

Számelmélet tételsor

Bácsi László
lackac@math.bme.hu

2002. december 10.

Tartalomjegyzék

1	Elemi számelmélet	1
1.1	Oszthatóság	1
1.2	Maradékos osztás	1
1.3	LegNagyobb Közös Osztó	1
1.4	Lineáris diofantoszi egyenletek	3
1.5	Prímszámok	3
2	Kongruenciák	4
2.1	Kongruenciák tulajdonságai	5
2.2	Maradékosztályok, maradékrendszerek	6
2.3	Euler- és Fermat-tételek	7
2.4	Moduláris aritmetika	7
3	Lineáris kongruenciák	8
3.1	Lineáris kongruenciák megoldása	8
3.2	Lineáris kongruenciarendszerek	8
4	Magasabb fokú kongruenciák	9
4.1	Magasabb fokú kongruenciák megoldása	9
4.2	Polinomok modulo prím	10
5	Rend, hatványmaradékok	10
5.1	Rend	10
5.2	Négyzetes (kvadratikus) maradékok	11
6	Számelméleti függvények	13
6.1	Függvénydefiníciók, multiplikatívitas, additivitás	13
6.2	Összegzések	15
6.3	Minimális univerzális kitevő (exponens)	17

1 Elemi számelmélet

1.1 Oszthatóság

DEFINÍCIÓ 1.1.1.

$a, b \in \mathbb{Z}$,

a osztója b -nek, ha $\exists q \in \mathbb{Z} : b = qa$.

TÉTEL 1.1.2.

Az oszthatóság $\mathbb{N}$ -en *részbenrendezés*

TÉTEL 1.1.3.

$a, b, c, m, n \in \mathbb{Z} : c \mid a, c \mid b \Rightarrow c \mid (am + bn)$

Általánosítva: $a_i, m_i, c \in \mathbb{Z} : c \mid a_i, 1 \leq i \leq k \Rightarrow c \mid \sum_{i=1}^k a_i m_i$

TÉTEL 1.1.4.

$a \mid b, b \neq 0 : a, b \in \mathbb{Z} \Rightarrow 0 < |a| \leq |b|$

TÉTEL 1.1.5.

$n \neq 0, a \mid b \Leftrightarrow na \mid nb$

1.2 Maradékösztás

TÉTEL 1.2.1 (MARADÉKOS OSZTÁS).

$a, b \in \mathbb{N}^+, b \neq 0 : \exists! q, r \in \mathbb{N} : a = bq + r$ és $0 \leq r < b$

Általánosítva: $a, b \in \mathbb{Z}, b \neq 0 : \exists! q, r \in \mathbb{Z} : a = bq + r$ és $0 \leq r < b$

Megjegyzés: $a = bq + r$ -nél: $q = \begin{cases} \left\lfloor \frac{a}{b} \right\rfloor & \text{ha } b > 0 \\ \left\lceil \frac{a}{b} \right\rceil & \text{ha } b < 0 \end{cases}$

TÉTEL 1.2.2.

$t > 1, t, n \in \mathbb{Z}^+, \exists! a_1, \dots, a_m \in \mathbb{Z}, a_m \neq 0, 0 \leq a_i < t, (1 \leq i \leq m)$

$$n = a_m t^m + a_{m-1} t^{m-1} + \dots + a_1 t + a_0$$

1.3 LegNagyobb Közös Osztó

DEFINÍCIÓ 1.3.1.

Legyen $a, b \in \mathbb{Z}$, nem mindkettő 0, a és b *legnagyobb közös osztója* c , ha $c > 0$, közös osztó, és $\forall d$ közös osztóra $d \leq c$

Jelölés: $(a, b), \gcd(a, b), \text{luko}(a, b)$

DEFINÍCIÓ 1.3.2.

$a, b \in \mathbb{Z}$ relatív prímek, ha $(a, b) = 1$

Általánosítva: $a_1, \dots, a_n$ relatív prímek, ha $(a_1, \dots, a_n) = 1$

páronként relatív prímek, ha $\forall i < j : (a_i, a_j) = 1 \quad (1 \leq i, j \leq n)$

TÉTEL 1.3.3.

$$d = (a, b) \Rightarrow \exists m, n \in \mathbb{Z} : d = am + bn$$

TÉTEL 1.3.4.

$d \in \mathbb{N}^+, a, b \in \mathbb{Z}$ nem mindkettő 0. Az alábbi állítások ekvivalensek:

1. $d = (a, b)$
2. $d = \min \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$
3. d közös osztó és $\forall c$ közös osztóra $c \mid d$

TÉTEL 1.3.5 (LNKO TULAJDONSÁGAI).

1. $\forall c \in \mathbb{N}^+ : (ca, cb) = c(a, b)$
2. $(a, c) = (b, c) = 1 \Rightarrow (ab, c) = 1$
3. $a, b, c \in \mathbb{Z} : (a, b) = (b, a) = (a, -b) = (a, b + ac)$
4. $c \mid ab, (a, c) = 1 \Rightarrow c \mid b$

TÉTEL 1.3.6.

$a, b \in \mathbb{N}^+$

$$\begin{array}{ll} a = bq_1 + r_1 & 0 < r_1 < b \\ b = r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 < r_3 < r_2 \\ \vdots & \vdots \\ r_{k-2} = r_{k-1}q_k + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} = r_kq_{k+1} & \end{array}$$

A fenti egyenletek sorozata véges és $r_k = (a, b)$

1.4 Lineáris diofantoszi egyenletek

TÉTEL 1.4.1.

Az $ax + by = m$ egyenlet

1. megoldható $\Leftrightarrow (a, b) \mid m$
2. ha x_0, y_0 jó megoldás $\Rightarrow$ az összes megoldás:

$$x = x_0 + \frac{b}{(a, b)}k, \quad y = y_0 - \frac{a}{(a, b)}k$$

TÉTEL 1.4.2.

$a, b > 0, ax + by = m$ pozitív megoldásainak száma egyenlő azon k értékek számával, melyekre $-(a, b)\frac{x_0}{b} < k < (a, b)\frac{y_0}{a}$

1.5 Prímszámok

DEFINÍCIÓ 1.5.1.

A $p > 1$ egészt *felbonthatatlannak* (*irreducibilisnek*) nevezzük, ha

$p = ab \Rightarrow a$ vagy b egység.

Megjegyzés: ezzel ekvivalens: $p > 1$ felbonthatatlan, ha 1-en és önmagán kívül nincs pozitív osztója.

DEFINÍCIÓ 1.5.2.

A $p > 1$ egész *prím*, ha $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

TÉTEL 1.5.3.

$p \in \mathbb{N}$ prím $\Leftrightarrow p$ felbonthatatlan.

LEMMA 1.5.4.

$n > 1 \Rightarrow$ van felbonthatatlan osztója.

TÉTEL 1.5.5 (SZÁMELMÉLET ALAPTÉTELE).

$\forall n > 1$ egész egyértelműen előáll prímelem nem csökkenő sorozatának szorzataként.

DEFINÍCIÓ 1.5.6.

$n > 1$, n *kanonikus alakja*:

$n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$, ahol $\alpha_i > 0$ ($i = 1, \dots, r$) ($p_1 < p_2 < \dots < p_r$)

TÉTEL 1.5.7 (KANONIKUS ALAKRÓL).

1. $a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ -nek d osztója $\Leftrightarrow d = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}$ $0 \leq \beta_i \leq \alpha_i$

2. a osztóinak száma: $\delta(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_r + 1)$

3. $a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ ($\alpha_i \geq 0$), $b = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}$ ($\beta_i \geq 0$)

$$(a, b) = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)} \quad [a, b] = \prod_{i=1}^r p_i^{\max(\alpha_i, \beta_i)}$$

TÉTEL 1.5.8 ($n!$ KANONIKUS ALAKJA).

1. p prím $e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \Rightarrow p^e \parallel n!$ ($p^e \mid n!$, de $p^{e+1} \nmid n!$)

2. $n! = \prod_{p \leq n} p^{e_p}$, ahol $e_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$

DEFINÍCIÓ 1.5.9.

$a, b \in \mathbb{Z}$ legkisebb közös többszöröse az a legkisebb $c \geq 0, c \in \mathbb{Z}$, melyre $a \mid c, b \mid c$

Jelölés: $[a, b] = c$

TÉTEL 1.5.10 (LKKT TULAJDONSÁGAI).

1. $[0, 0] = 0, [a, 0] = 0, [a, a] = |a|$

2. $a \mid b \Rightarrow [a, b] = |b|$

3. $[a, b] = n \in \mathbb{N}$:

- $a \mid n, b \mid n$
- $a \mid m, b \mid m \Rightarrow n \mid m$

4. $a, b = |a, b|$

TÉTEL 1.5.11 (LAME).

A legnagyobb közös osztó megtalálásában az euklidészi algoritmusban szükséges lépések száma $\leq 5 \cdot$ a kisebbik szám számjegyeinek a száma.

2 Kongruenciák

DEFINÍCIÓ 2.0.12.

Ha $a \in \mathbb{Z}$ és $m \in \mathbb{Z} \setminus \{0\}$, akkor a -nak m -mel vett (legkisebb nemnegatív) osztási maradékát $a \bmod m$ jelöli.

DEFINÍCIÓ 2.0.13.

$$x, y \in \mathbb{R}, y \neq 0 \quad x \bmod y := x - |y| \left\lfloor \frac{x}{|y|} \right\rfloor$$

DEFINÍCIÓ 2.0.14.

$m \neq 0, m \in \mathbb{Z}$ Azt mondjuk, hogy a kongruens b -vel modulo m , ha $a \bmod m = b \bmod m$

Jelölés: $a \equiv b \pmod{m}$, $a \equiv b (m)$

2.1 Kongruenciák tulajdonságai

TÉTEL 2.1.1.

1. $a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{-m}$
2. $\forall a, b \in \mathbb{Z}: a \equiv b \pmod{1}$
3. $a \equiv b \pmod{m}, b \equiv a \pmod{m}, a - b \equiv 0 \pmod{m}, m \mid b - a$ ekvivalensek

$$4. a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$\Rightarrow a \equiv b \pmod{m}$ ekvivalenciareláció (reflexív, szimmetrikus, tranzitív)

$$5. a \equiv b \pmod{m} \Leftrightarrow a \equiv b + mq \pmod{m} (q \in \mathbb{Z})$$

$$6. a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow$$

- $a \pm c \equiv b \pm d \pmod{m}$
- $ac \equiv bd \pmod{m}$

$$\Rightarrow a \equiv b \pmod{m} \Rightarrow$$

- $a + c \equiv b + c \pmod{m}$
- $ac \equiv bc \pmod{m}$
- $a^n \equiv b^n \pmod{m} (n \in \mathbb{N}^+)$

$$\Rightarrow f \text{ tetszőleges egész együtthatós polinom } (f \in \mathbb{Z}[x]), \text{ és } a \equiv b \pmod{m} \\ \Rightarrow f(a) \equiv f(b) \pmod{m}$$

TÉTEL 2.1.2 (KONGRUENCIÁK KAPCSOLATA).

1. $a \equiv b \pmod{m}, d \mid m \Rightarrow a \equiv b \pmod{d}$
2. $a \equiv b \pmod{m}, c \neq 0 \Rightarrow ac \equiv bc \pmod{mc}$

3. $ax \equiv bx \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(x,m)}}$
4. $ax \equiv bx \pmod{m}, (x,m) = 1 \Rightarrow a \equiv b \pmod{m}$
5. $a \equiv b \pmod{m_i}, i = 1, 2, \dots, r \Leftrightarrow a \equiv b \pmod{[m_1, \dots, m_r]}$

2.2 Maradékosztályok, maradékrendszerek

DEFINÍCIÓ 2.2.1.

Az a -val kongruens $\pmod{m}$ számok halmazát az a által reprezentált *maradékosztálynak* nevezzük.

Jelölés: $[a]_m, [a] \pmod{m}, (a)_m, (a) \pmod{m}, [a], (a), a$

DEFINÍCIÓ 2.2.2.

modulo m teljes maradékrendszer m szám halmaza, melyben minden maradékosztályból van reprezentáns.

LEMMA 2.2.3.

$$a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$$

DEFINÍCIÓ 2.2.4.

modulo m redukált maradékrendszer m -hez relatív prím, $\pmod{m}$ inkongruens egészek olyan halmaza, mely $\varphi(m)$ elemű.

ÁLLÍTÁS 2.2.5.

1. $T \subseteq \mathbb{Z}$ tmrsz. $\pmod{m} \Leftrightarrow$
 - $|T| = m$
 - $r_i, r_j \in T : r_i \not\equiv r_j \pmod{m}$
2. $R \subseteq \mathbb{Z}$ rmrsz. $\pmod{m} \Leftrightarrow$
 - $|R| = \varphi(m)$
 - $r_i, r_j \in R : r_i \not\equiv r_j \pmod{m}$
 - $(r_i, m) = 1 \ (\forall i \in R)$

TÉTEL 2.2.6.

$(a, m) = 1$ és $\{r_1, \dots, r_k\}$ teljes/redukált mrsz. $\pmod{m}$
 $\Rightarrow \{ar_1, \dots, ar_k\}$ is teljes/redukált mrsz. $\pmod{m}$

2.3 Euler- és Fermat-tételek

TÉTEL 2.3.1 (KIS-FERMAT-TÉTEL).

- p prím $\Rightarrow a^p \equiv a \pmod{p}$
- p prím, $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

TÉTEL 2.3.2 (EULER-FERMAT-TÉTEL).

$$(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

ÁLLÍTÁS 2.3.3.

$$(m, n) = 1 \Rightarrow \varphi(m, n) = \varphi(m)\varphi(n)$$

ÁLLÍTÁS 2.3.4.

$$\begin{aligned} \varphi(p^\alpha) &= p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p}) \\ \Rightarrow n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} &\Rightarrow \varphi(n) = n \prod_{i=1}^r (1 - \frac{1}{p_i}) \end{aligned}$$

2.4 Moduláris aritmetika

DEFINÍCIÓ 2.4.1.

- $[a]_m + [b]_m := [a + b]_m$
- $[a]_m \cdot [b]_m := [ab]_m$

PÉLDA 2.4.2.

(mod 5) művelet táblák

+	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

és

*	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

ÁLLÍTÁS 2.4.3.

A $(\text{mod } m)$ maradékosztályok a fenti két művelettel kommutatív egységelemes gyűrűt adnak.

Ha m prím $\Rightarrow$ a maradékosztályok testet adnak.

DEFINÍCIÓ 2.4.4.

$[a]_m$ inverze $[\bar{a}]_m$: $[a]_m \cdot [\bar{a}]_m = [1]_m$ $a\bar{a} \equiv 1 \pmod{m}$

($[a]_m$ invertálható, ha $\exists$ inverze)

Jelölés: $[a]_m^{-1}$, $a^{-1} \pmod{m}$

TÉTEL 2.4.5.

1. a invertálható $\pmod{m} \Leftrightarrow (a, m) = 1$
2. a invertálható $\pmod{m} \Rightarrow \pmod{m}$ egyértelmű

3 Lineáris kongruenciák

3.1 Lineáris kongruenciák megoldása

TÉTEL 3.1.1.

1. $ax \equiv b \pmod{m}$ megoldható $\Leftrightarrow (a, m) \mid b$
2. a megoldások száma: (a, m)

Megjegyzés: $ax \equiv b \pmod{m} \Leftrightarrow ax + my = b$

TÉTEL 3.1.2 (WILSON).

1. p prím $\Rightarrow (p-1)! \equiv -1 \pmod{p}$
 2. $m = 4 \Rightarrow (m-1)! \equiv 2 \pmod{m}$
 3. $m > 4 \Rightarrow (m-1)! \equiv 0 \pmod{m}$
- $\Rightarrow m > 1$ prím $\Leftrightarrow (m-1)! \equiv -1 \pmod{m}$

3.2 Lineáris kongruenciarendszerek

TÉTEL 3.2.1.

1. $\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{array} \right\}$ megoldható $\Leftrightarrow (m_1, m_2) \mid c_2 - c_1$
2. $\exists! \pmod{[m_1, m_2]}$

TÉTEL 3.2.2 (KÍNAI MARADÉKTÉTEL).

$m_1, \dots, m_r > 0$ páronként relatív prímek,

$a_1, \dots, a_r \in \mathbb{Z}$ ekkor az

$$\left. \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{array} \right\} \begin{array}{l} \text{szimultán lineáris} \\ \text{kongruenciarendszer} \\ \text{megoldható} \\ \exists! \text{ mo. } \pmod{[m_1, \dots, m_r]} \end{array}$$

azaz $\forall \text{ mo. } x = x_0 + km_1 \cdot \dots \cdot m_r \quad (k \in \mathbb{Z})$ alakú

4 Magasabb fokú kongruenciák

4.1 Magasabb fokú kongruenciák megoldása

TÉTEL 4.1.1.

Tetszőleges n -edfokú polinom kongruens egy legfeljebb $p - 1$ -edfokú polinommal $(\text{mod } p)$, ha p prím.

DEFINÍCIÓ 4.1.2.

A k egész az $f(x) \equiv 0 \pmod{m}$ polinom kongruencia egy *megoldása*, ha $f(k) \equiv 0 \pmod{m}$.

TÉTEL 4.1.3.

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ egészegyütthatós

$\Rightarrow f(x+y) = f(x) + yf'(x) + y^2 g(x, y)$ Ezt felhasználva:

$$f(a+tp) = f(a) + tpf'(a) + t^2 p^2 g(a, tp) \equiv f(a) + tpf'(a) \pmod{p^2}$$

Ha $f(a) \equiv 0 \pmod{p}$ és $f(a+tp) \equiv 0 \pmod{p^2}$, akkor p -vel osztva:

$$tf'(a) \equiv -(f(a)/p) \pmod{p}$$

és ennek a lineáris kongruenciának egyetlen megoldása van.

TÉTEL 4.1.4.

Legyen a az $f(x) \equiv 0 \pmod{p^r}$ egy megoldása.

1. $p \nmid f'(a) \Rightarrow f(x) \equiv 0 \pmod{p^{r+1}}$ egyetlen megoldása $x = a + p^r t$, ahol t az egyetlen megoldása a $p^r t f'(a) \equiv -f(a) \pmod{p^{r+1}}$ kongruenciának.
2. $p \mid f'(a)$ és $p^{r+1} \mid f(a) \Rightarrow f(x) \equiv 0 \pmod{p^{r+1}}$ megoldásainak száma p , és ezek alakja $x \equiv a + p^r t \pmod{p^{r+1}}$, t tetszőleges.

3. $p \mid f'(a)$ és $p^{r+1} \nmid f(a) \Rightarrow f(x) \equiv 0 \pmod{p^{r+1}}$ nem oldható meg úgy, hogy $x \equiv a \pmod{p^r}$ legyen.

4.2 Polinomok modulo prím

TÉTEL 4.2.1.

Ha f n -edfokú polinom, p prím és f nem mindegyik együtthatója osztható p -vel, akkor az $f(x) \equiv 0 \pmod{p}$ kongruenciának legfeljebb n megoldása van $\pmod{p}$.

TÉTEL 4.2.2.

$F : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \Rightarrow \exists f \max(p-1)$ -edfokú polinom : $F(x) \equiv f(x) \pmod{p} \forall x$

TÉTEL 4.2.3.

$f(x) \equiv 0 \pmod{p}$, f n -edfokú, főegyütthatója 1

f -nek pontosan n különböző megoldása van $\Leftrightarrow f(x)$ az $x^p - x$ tényezője.

$$x^p - x = f(x) \cdot q(x) + p \cdot s(x), \deg q = p - n, \deg s < n$$

Következmény: $d \mid p - 1 \Rightarrow x^d \equiv 1 \pmod{p}$ kongruenciának d különböző megoldása van.

5 Rend, hatványmaradékok

5.1 Rend

DEFINÍCIÓ 5.1.1.

$m > 0$, $m, a \in \mathbb{Z}$, $(a, m) = 1$ Azt mondjuk, hogy

a rendje h , ha $a^h \equiv 1 \pmod{m}$, de $a^k \not\equiv 1 \pmod{m}$, ha $0 < k < h$

Jelölés: $\text{ord}_m a = h$, $o_m(a) = h$

TÉTEL 5.1.2 (REND TULAJDONSÁGAI).

$$1. \text{ord}_m a = h \Rightarrow a^k \equiv 1 \pmod{m} \Leftrightarrow h \mid k$$

$$\Rightarrow (a, m) = 1 \Rightarrow \text{ord}_m a \mid \varphi(m)$$

$$\Rightarrow (a, m) = 1, a^i \equiv a^j \pmod{m} \Leftrightarrow i \equiv j \pmod{\text{ord}_m a}$$

$$2. \text{ord}_m a = h \Rightarrow \text{ord}_m a^k = \frac{h}{(h, k)}$$

DEFINÍCIÓ 5.1.3.

g primitív gyök $\pmod{m}$, ha $\text{ord}_m g = \varphi(m)$

TÉTEL 5.1.4.

m -nek ($m > 1$) pontosan akkor van primitív gyöke, ha $m = 2$ vagy $m = 4$ vagy $m = p^\alpha$ vagy $m = 2 \cdot p^\alpha$, ahol p páratlan prím és $\alpha > 0$.

TÉTEL 5.1.5.

$a \pmod{m}$ primitív gyökök száma $\varphi(\varphi(m))$.

DEFINÍCIÓ 5.1.6.

p prím, $(a, p) = 1$ és $x^n \equiv a \pmod{p}$ -nek van megoldása, akkor a n . *hatványmaradék*.

DEFINÍCIÓ 5.1.7.

g primitív gyök $\pmod{m}$, $(a, m) = 1$ és $g^n \equiv a \pmod{m} \Rightarrow \text{ind}_g a = n$ (n a -nak g alapú indexe) ($1 \leq n \leq \varphi(m)$).

Megjegyzés: az index ugyanúgy működik, mint a logaritmus.

TÉTEL 5.1.8.

p prím $(a, p) = 1$ a $x^n \equiv a \pmod{p}$ kongruenciának

$$\begin{array}{l} (n, p-1) \text{ megoldása van} \\ 0 \text{ megoldása van} \end{array} \Leftrightarrow \begin{array}{l} a^{\frac{p-1}{(n, p-1)}} \equiv 1 \pmod{p} \\ a^{\frac{p-1}{(n, p-1)}} \not\equiv 1 \pmod{p} \end{array} \Leftrightarrow \begin{array}{l} (n, p-1) \mid \text{ind}_g a \\ (n, p-1) \nmid \text{ind}_g a \end{array}$$

5.2 Négyzetes (kvadratikus) maradékok

DEFINÍCIÓ 5.2.1.

$(a, m) = 1$, a négyzetes (kvadratikus) maradék/nemmaradék, ha $x^2 \equiv a \pmod{m}$ -nek van/nincs megoldása.

DEFINÍCIÓ 5.2.2.

p páratlan prím, ekkor $\left(\frac{a}{p}\right)$ -t Legendre-jelnek (Legendre-szimbólumnak) nevezzük és a következőképp definiáljuk:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{akvadratikus maradék} \\ -1, & \text{akvadratikus nemmaradék} \\ 0 & a \equiv 0 \pmod{p} \end{cases}$$

TÉTEL 5.2.3 (A LEGENDRE-JEL TULAJDONSÁGAI).

p páratlan prím

$$1. \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$2. \text{ a kvadratikus maradékok száma } \pmod{p} \frac{p-1}{2}$$

$$3. \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right), \quad \left(\frac{a_1}{p}\right) \cdot \dots \cdot \left(\frac{a_k}{p}\right) = \left(\frac{a_1 \dots a_k}{p}\right)$$

$$4. a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

$$5. (a, p) = 1 \Rightarrow \left(\frac{a^2}{p}\right) = 1, \quad \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$$

$$6. \left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p = 4k+1 \\ -1, & p = 4k-1 \end{cases}$$

$\Rightarrow x^2 + 1 \equiv 0 \pmod{p}$ megoldható, ha $p = 4k+1$, nem megoldható ha $p = 4k-1$, a megoldás $\pm \left(\frac{p-1}{2}\right)!$

TÉTEL 5.2.4 (GAUSS-LEMMA).

$(a, p) = 1$, tekintsük $a, 2a, \dots, \frac{p-1}{2}a$ számok legkisebb abszolútértékű maradékát $\pmod{p}$ és legyen m a negatívok száma.

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

TÉTEL 5.2.5.

p páratlan prím

$$1. (a, 2p) = 1 \Rightarrow \left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ai}{p} \right\rfloor}$$

$$2. \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

LEMMA 5.2.6.

a, b páratlanok, $(a, b) = 1$

$$\frac{a-1}{2} \cdot \frac{b-1}{2} = \sum_{i=1}^{\frac{b-1}{2}} \left\lfloor \frac{ai}{b} \right\rfloor + \sum_{j=1}^{\frac{a-1}{2}} \left\lfloor \frac{bj}{a} \right\rfloor$$

TÉTEL 5.2.7 (GAUSS-FÉLE KVADRATIKUS RECIPROCITÁSI TÉTEL).

p, q páratlan prím $(p \neq q) \Rightarrow \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

$$\Rightarrow \begin{cases} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \\ \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \end{cases} \Leftrightarrow \begin{matrix} p \text{ vagy } q & 4k+1 \text{ alakú} \\ p \text{ és } q & 4k+3 \text{ alakúak} \end{matrix}$$

DEFINÍCIÓ 5.2.8.

$m > 1$ páratlan, $m = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$, $(a, m) = 1$ ekkor $\left(\frac{a}{m}\right)$ -t *Jacobi-jelnek* (Jacobi-szimbólumnak) nevezzük és a következőképp definiáljuk:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdot \dots \cdot \left(\frac{a}{p_r}\right)^{k_r}$$

Megjegyzések:

- m prím $\Rightarrow$ a Jacobi-jel azonos a Legendre-jellel
- $\left(\frac{a}{m}\right) = 1$ nem jelenti, hogy $x^2 \equiv a \pmod{m}$ megoldható, csak ha $\forall p \mid m$ -re $\left(\frac{a}{p}\right) = 1$

TÉTEL 5.2.9 (A JACOBI-JEL TULAJDONSÁGAI).

$n, m > 1$, $(a, m) = (b, m) = 1$

1. $\left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right)$
2. $\left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right) = \left(\frac{a}{mn}\right)$
3. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$
4. $a \equiv b \pmod{m} \Rightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$
5. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$
6. m, n páratlanok, $(m, n) = 1 \Rightarrow \left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$

ÁLLÍTÁS 5.2.10 (MODULÁRIS NÉGYZETGYÖKVONÁS).

$n = pq$, p, q páratlan prímek

$x^2 \equiv a \pmod{n}$ megoldható $\Rightarrow$ 4 különböző megoldás van

6 Számelméleti függvények

6.1 Függvénydefiníciók, multiplikatívitas, additivitás

DEFINÍCIÓ 6.1.1.

f függvény számelméleti függvény, ha $\mathbb{Z}^+ \subseteq \mathcal{D}_f$

DEFINÍCIÓ 6.1.2.

f számelméleti függvény

- *multiplikatív*, ha $f(nm) = f(n)f(m) \forall (n, m) = 1$
- *additív*, ha $f(nm) = f(n) + f(m) \forall (n, m) = 1$
- *teljesen multiplikatív*, ha $f(nm) = f(n)f(m) \forall n, m$
- *teljesen additív*, ha $f(nm) = f(n) + f(m) \forall n, m$

ÁLLÍTÁS 6.1.3.

1. $\exists n : f(n) \neq 0$ és f multiplikatív $\Rightarrow f(1) = 1$
2. g additív $\Rightarrow g(1) = 0$

TÉTEL 6.1.4.

Multiplikatív és additív függvényeket elég csak prímszámokra, teljesen multiplikatív és teljesen additív függvényeket pedig csak prímszámokra ismerni:

$$\begin{aligned}
 f \text{ mult.} \quad & \text{ha } f\left(\prod_{\forall i} p_i^{\alpha_i}\right) = \prod_{\forall i} f(p_i^{\alpha_i}) \\
 f_t \text{ t. mult.} \quad & \text{ha } f_t\left(\prod_{\forall i} p_i^{\alpha_i}\right) = \prod_{\forall i} f_t(p_i)^{\alpha_i} \\
 g \text{ add.} \quad & \text{ha } g\left(\prod_{\forall i} p_i^{\alpha_i}\right) = \sum_{\forall i} g(p_i^{\alpha_i}) \\
 g_t \text{ t. add.} \quad & \text{ha } g_t\left(\prod_{\forall i} p_i^{\alpha_i}\right) = \sum_{\forall i} g_t(p_i)^{\alpha_i}
 \end{aligned}$$

TÉTEL 6.1.5.

Két multiplikatív függvény szorzata és hányadosa is multiplikatív.

DEFINÍCIÓ 6.1.6.

- $d(n) := n$ osztóinak száma
- $\sigma(n) := n$ osztóinak összege
- $v(n) := n$ prímtényezőinek száma
- $\kappa(n) := n$ különböző prímtényezőinek száma
- $\varphi(n) := n$ -nél kisebb n -hez relatív prímek száma

$$\bullet \mu(n) := \begin{cases} 1, & n = 1 \\ (-1)^r, & n = p_1 \cdot \dots \cdot p_r \text{ } p_i \neq p_j, \text{ ha } i \neq j \\ 0, & \text{egyébként} \end{cases}$$

ÁLLÍTÁS 6.1.7.

d, σ, φ, μ multiplikatív függvények

TÉTEL 6.1.8.

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$$

$$1. \ d(n) = \prod_{i=1}^r (\alpha_i + 1)$$

$$2. \ \sigma(n) = \prod_{i=1}^r \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

$$3. \ \varphi(n) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

6.2 Összegzések

TÉTEL 6.2.1.

$$\sum_{d|n} \varphi(d) = n$$

DEFINÍCIÓ 6.2.2.

- f számelméleti függvény *összegzési függvénye* f^+ , melyre: $f^+(n) = \sum_{d|n} f(d)$
- f számelméleti függvény *megfordítási függvénye* f^- , melyre: $f(n) = \sum_{d|n} f^-(d) \quad ((f^-)^+ = f)$

ÁLLÍTÁS 6.2.3.

f^- egyértelműen létezik

ÁLLÍTÁS 6.2.4.

f multiplikatív $\Leftrightarrow f^+$ is multiplikatív

ÁLLÍTÁS 6.2.5.

$$\mu^+(n) = e(n) := \begin{cases} 1, & \text{ha } n = 1 \\ 0, & \text{ha } n > 1 \end{cases}$$

TÉTEL 6.2.6 (MÖBIUS-FÉLE INVERZIÓS/MEGFORDÍTÁSI FORMULA).

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d)$$

DEFINÍCIÓ 6.2.7.

f és g számelméleti függvények *konvolúcióját* a következőképpen definiáljuk:

$$(f \star g)(n) := \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right)$$

Megjegyzés:

- $f^+ = f \star 1$
- $f^- = f \star \mu$

TÉTEL 6.2.8.

A $\star$ reláció kommutatív, asszociatív, egységelemes: $e(n) = \begin{cases} 1, & \text{ha } n = 1 \\ 0, & \text{ha } n > 1 \end{cases}$

DEFINÍCIÓ 6.2.9 (DIRICHLET-SOR).

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \text{ (azon } s \text{ helyeken, ahol konvergens)}$$

DEFINÍCIÓ 6.2.10 (RIEMANN-FÉLE ZETA FÜGGVÉNY).

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ (abszolót konvergens, } s > 1)$$

TÉTEL 6.2.11 (EULER-FÉLE SZORZATALAK).

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prím}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

TÉTEL 6.2.12.

f, g, h számelméleti függvények és F, G, H Dirichlet-soraik abszolút konvergensek, ekkor

$$h = f \star g \Rightarrow H = F \cdot G$$

TÉTEL 6.2.13 (VÖLGYTÉTEL).

$$\forall K \in \mathbb{N}^+ : \exists \infty \text{ sok } n : d(n-1) - d(n) > K, d(n+1) - d(n) > K$$

TÉTEL 6.2.14 (HEGYTÉTEL).

$$\forall K \in \mathbb{N}^+ : \exists^\infty \text{ sok } n : d(n) - d(n-1) > K, d(n) - d(n+1) > K$$

TÉTEL 6.2.15.

$$\left| \frac{\sum_{i=1}^n d(i)}{n} - \ln n \right| < 1$$

6.3 Minimális univerzális kitevő (exponens)

DEFINÍCIÓ 6.3.1.

$\lambda > 0$ *minimális univerzális kitevő* (mod n), ha λ a legkisebb olyan egész, hogy $a^\lambda \equiv 1 \pmod{n} \quad \forall (a, n) = 1$ esetén (szokás $\lambda(n)$ függvényként írni)

Megjegyzés:

- ha $\exists$ primitív gyök $\Rightarrow \lambda(n) = \varphi(n)$
- ha $\text{ord}_n a = k \Rightarrow k \mid \lambda(n)$

LEMMA 6.3.2.

$$\text{ord}_n a = k, \text{ord}_n b = l \Rightarrow \exists g : \text{ord}_n g = [k, l]$$

LEMMA 6.3.3.

M a maximális rend $\Rightarrow M = \lambda(n)$, $\exists \lambda(n)$ rendű elem.

TÉTEL 6.3.4.

p prím $\Rightarrow \exists$ primitív gyök (mod p)