

## Számelméleti alapok II.

### Kongruenciák

**Definíció.** Ha az  $m$  nemnulla egész osztja az  $a - b$  különbséget, akkor azt mondjuk, hogy az  $a$  szám *kongruens*  $b$ -vel modulo  $m$ .

Jelölés:  $a \equiv b \pmod{m}$

**Tétel.** Legyenek  $a, b, c, d, x$  és  $y$  egész számok.

(a) Ha  $a \equiv b \pmod{m}$  és  $b \equiv c \pmod{m}$ , akkor  $a \equiv c \pmod{m}$ .

(b) Ha  $a \equiv b \pmod{m}$  és  $c \equiv d \pmod{m}$ , akkor  $ax + cy \equiv bx + dy \pmod{m}$ .

(c) Ha  $a \equiv b \pmod{m}$  és  $c \equiv d \pmod{m}$ , akkor  $ac \equiv bd \pmod{m}$

**Tétel.** Legyen  $f$  egész együtthatós polinom. Ha  $a \equiv b \pmod{m}$ , akkor  $f(a) \equiv f(b) \pmod{m}$ .

**Tétel.**  $ax \equiv ay \pmod{m}$  akkor és csak akkor, ha  $x \equiv y \pmod{\frac{m}{(a,m)}}$ .

**Tétel.** Ha  $ax \equiv ay \pmod{m}$  és  $(a, m) = 1$  akkor  $x \equiv y \pmod{m}$ .

**Definíció.** Ha  $x \equiv y \pmod{m}$ , akkor  $y$ -t az  $x$  szám  $m$  szerinti maradékának nevezzük. Az  $x_1, \dots, x_m$  számok halmazát *teljes maradékrendszernek* nevezzük modulo  $m$ , ha tetszőleges  $y$  egész számhoz létezik egy és csak egy  $x_j$ , amelyre  $y \equiv x_j \pmod{m}$ .

**Definíció.** Az  $r_i$  egész számok halmazát *redukált maradékrendszernek* nevezzük modulo  $m$ , ha  $(r_i, m) = 1$ ;  $r_i \not\equiv r_j \pmod{m}$ , valahányszor  $i \neq j$ , és tetszőleges,  $m$ -hez relatív prím  $x$  egész számhoz található olyan, halmazbeli  $r_i$ , hogy  $x \equiv r_i \pmod{m}$ .

**Jelölés:** Minden redukált maradékrendszer  $(\text{mod } m)$  ugyanannyi elemet tartalmaz. Ezt a közös elemszámot  $\phi(m)$ -el jelöljük és Euler-féle  $\phi$  függvénynek nevezzük.

**Tétel.** A  $\phi(m)$  szám az  $m$ -nél nem nagyobb,  $m$ -hez relatív prím pozitív egészek száma.

**Tétel.** (Euler) Ha  $(a, m) = 1$ , akkor

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Euler(1707-1783)

**Tétel.** (Fermat) Legyen  $p$  prímszám és tegyük fel, hogy  $(a, p) = 1$ , ekkor

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Tétel.** Legyen  $g = (a, m)$ . Ha  $g \nmid b$ , akkor az  $ax \equiv b \pmod{m}$  kongruenciának nincs megoldása; ha viszont  $g \mid b$ , akkor a kongruenciának  $g$  megoldása van, és a megoldások: az

$$x \equiv \frac{b}{g}x_0 + t\frac{m}{g} \pmod{m}, t = 0, 1, \dots, g - 1$$

értékek, ahol  $x_0$  az

$$\frac{a}{g}x \equiv 1 \pmod{\frac{m}{g}}$$

kongruencia tetszőleges megoldása.

**Példa.** Oldjuk meg a

$$15x \equiv 25 \pmod{35}$$

lineáris kongruenciát.

Mivel  $(15, 35) = 5$  és  $5 \mid 25$  a kongruencia megoldható.

$$3x \equiv 1 \pmod{7} \Rightarrow x_0 = 5$$

$g = (a, m)$ , kibővített Euklideszi algoritmus segítségével  $au + mv = g \Rightarrow u = x_0$

Megoldás:  $x \equiv 25 + 7t \pmod{35}$

**Tétel.** (Kínai maradéktétel.)

Ha az  $m_1, m_2, \dots, m_r$  pozitív egészek páronként relatív prímek, és  $a_1, a_2, \dots, a_r$  tetszőleges egész számok, akkor az

$$x \equiv a_i \pmod{m_i} \quad i = 1, 2, \dots, r$$

kongruenciáknak van közös megoldása. Bármely két megoldás kongruens modulo  $m_1 m_2 \cdots m_r$ .

**Módszer:**  $m = m_1 m_2 \cdots m_r$

$$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$$

$$x_0 = \sum_{j=1}^r \frac{m}{m_j} b_j a_j$$

**Példa.** Válasszunk egy 60-nál kisebb számot, osszuk el 3,4,5 számokkal és közöljük a maradékot.

A gondolt szám  $40a + 45b + 36c$  szám 60-nal való osztási maradéka, feltéve ha a maradékok rendre  $a, b, c$ . Ha a választott szám 29, akkor  $40 \cdot 2 + 45 \cdot 1 + 36 \cdot 4 = 269$ .

**Megoldás.**

$$20b_1 \equiv 1 \pmod{3}$$

$$15b_2 \equiv 1 \pmod{4}$$

$$12b_3 \equiv 1 \pmod{5}$$

Ekkor  $b_1 = 2, b_2 = 3, b_3 = 3$ .

$$x_0 = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 4 \pmod{60} = 29$$