1. A kanonikus alak alkalmazásai

A kanonikus alak
Vonjuk össze a prímtényezős felbontásban az asszociált prímeket.

Példa
$-36 = 2 \cdot 2 \cdot 3 \cdot (-3) = (-1)2^2 3^2$.

HF: A $-$ jelet a szám elején nem lehet megúszni.

Definíció (FGy1.6.1, K3.1.16)
Egy szám kanonikus alakja $ep_1^{\alpha_1} \dots p_k^{\alpha_k}$, ahol e egység, $\alpha_i > 0$ egész, a p_i felbonthatatlanok pedig páronként nem asszociáltak.

(1) A kanonikus alakban a kitevők egyértelműen meghatározottak, a prímek pedig asszociáltság erejéig (K3.1.18).

(2) Pozitív egész szám kanonikus alakjában pozitív prímeket használunk, és az egységtényező is elmarad (K3.1.17).

(3) Néha érdemes megengedni 0 kitevőket (K3.1.22)

Az osztók kanonikus alakja és száma

Tétel (FGy1.6.2, 1.6.3)
Legyen $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ kanonikus alakú, ahol $p_i > 0$ és $\alpha_i \geq 0$. Ekkor n pozitív osztói egyértelműen felírhatók $d = p_1^{\beta_1} \dots p_k^{\beta_k}$ alakban, ahol $0 \leq \beta_i \leq \alpha_i$.
Az osztók száma $(\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1)$, jele $d(n)$.

Az nyilvánvaló, hogy az ilyen alakú d számok osztói n-nek.
Megfordítva, tegyük fel, hogy $n = dq$. Írjuk föl a d és q számokat pozitív prímek szorzataként. Az egyértelműség miatt mindkét oldalon ugyanazok a prímek szerepelnek, így $d = p_1^{\beta_1} \dots p_k^{\beta_k}$ és $q = p_1^{\gamma_1} \dots p_k^{\gamma_k}$ (mindegyik kitevő lehet nulla). Ekkor $p_1^{\alpha_1} \dots p_k^{\alpha_k} = p_1^{\beta_1+\gamma_1} \dots p_k^{\beta_k+\gamma_k}$, ahonnan a kanonikus alak egyértelműsége miatt $\alpha_i = \beta_i + \gamma_i$. Mivel $0 \leq \beta_i \leq \alpha_i$, ezért β_i-re $\alpha_i + 1$ lehetőség adódik. Ezeket függetlenül választhatjuk, ezért a lehetőségek összeszorzódnak. □

A kitüntetett közös osztó képlete

Tétel (FGy1.6.4)
Legyen $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ és $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ kanonikus alakú,
ahol $p_i > 0$ és $\alpha_i, \beta_i \geq 0$.
Ekkor $(a, b) = p_1^{\gamma_1} \dots p_k^{\gamma_k}$, ahol $\gamma_i = \min(\alpha_i, \beta_i)$ minden i-re.

Itt $\min(x, y)$ jelöli az x és y számok közül a nem nagyobbat.
(Hasonlóan $\max(x, y)$ az x és y számok közül a nem kisebb.)

Bizonyítás
Legyen $d = p_1^{\gamma_1} \dots p_k^{\gamma_k}$. Nyilván $d \mid a$ és $d \mid b$.
Megfordítva, ha $c \mid a$ és $c \mid b$, akkor az előző tétel szerint $c = p_1^{\delta_1} \dots p_k^{\delta_k}$, ahol $\delta_i \leq \alpha_i$ és $\delta_i \leq \beta_i$. De akkor $\delta_i \leq \gamma_i = \min(\alpha_i, \beta_i)$, ezért $c \mid d$. Vagyis d minden közös osztónak többszöröse. □

Kitüntetett közös többszörös

Definíció (FGy1.6.5, HF)
Az a és b pozitív egészek *kitüntetett közös többszöröse* c, ha közös többszörös, és minden közös többszörösnek osztója. Ez a pozitív közös többszörösök között nagyságra a legkisebb, jele $[a, b]$.

Tétel (FGy1.6.6)
Legyen $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ és $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ kanonikus alakú,
ahol $p_i > 0$ és $\alpha_i, \beta_i \geq 0$.
Ekkor $[a, b] = p_1^{\gamma_1} \dots p_k^{\gamma_k}$, ahol $\gamma_i = \max(\alpha_i, \beta_i)$ minden i-re.
Teljesül, hogy $(a, b)[a, b] = ab$.

Az első állítás a korábbiakhoz hasonlóan igazolható. A másodikhoz azt elég megmutatni, hogy $\min(x, y) + \max(x, y) = x + y$. Az x és y esetleges cseréjével feltehető, hogy $x \leq y$, ekkor $\min(x, y) = x$ és $\max(x, y) = y$, ezek összege tényleg $x + y$. □

További összefüggések

Tétel (FGy1.6.6, 1.6.7)
Legyenek a, b, c pozitív egészek. Ha $a \mid c$, $b \mid c$ és $(a, b) = 1$, akkor $ab \mid c$.
Speciálisan $a \mid b$ pontosan akkor, ha a minden prímhatvány-osztója osztja b-t.
$(a, b) = 1$ akkor és csak akkor, ha nincs közös prímosztójuk.
$(c, ab) = 1$ akkor és csak akkor, ha $(c, a) = 1$ és $(c, b) = 1$.

Az első állítás bizonyításához vegyük észre, hogy a kitüntetett közös többszörös definíciója miatt $[a, b] \mid c$. De ha $(a, b) = 1$, akkor $ab = (a, b)[a, b] = [a, b]$.

A második állítás abból következik, hogy egy szám pontosan akkor egység, ha nincs prímosztója.

A harmadik pedig a másodikból: ha a p prím közös osztója c-nek és ab-nek, akkor osztója a-nak vagy b-nek is, ezért (a, c) vagy (b, c) nem lehet 1. □

Az $n!$ kanonikus alakja

Tétel (FGy1.6.8, Legendre-formula)
Az $n!$ szám kanonikus alakjában a $p > 0$ prím kitevője
$\alpha_p = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \ldots + \lfloor n/p^k \rfloor + \ldots$,
ahol $\lfloor x \rfloor$ az x szám *alsó egészrésze*, vagyis az x-nél kisebb vagy egyenlő egészek közül a legnagyobb.

Az α_p összeg mindig véges, mert előbb-utóbb $p^k > n$.
Speciálisan $p > n$ esetén $\alpha_p = 0$ (üres összeg).

Bizonyítás
Az $1, 2, \ldots, n$ számok közül $\lfloor n/p \rfloor$ osztható p-vel, mert $1 \leq pt \leq n$ pontosan akkor, ha $0 < t \leq n/p$. További $\lfloor n/p^2 \rfloor$ szám osztható p^2-tel is, és így tovább. Ha egy $1 \leq m \leq n$ számban a p kitevője k, akkor m az α_p összeg k tagjához járul hozzá 1-gyel. □

Végtelen sok prímszám van

Tétel (FGy5.1.1)
Az egész számok között a prímek száma végtelen.

Euklidész bizonyítása
Tegyük föl indirekt, hogy csak véges sok van, ezek $p_1, p_2, \ldots, p_n$.
Tekintsük az $A = p_1 p_2 \ldots p_n + 1$ számot. Mivel $A > 1$, ezért van egy p prímosztója. Ez a p valamelyik p_k-val egyenlő, ezért $p \mid p_1 p_2 \ldots p_n$. De $p \mid A$, ezért $p \mid A - p_1 p_2 \ldots p_n = 1$. Ez ellentmondás. □

HF: Módosítsuk ezt a bizonyítást annak megmutatására, hogy végtelen sok olyan prím van, amely 4-gyel osztva 3-at, és olyan is, ami 6-tal osztva 5-öt ad maradékul. Igazoljuk, hogy az n-edik (pozitív) prímszám kisebb, mint 2^{2^n}.

Eratoszteneszi szita

Tétel (FGy5.1.2)
Azt, hogy n prímszám-e, eldönthetjük a következőképpen. Írjuk fel a számokat 2-től n-ig. Karikázzuk be a 2-t, és húzzuk ki a többszöröseit. Ezt ismételjük: az első nem kihúzott és nem karikázott szám (most a 3) prím, karikázzuk be, és húzzuk ki a többeseit. Folytassuk, amíg $\sqrt{n}$-ig nem érünk. Ekkor a bekarikázottak és a jelöletlenek a prímek n-ig.

Amit kihúztunk, összetett, mert van nála kisebb osztója. A karikásaknak nincs, ezért prímek. Végül egy jelöletlen m azért prím, mert ha az lenne, akkor legyen p a legkisebb prímosztója. Ekkor $m = pb$, ahol $b \neq 1$. De akkor $p \leq b$, hiszen b-nek is van prímosztója, és így $p^2 \leq pb \leq n$, azaz $p \leq \sqrt{n}$. Ezért m-et kihúztuk volna p-nél. □

2. Számolás maradékokkal

Vizsgálat mod 5

Diofantikus egyenlet: az egész megoldásokat keressük.
Oldjuk meg: $x^2 + 5y = 1002$.

Ötlet: Osszuk el mindkét oldalt maradékosan 5-tel. Azt kapjuk, hogy x^2 maradéka 2 kell, hogy legyen.
Ha $x = 5q + r$, akkor $x^2 = 25q^2 + 10qr + r^2 = 5(5q^2 + 2r) + r^2$. Az r lehetséges értékei 0, 1, 2, 3, 4. Ezért r^2 értékei 0, 1, 4, 9, 16. Ezek maradéka öttel osztva rendre 0, 1, 4, 4, 1. Soha nem lesz 2. Ezért négyzetszám 5-tel osztva nem adhat 2 maradékot. Tehát az eredeti diofantikus egyenletnek *nincs megoldása.*

Beláttuk
Négyzetszám 5-tel osztva csak 0, 1, 4 maradékot adhat.

Az egyenlet megoldását visszavezettük véges sok próbálgatásra.
A modulo 5 *maradékokkal számoltunk.*

Számolás maradékokkal

Definíció (K1.1.4)
Ha $n \geq 1$ egész, akkor legyen $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Összeadás: $a +_n b$ az $a + b$ maradéka n-nel osztva. Szorzás: $a *_n b$ az ab maradéka n-nel osztva.

Példa (K, 4. oldal)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ezek a *modulo* 5 *műveleti táblázatok.*

Összeg és szorzat maradéka
Megmutattuk, hogy ha $x = 5q + r$, akkor x^2 és r^2 ugyanazt a maradékot adja 5-tel osztva. Ezért az eredeti számok helyett a maradékaikkal számolhatunk.

Tétel (K1.1.6)
Legyen $n \geq 1$ egész, és jelölje felülvonás az n-nel való osztási maradékot. Ekkor $\overline{x+y} = \overline{x} +_n \overline{y}$ és $\overline{xy} = \overline{x} *_n \overline{y}$. Azaz *összeg maradéka a maradékok (mod n vett) összege; Szorzat maradéka a maradékok (mod n vett) szorzata.* A mod n maradékképzés tehát *művelettartó.*

Kulcs: ha $n \mid a - b$, akkor a és b ugyanazt a maradékot adja n-nel osztva. Valóban, legyen $a = nq + r$ és $b = ns + t$. Ekkor $a - b = n(q - s) + (r - t)$, ezért $n \mid r - t$. Ha $0 \leq r, t < n$, akkor $0 \leq r - t < n$, ezért $r = t$.

A részletes bizonyításhoz bevezetünk egy új jelölést.

3. Összefoglaló

A 10. előadáshoz tartozó vizsgaanyag

Fogalmak
Kanonikus alak (FGy1.6.1. K3.1.16, 3.1.27, 3.1.18, 3.1.22). Kitüntetett közös többszörös (FGy1.6.5). Műveletek mod n (K1.1.4).

Tételek
Az osztók kanonikus alakja és száma (FGy1.6.2, 1.6.3). A kitüntetett közös osztó és többszörös képlete (FGy1.6.4,1.6.6). A relatív prímség elemi tulajdonságai (FGy1.6.6,1.6.7). Az $n!$ kanonikus alakja (FGy1.6.8). Végtelen sok prímszám van (FGy5.1.1). Eratoszteneszi szita (FGy5.1.2). A mod n maradékképzés művelettartó (K1.1.6).