1. tétel

Számelméleti alapfogalmak, a számelmélet alaptétele. A prímszámelmélet elemei. A kongruencia fogalma, maradékosztályok, Euler-Fermat-tétel. Lineáris és magasabb fokú algebrai kongruenciák. Binom kongruenciák, kvadratikus kongruenciák.

A számelmémet az egész számok gyűrűjével foglalkozik. A (**Z**, +, ·) integritástartomány (= egységelemes, zérusosztómentes kommutatív gyűrű).
Gyűrű = (H, +, ·) gyűrű, ha a (H, +) kommutatív csoport (=asszociatív és invertálható) és (H, ·) félcsoport (=asszociatív) és „ · ” disztributív a „ + ” –ra. Különböző fogalmak vannak értelmezve benne.

1. <u>abszolútérték</u>

$$x \in \mathbf{Z},\ |x| = \begin{cases} x, \text{ ha } x \in \mathbf{N} \\ -x, \text{ ha } x \in \mathbf{Z} / \mathbf{N} \end{cases}$$

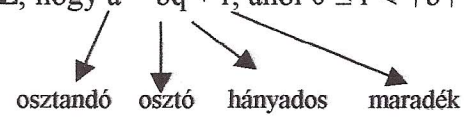
$|a + b| \le |a| + |b|$
$|a \cdot b| = |a| \cdot |b|$

2. <u>reláció</u>
   a, b ∈ **Z** , a ≤ b:
   - ha a ∈ **Z**, b ∈ **N** ⇒ a< b
     b ∈ **Z**, a ∈ **N** ⇒ b < a
   - ha a, b ∈ **Z** ⇒ az a kisebb, amelyiknek az abszolútértéke a nagyobb

<u>Rendezési reláció</u>
δ ⊆ H × H rendezési reláció, ha reflexív, antiszimmetrikus és tranzitív
Jele: $a \underset{=}{\prec} b$

<u>Részben rendezett halmaz</u>
H ≠ ∅ és H-n értelmezve van egy rendezési reláció ⇒ H-t részben rendezett halmaznak nevezzük.
(jól rendezett halmaz, ha minden nem üres részhalmazának van legkisebb eleme)
A (**Z**, ≤) nem jól rendezett, de rendezett halmaz.

<u>Maradékos osztás tétele</u>
∀ a, b (≠0) ∈ **Z** számokhoz egyértelműen létezik q, r ∈ **Z**, hogy a = bq + r, ahol 0 ≤ r < |b|



r a legkisebb nemnegatív maradék

<u>Euklideszi algoritmus</u>
Adottak a, b (≠0) ∈ **Z** számok, a maradékos osztás tétele szerint

$$a = bq_0 + r_1, \text{ ahol } 0 \le r_1 < |b|$$

- ha $r_1 \neq 0 \Rightarrow$ b és r_1 egészekre a maradékos osztást elvégezve

$$b = r_1 q_1 + r_2, \text{ ahol } 0 \le r_2 < r_1$$

Hasonlóan folytatva a maradékos osztásokat a következő ún. euklideszi algoritmust kapjuk.

Véges sok lépés után a maradéknak 0-nak kell lennie.

$$a = bq_0 + r_1 \quad , 0 < r_1 < |b|$$

$$b = r_1 q_1 + r_2 \quad , 0 < r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \quad , 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad , 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n + r_{n+1} \quad , r_{n+1} = 0$$

r_n: az algoritmus utolsó zérustól különböző maradéka

Tétel: $r_n = ax + by \longrightarrow r_n$ felírható a és b lineáris kombinációjaként.

Oszthatóság

Def: Az *a* egész szám osztója a *b* egész számnak, ha az ax = b egyenlet megoldható **Z**-ben.

a | b, tagadása a ∤ b

b az *a* egész számú többszöröse

Az oszthatóság binér reláció.

Tétel: **Z**-ben az oszthatósági reláció

a) reflexív a | a
b) nem szimmetrikus a | b ⇏ b | a
c) nem antiszimmetrikus
d) tranzitív a | b, b | c ⇒ a | c

Tétel: Bármely a, b, c ∈ **Z**-re

1. ha a | b és a | c ⇒ a | b + c additív tulajdonság
2. ha a | b és c | d ⇒ ac | bd multiplikatív tulajdonság

A 0 csak önmagának osztója, de a nullát bármely szám osztja.

Legnagyobb közös osztó

Def: Az *a* és *b* (≠0) egész számok legnagyobb közös osztójának nevezünk egy *d* egész számot, ha

1. d közös osztó, azaz d | a és d | b
2. d a közös osztók közül a legnagyobb, azaz d' | a és d' | b ⇒ d' | d

Jele: (a, b) = d

Tétel: Ha a, b nem mindkettő0, akkor ∃ legnagyobb közös osztó, előjeltől eltekintve egyértelműen meghatározott.

Tétel: Bármely a, b (≠0), c ∈ **N** igazak a következő tulajdonságok:

1. (a, b) = (b, a) kommutatív
2. ((a, b), c) = (a, (b, c)) asszociatív
3. (b, b) = b idempotens
4. (a, b)c = (ac, bc) ha c≠ 0
5. (a, b) = b ⇔ b | a elnyelés
6. (a, b) = (a + kb, b), ahol k∈ **Z**

Tétel: Bármely a, b (≠0) ∈ **N** igaz, hogy

$$\left[\frac{a}{(a,b)}; \frac{b}{(a,b)}\right] = 1$$

Def: Legyen a, b(≠0) ∈ **Z** és m ∈ **Z**. Azt mondjuk, hogy a és b egészek legkisebb közös többszöröse az az m egész,

1. m közös többszörös, azaz $a \mid m \wedge b \mid m$,
2. m közös többszörösök közül a legkisebb, ha $\exists\, m' \in \mathbf{Z}$, hogy $a \mid m' \wedge b \mid m' \Rightarrow m \mid m'$

Jele: $[a, b]$

Tétel: Ha a, b $\in \mathbf{Z}/\{0\}$ egészeknek $\exists$ legkisebb közös többszöröse, azaz az asszociáltság erejéig egyértelműen meghatározott.

Tétel: $\forall$ a, b, c $\in \mathbf{Z}^+$ igazak az alábbi tulajdonságok:

1. $[a,b]=[b,a]$ kommutatív
2. $[[a,b],c]=[a[b,c]]$ asszociatív
3. $[a,a]=[a]$ idempotens
4. $[a,b]c=[ac,bc]$
5. $[a,b]=b \Leftrightarrow a \mid b$ elnyelés

Tétel: Bármely a, b $\in \mathbf{Z}^+$-nak van legkisebb közös többszöröse

$$[a, b] = \frac{ab}{(a,b)}$$

Irreducibilis és prímszámok

Faktorizáció: Ha egy egész számot 2 egész szám szorzatára bontjuk, akkor faktorizálásról beszélünk.

Def: A 0-tól és ±1-től különböző p egész számot **irreducibilis**nek (felbonthatatlannak) nevezzük, ha nincs valódi osztója (faktorizációja). Ellenkező esetben p **reducibilis**.

Def: A 0-tól és a ±1-től különböző p egész számot **prím**nek nevezzük, ha az valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat legalább egyik tényezőjének. (azaz a, b $\in \mathbf{Z}$, $p \mid ab$, de $p \nmid a \Rightarrow p \mid b$)

Tétel: A ($\mathbf{Z}$, +, ·) integritástartományban az irreducibilis egészek és a prímek megegyeznek. (azaz a p egész szám $\Leftrightarrow$ irreducibilis, ha prím)

A számelmélet alaptétele

Minden 0, ±1-től különböző egész szám sorrendtől és egységtényezőként eltekintve egyértelműen állítható elő véges sok prímszám szorzataként, ahol prímszámokon a pozitív prímeket értjük és az egytényezős szorzat is megengedett.

Következménye a kanonikus felbontás.

$n \in \mathbf{N}$; $p \geq 2 \Rightarrow n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ $\alpha_i \geq 1$

Tétel: Ha n ≥ 2 természetes számnak nincs $\sqrt{n}$-nél nem nagyobb osztója, akkor n prímszám, azaz minden összetett természetes számnak van négyzetgyökénél nem nagyobb prímosztója.

Nevezetes prímek

Def: Ha egy n pozitív egész összetett és kielégíti az $n \mid (2^{n-1} - 1)$, azaz $2^{n-1} \equiv 1 \pmod{n}$, akkor **pszeudoprím** (száma végtelen) számnak nevezzük.

Tétel: Ha n egy pszeudoprím szám, akkor 2^{n-1} is pszeudoprím.

Tétel: Ha n ≥ 0 természetes szám és $F_n = 2^{2^n} + 1$ nem prím, akkor pszeudoprím. F_n **Fermat-szám**, n = 0, 1, 2, 3, 4-re prím!

Tétel: Legyen p > 2 egy prímszám. Ekkor $M_p = 2^p - 1$ vagy prím vagy pszeudoprím. M_p **Mersenne-szám**. M_2, M_3, M_5, M_7 prímek, M_{11} nem!

Ma 34 darab ilyen prímet ismerünk. Szükséges, de nem elégséges, hogy p prím.

Pszeudoprímek: $n \in \mathbf{Z}^+$, $(a, n) = 1$ n összetett

$n \mid a^{n-1} - 1$

ha a Mersenne és Fermat számok nem prímek, akkor a = 2-re pszeudoprímek.

A prímek végtelensége

Tétel: A prímszámok száma végtelen.

Tétel: Dirichlet

Végtelen sok $4k + 1$ és $4k - 1$ alakú prímszám van.

Tétel: Megadható két pozitív valós szám c_1, c_2 úgy, hogy az n-nél nem nagyobb prímszámok reciprokösszegére, ha n elég nagy

$$c_1 \log(\log n) < \sum_{p \le n} \frac{1}{p} < c_2 \log(\log n)$$

$$\Downarrow$$

aszimmetrikus egyenlőség is igaz: $\sum_{p \le n} \frac{1}{p} \sim \log(\log n)$

Tétel: Bertrand posztolátum

Ha n egész szám és $n > 1$, akkor az $(n, 2n)$ nyílt intervallum tartalmaz legalább egy prímet.

Izolált prímek: sem előtte, sem utána nincs prím.

Kongruenciák

Def: Legyen $a, b, m \in \mathbf{Z}$, ahol m rögzített. Az *a* egész számot **kongruens**nek nevezzük *b*-vel az m modulusra nézve, ha $m \mid (a - b)$

Jelölés: $a \equiv b \pmod m$

„ $\equiv$ ” reflexív, szimmetrikus, tranzitív (ekvivalenciareláció), additív, multiplikatív

Tétel: Bármely $a, b, c, d \in \mathbf{Z}$-re igazak a következő tulajdonságok:

1. $a \equiv a \pmod m$ reflexív
2. ha $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ szimmetrikus
3. ha $a \equiv b \pmod m$ és $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ tranzitív
4. ha $a \equiv b \pmod m$ és $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$ additív és $a \cdot c \equiv b \cdot d \pmod m$ multiplikatív

Tehát a kongruencia kongruenciareláció $(\mathbf{Z}, +, \cdot)$ integritástartományon, struktúrán.

Tétel: Bármely egész számra igaz, $a, b, c \in \mathbf{Z}$

1. ha $a \equiv b \pmod m$ és $m_1 \mid m \Rightarrow a \equiv b \pmod{m_1}$
2. ha $a \cdot c \equiv b \cdot c \pmod m \Rightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$
3. ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2} \Rightarrow a \equiv b \pmod{[m_1, m_2]}$

Maradékosztályok (kongruencia szerint)

Def: A kongruenciareláció a $(\mathbf{Z}, +, \cdot)$ integritástartomány kompatíbilis osztályozását adja. Egy osztályba tartoznak azok az a és b egészek, melyekre $a \equiv b \pmod m$ igaz, azaz m-mel osztva ugyanazt a legkisebb nemnegatív maradékot adják.

Az ilyen osztályokat modulo m **maradékosztály**oknak nevezzük. Az osztályok halmazát modulo m **faktorhalmaz**nak nevezzük.

Def: Azokat a modulo m maradékosztályokat, amelyeknek az elemei m-hez relatív prímek, **redukált maradékosztályok**nak nevezzük. Száma $\varphi(m)$

$\varphi(m) = 1$, ha $m = 1$ és ha $m > 1$, akkor $\varphi(m) = 0, 1, 2, \ldots, m - 1$ közül a relatív prímek száma.
Jele: P(m)

Redukált reprezentáns rendszer
Pontosan egy reprezentánst választunk ki minden modulo m maradékosztályból

$$\varphi: \mathbf{N} / \{0\} \to \mathbf{N}, \varphi(m) = \begin{cases} 1, \text{ ha } m = 1 \text{ Euler-féle } \varphi \text{ függvény} \\ k, \text{ ha } m \geq 2 \end{cases}$$

Tétel: Euler-Fermat-tétel
Ha $a \in \mathbf{Z}$ és $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Tétel: Kis Fermat-tétel
Legyen p prím. Ha $(p, a) = 1 \Rightarrow a^{p-1} = 1 \pmod p$ vagy $a^p \equiv a \pmod p$

A $(\mathbf{Z}/_{(m)}, +, \cdot)$ faktorstruktúrában az összeadás és a szorzás műveletek a következők:

1. $\bar{a} + \bar{b} = \overline{a+b}$, ahol $\bar{a}, \bar{b} \in \mathbf{Z}/_{(m)}$
2. $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$, ahol $\bar{a}, \bar{b} \in \mathbf{Z}/_{(m)}$

Tétel: A $(\mathbf{Z}/_{(m)}, +, \cdot)$ struktúra egységelemes kommutatív gyűrű.

Tétel: A $(\mathbf{Z}/_{(m)}, +, \cdot) \Leftrightarrow$ test, ha m prím.

Tétel: Wilson-tétel
Az $m \geq 2$ egész szám $\Leftrightarrow$ prím, ha $(m - 1)! \equiv -1 \pmod m$

Algebrai kongruenciák
Def: Legyen f(x) modulo m n-edfokú ($n \geq 1$) egész együtthatós polinom.
Az $f(x) \equiv 0 \pmod m$ kongruenciát **n-edfokú egyismeretlenes algebrai kongruenciának** nevezzük, ha $f(x_0) \equiv 0 \pmod m$ és ha x_0 megoldás, akkor $\overline{x_0}$ maradékosztály minden eleme is megoldás.

Def: Lineáris kongruencia
Az $a \cdot x \equiv b \pmod m$ algebrai kongruenciát, ahol $a \equiv 0 \pmod m$ **lineáris kongruenciának** nevezzük.

Tétel: Az $a \cdot x \equiv b \pmod m$ lineáris kongruencia $\Leftrightarrow$ oldható meg, ha $(a, m) = d \mid b$, továbbá ha megoldható, akkor az inkongruens megoldások száma: d. Ha x_0 egy megoldás, akkor az összes inkongruens megoldás.

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d - 1)\frac{m}{d}$$

Tétel: Kínai maradéktétel
Ha az $a_1 x \equiv b_1 \pmod m$
$a_2 x \equiv b_2 \pmod m$
$\vdots$
$a_n x \equiv b_n \pmod m$, ahol $n > 1$ lineáris kongruenciarendszerben az $m_1, m_2, \ldots, m_n$ modulusok páronként relatív prímek, továbbá $(a_i, m_i) = 1$ minden $1 \leq i \leq n$-re $\Rightarrow$ tetszőleges b_i egészek esetén megoldható és a megoldás modulo $[m_1, m_2, \ldots, m_n]$-re nézve egyértelmű.

Magasabb fokú kongruenciák

Az $f(x) \equiv a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}$ n-edfokú kongruencia redukciós eljárással oldható meg: - együtthatók redukciója
- modulus redukciója
- fokszám redukciója → prím modulus esetén

Tétel: Fokszám tétel

Az $f(x) \equiv 0 \pmod{p}$ prímmoduludú n.edfokú kongruenciának legfeljebb n inkongruens megoldása van. Soha nem lehet több megoldása mint foka!

Binom kongruenciák

Def: Az $ax^k \equiv b \pmod{m}$ kongruenciát, ahol $a \not\equiv 0 \pmod{m}$ és $k \in \mathbf{N}^+$, **k-adfokú binom kongruenciának** nevezzük.

Def: Rend

Legyen $(a, p) = 1$ és p prím. Azt a legkisebb pozitív k egész számot, melyre $a^k \equiv 1 \pmod{p}$ azt az egész szám **rendjének** nevezzük $(\bmod p)$.

Tétel: Ha $a \equiv b \pmod{p}$ és *a* rendje k modulo p, akkor *b* rendje is k modulo p.

Def: A g egész számot **primitív gyök**nek nevezzük modulo p, ha $(g, p) = 1$ és g rendje $p - 1$ modulo p.

Def: Index (diszkrét logaritmus)

Legyen g primitív gyök modulo p és $(a, p) = 1$. Az a egész szám g alapú modulo p indexének nevezzük és $\mathrm{ind}_g a$-val jelöljük azt a legkisebb természetes számot, melyre

$g^{\mathrm{ind}_g a} \equiv a \pmod{p}$.

Tétel: Legyenek g és q primitív gyökök modulo p, továbbá legyen $(a, p) = (b, p) = 1$ és $k \in \mathbf{N}$. Ekkor

a) $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g a + \mathrm{ind}_g b \pmod{p-1}$

b) $\mathrm{ind}_g a^k \equiv k \cdot \mathrm{ind}_g a \pmod{p-1}$

c) $\mathrm{ind}_g a \equiv (\mathrm{ind}_q a)(\mathrm{ind}_g q) \pmod{p-1}$

Tétel: Az $x^k \equiv a \pmod{p}$ $(p \nmid a)$ kongruencia akkor és csak akkor oldható meg, ha

$(k, p-1) \mid \mathrm{ind}_g a$,

vagy ami ezzel ekvivalens, ha

$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}$.

Tétel: Az $x^2 \equiv a \pmod{p}$ $(p \nmid a, p > 2)$ kongruencia akkor és csak akkor oldható meg, azaz, a akkor és csak akkor kvadratikus maradék modulo p, ha

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$,

vagy ami ezzel ekvivalens, ha

$2 \mid \mathrm{ing}_g a$,

ahol g primitív gyök modulo p. ha megoldható, akkor az inkongruens megoldások száma 2.

Tétel: Euler-lemma

Legyen $p > 2$ és $p \nmid a$. Ekkor

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p, \text{ ha a kvadratikus maradék modulo p,} \\ -1 \pmod p, \text{ ha a nem kvadratikus maradék modulo p.} \end{cases}$$

Tétel: Legrende-szimbólum

Legyen $p > 2$ prím és $p \nmid a$. Ekkor az

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ ha a kvadratikus maradék modulo p,} \\ -1, \text{ ha a nem kvadratikus maradék modulo p} \end{cases}$$

Egyenlőséggel definiált $\left(\frac{a}{p}\right)$ számot Legrende-szimbólumnak nevezzük.

Tétel: Gauss-lemma

Legyen $p > 2$ és $p \nmid a$. Tekintsük az

$$a, 2a, 3a, \ldots, \frac{p-1}{2}\, a$$

számot modulo p vett legkisebb pozitív maradékait. Legyen ezek között m darab, amely nagyobb, mint $\frac{p}{2}$. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^m,$$

Azaz m paritása már meghatározza az a kvadratikus karakterét.