Bevezetés az algebrába 1

Egész számok

Wettl Ferenc diáinak felhasználásával

Prímszámok

Prímszámok

Felbonthatatlan számok, prímszámok

D **Felbonthatatlan számok**

$p \in \mathbb{N}^+$ felbonthatatlan, ha $p \neq 1$ és nincs valódi osztója, azaz $p = ab$, $a, b \in \mathbb{N}^+ \Rightarrow a = 1$ vagy $b = 1$.

$p \in \mathbb{Z}$ felbonthatatlan, ha p nem egység és nincs valódi osztója, azaz $p = ab$, $a, b \in \mathbb{Z} \Rightarrow a$ vagy b egység.

Mj 1. A második megfogalmazás $\mathbb{N}^+$-ra is érvényes: $p \in \mathbb{N}^+$ pontosan akkor felbonthatatlan természetes számként, ha egész számként felbonthatatlan.

2. A 0 nem felbonthatatlan $\mathbb{Z}$-ben, ui. a $0 = 0 \cdot 0$ felbontásban egyik tényező sem egység.

D $a \in \mathbb{N}^+$ összetett szám ha $a \neq 1$ és nem felbonthatatlan.

T Minden 1-nél nagyobb egésznek van felbonthatatlan osztója.

B Indirekt: ha van ellenpélda, legyen n a legkisebb.

$\Rightarrow n$ nem felbonthatatlan $\Rightarrow n = ab$, ahol $1 < a < n \Rightarrow a$-nak az n minimalitása miatt van felbonthatatlan osztója, de az osztja n-et is, $\lightning$

D **Prímszám**

$p \in \mathbb{N}^+$ prím, ha $p \neq 1$ és
$p \mid ab$, $a, b \in \mathbb{N}^+ \Rightarrow p \mid a$ vagy $p \mid b$.

$p \in \mathbb{Z}$ prím, ha $p \neq 0$ és nem egység, és
$p \mid ab$, $a, b \in \mathbb{Z} \Rightarrow p \mid a$ vagy $p \mid b$.

Mj 0-ra is igaz, hogy ha $0 \mid ab$, akkor $0 \mid a$ vagy $0 \mid b$, de a 0-t kizártuk a prímek definíciójánál.

Mj $p \in \mathbb{Z}$ felbonthatatlan $\mathbb{Z}$-ben $\Leftrightarrow$ $|p|$ felbonthatatlan $\mathbb{N}^+$-ban.
$p \in \mathbb{Z}$ prím $\mathbb{Z}$-ben $\Leftrightarrow$ $|p|$ prím $\mathbb{N}^+$-ban.

P Mik a felbonthatatlanok és mik a prímek $2\mathbb{Z}$-ben?

m Felbonthatatlanok: $2k$, ahol $2 \nmid k$, ui. $n \mid ab \rightsquigarrow 4 \mid n$.

Prímek: nincsenek, ui. $a \mid 2a$, de $a \nmid 2$, $a \nmid a$, ha $a \in 2\mathbb{Z} \setminus \{0\}$.

T **Prímek és felbonthatatlan számok**

$p \in \mathbb{Z}$ (illetve $p \in \mathbb{N}^+$) pontosan akkor prím, ha felbonthatatlan.

B A korábbi megjegyzés miatt elég $\mathbb{N}^+$-ra bizonyítani:

(prím $\Rightarrow$ felbonthatatlan): Tfh. $p = ab$. Ekkor $p \mid ab$, de p prím, így $p \mid a$ vagy $p \mid b$. Feltehető, hogy $p \mid a$. Így $a \mid ab = p \mid a \Rightarrow a \leqslant p \leqslant a \Rightarrow p = a \Rightarrow b = 1$. Tehát p felbonthatatlan.

(felbonthatatlan $\Rightarrow$ prím): Tfh. $p \mid ab$. Ha $p \nmid a \Rightarrow (p, a) \neq p$, de $(p, a) \mid p$, így p felbonthatatlansága miatt $(p, a) = 1$. Ezért $p \mid ab \Rightarrow p \mid b$.

T **Euklidész tétele**

A prímszámok száma végtelen.

B Indirekt: tegyük fel, hogy csak véges sok prím létezik: p_1, p_2,..., p_k. Tekintsük az $n = p_1 p_2 \dots p_k + 1$ számot. $\exists q \mid n$, ami felbonthatatlan, tehát prím is. De $(p_i, n) = (p_i, 1) = 1$ miatt $q \neq p_i$ $(i = 1, \dots, k)$ ↯

T Ha $n \in \mathbb{N}^+$ összetett szám, akkor van $\sqrt{n}$-nél nem nagyobb prímtényezője.

B $n = ab$, $1 < a \leqslant b < n \Rightarrow a^2 \leqslant ab = n \Rightarrow a \leqslant \sqrt{n}$.

Algoritmus:

Eratoszthenész szitája

1. Írjuk fel egy lapra 1-től N-ig a számokat;
2. húzzuk át az 1-et;
3. karikázzuk be a legkisebb nem áthúzott számot;
4. húzzuk át ennek a többszöröseit;
5. ismételjük a 3., 4. lépést, amíg a bekarikázott szám nem éri el $\lfloor\sqrt{n}\rfloor$-et;
6. karikázzuk be a maradékot.

Így a bekarikázott számok éppen a prímszámok 1-től N-ig.

T Dirichlet tétel: ha a és b relatív prímek, akkor az $an + b$ $(n = 1, 2, 3, \dots)$ sorozatban végtelen sok prímszám van.

T Ben Green, Terrence Tao, 2006: létezik tetszőlegesen hosszú, csak prímekből álló számtani sorozat. (Pl. (2, 3), (3, 5, 7), 5, 11, 17, 23, 29), (7, 37, 67, 97, 127, 157), (199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089).)

T Prímszámtétel (Hadamard, de la Valleé-Poussin, 1896; elemi bizonyítás Selberg, Erdős, 1949) Az x-nél kisebb prímek száma, $\pi(x)$ aszimptotikusan $x/\ln x$, azaz

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Prímszámok

A számelmélet alaptétele

T **A számelmélet alaptétele**

Minden 1-nél nagyobb természetes szám előáll véges sok felbonthatatlan természetes szám szorzataként, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

B A felbonthatóság bizonyítása. Indirekt: tfh van ellenpélda, legyen n a legkisebb. n nem lehet felbonthatatlan, mert akkor az egyelemű szorzat a felbontás. $\Rightarrow$ Van $n = ab$ valódi felbontás, ahol $1 < a, b < n \Rightarrow a$ és b felbonthatók, így a szorzatuk is. $\lightning$

Az egyértelműség bizonyítása. Indirekt: tegyük fel, hogy van olyan természetes szám, mely nem bontható fel egyértelműen. Legyen n közülük a legkisebb. $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$.

p_1 prím, és $p_1 \mid q_1 \cdots q_s \Rightarrow p_1 \mid q_i$ valamely i-re. De q_i felbonthatatlan $\Rightarrow p_1 = q_i \Rightarrow \frac{n}{p_1} = p_2 \cdots p_r = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s$ is két különböző felbontás lenne. $\lightning$

D Az azonos prímek szorzatát hatvánnyal jelölve az 1-nél nagyobb egészek kanonikus alakjához jutunk: $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, ahol $p_1 < \dots < p_r$ prímek.

P $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$.

T **A számelmélet alaptétele $\mathbb{Z}$-re**

Minden 0-tól és egységtől különböző egész szám sorrendtől és egységszeresektől eltekintve egyértelműen előáll felbonthatatlanok szorzataként.

(Pl. $-6 = (-2)\cdot 3 = 2\cdot(-3) = 3\cdot(-2) = (-3)\cdot 2$)

B Előállítás: $a \in \mathbb{Z} \setminus \{0, \pm 1\} \Rightarrow$ az alaptétel miatt $1 < |a| = p_1 \cdots p_r \Rightarrow$ $a = p_1 p_2 \cdots p_r$ vagy $a = (-p_1) p_2 \cdots p_r$.

Egyértelműség: $a = p_1 \cdots p_r = q_1 \cdots q_s \Rightarrow$ $|a| = |p_1| \cdots |p_r| = |q_1| \cdots |q_s| \Rightarrow r = s$, és az egymásnak megfelelő prímekre $|p_i| = |q_j| \Rightarrow p_i = \pm q_j$.

F Bizonyítsuk be, hogy a pozitív páros számok körében is felbontható minden szám felbonthatatlanok szorzatára, de nem egyértelműen.

T **Legendre-formula**

$n!$ kanonikus alakjában a p prím kitevője

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots .$$

B $n \in \mathbb{N}^+$-re az $\{1, 2, \dots, n\}$-beli d-vel oszhatók száma $\lfloor \frac{n}{d} \rfloor$, ui. $0 < kd \leqslant n \iff 1 \leqslant k \leqslant \lfloor \frac{n}{d} \rfloor$, ez $\lfloor \frac{n}{d} \rfloor$ db.
$n! = 1 \cdot 2 \cdot 3 \cdots n$-ben $\lfloor \frac{n}{p} \rfloor$ tényező osztható p-vel, $\lfloor \frac{n}{p^2} \rfloor$ osztható p^2-tel (ez pluszban $\lfloor \frac{n}{p^2} \rfloor$ darab p-es tényezőt tesz hozzá), ..., bármely k-ra $\lfloor \frac{n}{p^k} \rfloor$ darab osztható p^k-val. Az összeg mindig véges, mert ha $p^m \leqslant n < p^{m+1}$, akkor $k > m$ esetén $\lfloor \frac{n}{p^k} \rfloor = 0$.

P 9! maximum mekkora 2-hatvánnyal osztható?

m $\lfloor \frac{9}{2} \rfloor + \lfloor \frac{9}{4} \rfloor + \lfloor \frac{9}{8} \rfloor = 4 + 2 + 1 = 7$, tehát 2^7-nel.

F $\left\lfloor \frac{a}{bc} \right\rfloor = \left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor$ és így $\left\lfloor \frac{n}{p^k} \right\rfloor$ kiszámítása gyorsabban: $\left\lfloor \frac{\lfloor \frac{n}{p^{k-1}} \rfloor}{p} \right\rfloor$

D **Legkisebb közös többszörös**

$a, b \in \mathbb{Z}$, $a, b \neq 0$-ra a és b legkisebb közös többszöröse az a legkisebb pozitív egész, amelynek a és b is osztója. Jelölései: $[a, b] = \text{lkkt}(a, b) = \text{lcm}(a, b)$ (least common multiple).

Á $m \in \mathbb{N}^+$-ra $m = [a, b] \Leftrightarrow$

(1) $a \mid m$, $b \mid m$,

(2) és ha $a \mid c$ és $b \mid c$ valamely c-re, akkor $m \mid c$.

Mj Ez azt jelenti, hogy a legkisebb közös többszörös a kitüntetett közös többszörös.

B $\Leftarrow$: m közös többszörös (1) miatt, és a legkisebb, mert minden más $c \in \mathbb{N}^+$ közös többszörösre $m \mid c$, így $m \leqslant c$.

$\Rightarrow$: $a \mid m$, $b \mid m$ ✓

Ha $a \mid c$ és $b \mid c$, akkor a $c = mq + r$ maradékos osztásból $a, b \mid r$, tehát r is közös többszörös, és $0 \leqslant r < m$. De m volt a legkisebb pozitív közös többszörös, így $r = 0$.

T Legyen $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ és $b = p_1^{b_1} \cdots p_r^{b_r}$, ahol $p_1, \ldots, p_r$ különböző pozitív prímek, és a_i, b_i nemnegatív egészek. (Bármely két $a, b \in \mathbb{N}^+$ felírható így, ha megengedjük a 0 kitevőket.)

(1) $a \mid b \iff 0 \leqslant a_i \leqslant b_i \ (i = 1, 2, \ldots, r)$.

(2) $(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_r^{\min(a_r,b_r)}$

(3) $[a, b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_r^{\max(a_r,b_r)}$

(4) Ha a és b pozitív egész, akkor $[a, b](a, b) = ab$.

B (1): ($\Leftarrow$): ✓ ($\Rightarrow$): $b = ac \Rightarrow c$ prímtényezői is $p_1, \ldots, p_r$ közül valók, és ha $c = p_1^{c_1} \cdots p_r^{c_r}$, akkor $b_i = a_i + c_i \geqslant a_i \ \forall i$.

(2): $c > 0$-ra $c \mid a, b \Leftrightarrow c = p_1^{c_1} \cdots p_r^{c_r}$, ahol $c_i \leqslant a_i, b_i \ \forall i$, azaz $c_i \leqslant \min\{a_i, b_i\} \ \forall i$. ezek közül mindnek osztója (1) szerint az, amelyikben a kitevők $\min\{a_i, b_i\}$.

(3): hasonlóan a (2)-höz.

(4): $\max(a_i, b_i) + \min(a_i, b_i) = a_i + b_i$,
$p_i^{\max(a_i,b_i)} p_i^{\min(a_i,b_i)} = p_i^{\max(a_i,b_i)+\min(a_i,b_i)} = p_i^{a_i+b_i} = p_i^{a_i} p_i^{b_i}$.

F Mutassuk meg, hogy bármely pozitív a és b egészhez van olyan m és n egész, hogy $m \mid a$, $n \mid b$, $(m, n) = 1$ és $mn = [a, b]$.

D $a_1, \ldots, a_n \in \mathbb{Z}$-re

$a_1, \ldots, a_n$ legnagyobb közös osztója, $(a_1, \ldots, a_n)$, az a $d \geqslant 0$ egész, amelyre $d \mid a_i \ \forall i$, és ha $d' \mid a_i \ \forall i$, akkor $d' \mid d$

$a_1, \ldots, a_n$ legkisebb közös többszöröse, $[a_1, \ldots, a_n]$, az a $c \geqslant 0$ egész, amelyre $a_i \mid c \ \forall i$, és ha $a_i \mid c' \ \forall i$, akkor $c \mid c'$

Mj Könnyen látható, hogy $(a_1, \ldots, a_{n-1}, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$, és $[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$.