rfloor - \left\lfloor \frac{999}{3\cdot 5} \right\rfloor + \left\lfloor \frac{999}{2\cdot 3\cdot 5} \right\rfloor.$$

Általános szita formula

Tétel

Legyenek $A_1, \ldots, A_n$ az A véges halmaz részhalmazai, $f : A \to \mathbb{R}$ tetszőleges függvény. Legyenek

$$S = \sum_{x \in A} f(x);$$

$$S_r = \sum_{0<i_1<i_2<\ldots<i_r \le n} \; \sum_{x \in A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}} f(x);$$

$$S_0 = \sum_{x \in A \setminus \bigcup_{i=1}^{n} A_i} f(x).$$

Ekkor $S_0 = S - S_1 + S_2 - S_3 \pm \ldots + (-1)^n S_n$.

Példa

$A = \{1, 2, \ldots, 999\}$, $A_1 = \{n : \ 1 \le n < 1000, 2 \mid n\}$,
$A_2 = \{n : \ 1 \le n < 1000, 3 \mid n\}$, $A_3 = \{n : \ 1 \le n < 1000, 5 \mid n\}$,
$f(x) = 1$.
S_0: 2-vel, 3-mal, 5-tel nem osztható 1000-nél kisebb számok száma.

Általános szita formula bizonyítása

$S_0 = S - S_1 + S_2 - S_3 \pm \ldots + (-1)^n S_n$:

$$S_0 = \sum_{x \in A \setminus \bigcup_{i=1}^n A_i} f(x), \quad S = \sum_{x \in A} f(x)$$

$$S_r = \sum_{0<i_1<i_2<\ldots<i_r \leq n} \; \sum_{x \in A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}} f(x)$$

Bizonyítás

Ha $x \in A \setminus \bigcup_{i=1}^n A_i$, akkor $f(x)$ mindkét oldalon egyszer szerepel.
Ha $x \in \bigcup_{i=1}^n A_i$, legyenek $A_{j_1}, \ldots, A_{j_t}$ azon részhalmazok, melyeknek x eleme. Ekkor $f(x)$ a bal oldalon nem szerepel. Jobb oldalon a

$$\sum_{0<i_1<i_2<\cdots<i_r \leq n} \; \sum_{x \in A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}} f(x)$$

összegben szerepel, ha $\{i_1, \ldots, i_r\} \subseteq \{j_1, \ldots, j_t\}$. Ilyen r elemű indexhalmaz $\binom{t}{r}$ darab van. Így $f(x)$ együtthatója

$$\sum_{r=0}^{t} \binom{t}{r} (-1)^r = 0$$ (Biz.: gyakorlaton). □

Véges halmazok

Definíció

Az X és Y halmazokat ekvivalensnek nevezzük, ha létezik $f : X \to Y$ bijekció. Jelölése: $X \sim Y$.

Állítás

Ha n természetes szám, akkor $\{1, 2, \ldots n\}$ nem ekvivalens egyetlen valódi részhalmazával sem.

Definíció

Egy X halmazt végesnek nevezünk, ha valamely $n \in \mathbb{N}$ esetén ekvivalens az $\{1, 2, \ldots n\}$ halmazzal, egyébként végtelennek nevezzük.
Azt az egyértelműen meghatározott természetes számot, amire egy adott X halmaz ekvivalens az $\{1, 2, \ldots, n\}$ halmazzal, az X számosságának nevezzük, jelölése: $|X|$ (esetleg $card(X), \natural(X), \#(X)$).

Véges halmazok

Tétel

Legyenek X és Y halmazok. Ekkor

1. ha X véges, és $Y \subseteq X$, akkor Y is véges, és $|Y| \leq |X|$;
2. ha X véges, és $Y \subsetneq X$, akkor $|Y| < |X|$;
3. ha X és Y végesek és diszjunktak, akkor $X \cup Y$ is véges, és $|X \cup Y| = |X| + |Y|$;
4. ha X és Y végesek, akkor $|X \cup Y| + |X \cap Y| = |X| + |Y|$;
5. ha X és Y végesek, akkor $X \times Y$ is véges, és $|X \times Y| = |X| \cdot |Y|$;
6. ha X véges, akkor 2^X is véges, és $|2^X| = 2^{|X|}$.

Állítás (Skatulyaelv)

Ha X és Y véges halmazok, és $|X| > |Y|$, akkor egy $f : X \to Y$ függvény nem lehet injektív.

Oszthatóság

Ha a és b racionális számok ($b \neq 0$), akkor az a/b osztás mindig elvégezhető (és az eredmény szintén racionális).

Ha a és b egész számok, az a/b osztás nem mindig végezhető el (a hányados nem feltétlenül lesz egész).

Definíció

Az a egész osztja a b egészet (b osztható a-val): $a \mid b$, ha létezik olyan c egész, mellyel $a \cdot c = b$ (azaz $a \neq 0$ esetén b/a szintén egész).

Példák

- $1 \mid 13$, mert $1 \cdot 13 = 13$;
- $1 \mid n$, mert $1 \cdot n = n$;
- $6 \mid 12$, mert $6 \cdot 2 = 12$;
- $-6 \mid 12$, mert $(-6) \cdot (-2) = 12$.

A definíció kiterjeszthető például a Gauss-egészekre: $\{a + bi : \ a, b \in \mathbb{Z}\}$.

Példák

- $i \mid 13$, mert $i \cdot (-13i) = 13$;
- $1 + i \mid 2$, mert $(1 + i) \cdot (1 - i) = 2$.

Oszthatóság tulajdonságai

Állítás (HF)

Minden $a, b, c, \ldots \in \mathbb{Z}$ esetén

1. $a \mid a$;
2. $a \mid b$ és $b \mid c \Rightarrow a \mid c$;
3. $a \mid b$ és $b \mid a \Rightarrow a = \pm b$;
4. $a \mid b$ és $a' \mid b' \Rightarrow aa' \mid bb'$;
5. $a \mid b \Rightarrow ac \mid bc$;
6. $ac \mid bc$ és $c \neq 0 \Rightarrow a \mid b$;
7. $a \mid b_1, \ldots, b_k \Rightarrow$
   $\Rightarrow a \mid c_1 b_1 + \ldots + c_k b_k$;
8. $a \mid 0$, ui. $a \cdot 0 = 0$;
9. $0 \mid a \Leftrightarrow a = 0$;
10. $1 \mid a$ és $-1 \mid a$;

Példák

1. $6 \mid 6$;
2. $2 \mid 6$ és $6 \mid 12 \Rightarrow 2 \mid 12$;
3. $a \mid 3$ és $3 \mid a \Rightarrow a = \pm 3$;
4. $2 \mid 4$ és $3 \mid 9 \Rightarrow 2 \cdot 3 \mid 4 \cdot 9$;
5. $3 \mid 6 \Rightarrow 5 \cdot 3 \mid 5 \cdot 6$;
6. $3 \cdot 5 \mid 6 \cdot 5$ és $5 \neq 0 \Rightarrow 3 \mid 6$;
7. $3 \mid 6, 9 \Rightarrow 3 \mid 6c_1 + 9c_2$

Egységek

Definíció

Ha egy ε szám bármely másiknak osztója, akkor ε-t egységnek nevezzük.

Állítás

Az egész számok körében két egység van: 1, -1.

Bizonyítás

A ± 1 nyilván egység.
Megfordítva: ha ε egység, akkor $1 = \varepsilon \cdot q$ valamely q egész számra. Mivel $|\varepsilon| \geq 1$, $|q| \geq 1 \Rightarrow |\varepsilon| = 1$, azaz $\varepsilon = \pm 1$. □

Példa A Gauss-egészek körében az i is egység: $a + bi = i(b - ai)$.

Megjegyzés

Pontosan 1 osztói az egységek.

Asszociáltak

Oszthatóság szempontjából nincs különbség a 12 ill. -12 között.

Definíció

Két szám asszociált, ha egymás egységszeresei.

Megjegyzés

a és b pontosan akkor asszociált, ha $a \mid b$ és $b \mid a$.

Bizonyítás

$\Longrightarrow$: Ha $b = \varepsilon a$ és $a = \varepsilon' b$, ahol $\varepsilon, \varepsilon'$ egységek, akkor $a|b$ és $b|a$ nyilvánvaló.
$\Longleftarrow$: Legyen $b = ab_1$ és $a = ba_1$. Ekkor $b = ab_1 = ba_1b_1$, így $a_1b_1 = 1$, vagyis a_1 és b_1 is egységek.

Definíció

Egy számnak az asszociáltjai és az egységek a triviális osztói.

Prímek, felbonthatatlanok

Definíció

Ha egy nem-nulla, nem egység számnak a triviális osztóin kívül nincs más osztója, akkor felbonthatatlannak (irreducibilisnek) nevezzük.

Példa $2, -2, 3, -3, 5, -5$ felbonthatatlanok.
6 nem felbonthatatlan, mert $6 = 2 \cdot 3$.

Definíció

Egy nem-nulla, nem egység p számot prímszámnak nevezünk, ha $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

Példa $2, -2, 3, -3, 5, -5$.
6 nem prímszám, mert $6 \mid 2 \cdot 3$ de $6 \nmid 2$ és $6 \nmid 3$.

Prímek, felbonthatatlanok

Állítás

Minden prímszám felbonthatatlan.

Bizonyítás

Legyen p prímszám és legyen $p = ab$ egy felbontás. Igazolnunk kell, hogy a vagy b egység.
Mivel $p = ab$, így $p \mid ab$, ahonnan például $p \mid a$. Ekkor $a = pk = a(bk)$, azaz $bk = 1$, ahonnan következik, hogy b és k is egység. □

A fordított irány nem feltétlenül igaz:

- $\mathbb{Z}$-ben igaz, (lásd később);
- $\{a + bi\sqrt{5} : \ a, b \in \mathbb{Z}\}$-ben nem igaz.

Maradékos osztás

A számelméletben a fő eszközünk a maradékos osztás lesz:

Tétel

Tetszőleges a egész számhoz és $b \neq 0$ egész számhoz egyértelműen léteznek q, r egészek, hogy

$$a = bq + r \quad \text{és} \quad 0 \leq r < |b|.$$

Bizonyítás

A tételt csak nemnegatív számok esetében bizonyítjuk.

1. Létezés: a szerinti indukcióval. $a = 0$ esetén $q = r = 0$ jó választás. Tegyük fel, hogy a-nál kisebb számok már felírhatók ilyen alakban.
   - Ha $a < b$, akkor $a = b \cdot 0 + a$ ($q = 0$, $r = a$).
   - Ha $a \geq b$, akkor legyen az indukciós feltevés értelmében $a - b = bq^* + r^*$. Ekkor $a = b(q^* + 1) + r^*$ ($q = q^* + 1$, $r = r^*$).
2. Egyértelműség: legyen $a = bq + r = bq^* + r^*$. Ekkor $b(q - q^*) = r^* - r$. Ez csak akkor lehet, ha $q = q^*$ és $r = r^*$. □