

# Oszthatóság

(Az alábbiakban mindenhol egész számokról beszélünk, ezért ezt nem mindig írjuk oda.)

**Definíció 1** (*Oszthatóság*) Legyen  $a, b \in \mathbb{Z}$ . Azt mondjuk, hogy  $b$  osztható  $a$ -val, ha  $\exists c \in \mathbb{Z}$ , hogy  $b = ac$ . Ekkor  $a$  osztója  $b$ -nek. Jelölés:  $a|b$ . (Megj: Az oszthatóság egy rendezési reláció.)

**Tétel 1** Ha  $a|b$  és  $a|c$ , akkor  $a|b+c$ .

Ha  $a|b$ , akkor  $a|bc$ .

Ha  $a|b$  és  $a|c$ , akkor  $a|\alpha b + \beta c$ .

**Definíció 2** (*Egység*) Az  $\varepsilon$ -t (most  $\varepsilon \in \mathbb{Z}$ , de más halmazokon is definiálható) egységnek nevezzük, ha minden  $a \in \mathbb{Z}$  oszthatója. Azaz  $\forall a \in \mathbb{Z}, \varepsilon|a$ . Egységek  $\mathbb{Z}$ -ben:  $-1, 1$ .

**Definíció 3** (*Asszociált*) Az  $a, b$  asszociáltak, ha egymás egységszeresei. Másik def: Kölcsonösen osztják egymást. A 2 def. ekvivalens. (Megj: Az asszociáltság egy ekvivalencia reláció.)

**Definíció 4** (*Felbonthatatlan (irreducibilis)*) Egy nem nulla, nem egység szám felbonthatatlan, ha az egységeken és önmaga egységszeresein kívül nincs más osztója.

**Definíció 5** (*Prím*) A nem nulla, nem egység  $p$ -t prímmek nevezzük, ha  $p|ab$  esetén  $p|a$  vagy  $p|b$ .

**Tétel 2**  $\mathbb{Z}$ -ben felbonthatatlan és a prím ekvivalens fogalmak. Azaz egy szám akkor és csak akkor felbonthatatlan, ha prím.

**Tétel 3** (*Számelmélet alaptétele, prímtenyezős felbontás*) Minden nem nulla, nem egység szám felírható felbonthatatlanok szorzataként és ez a felbontás a sorrendtől és egységszerestől eltekintve egyértelmű.

**Definíció 6** (*Legnagyobb közös osztó*) Az  $a$  és  $b$  legnagyobb közös osztója a  $d$  szám, ha

1.  $d|a$  és  $d|b$

2. Ha  $c|a$  és  $c|b$ , akkor  $c|d$ .

Jelölés  $d = \text{lko}(a, b)$  vagy  $d = (a, b)$ . Megj: Ha  $(a, b) = 1$ , akkor  $a$  és  $b$  relatív prímek.

**Tétel 4** (*Maradékos osztás*) Minden  $a, b \neq 0$ -hez egyértelműen létezik  $q, r$ , hogy  $a = bq + r$ , ahol  $0 \leq r < |b|$ .

**Tétel 5** (*Euklideszi algoritmus, eljárás  $(a, b)$  meghatározására*) Legyen  $a, b \neq 0$ . Maradékos osztások sorozatát végezzük  $a, b$ -ből kiindulva, amíg 0 maradékot nem kapunk:

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

$$\vdots$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}$$

$$r_n = r_{n+1}q_{n+2} + 0$$

Áll: Az utolsó nem nulla maradék éppen  $a$  és  $b$  legnagyobb közös osztója. Azaz:  $r_{n+1} = (a, b)$ .

**Definíció 7** (*Lineáris diofantoszi egyenlet*)

$$Ax + By = C$$

ahol  $A, B, C$  egészek és keressük az  $x, y$  egész megoldásokat.

**Tétel 6 (Lineáris diofantoszi egyenlet megoldhatósága)** Az  $Ax + By = C$  akkor és csak akkor megoldható, ha  $(A, B) | C$ . Ha  $x_0, y_0$  megoldás, akkor a többi (végtelen sok) megoldás alakja:

$$x = x_0 + k \frac{B}{(A, B)}, \quad y = y_0 + l \frac{A}{(A, B)}, \quad k, l \in \mathbb{Z}$$

**Definíció 8 (Kongruencia)** Az  $a, b$  számokat az  $m \neq 0$  számra (modulusra) nézve kongruensnek nevezzük, ha  $a$  és  $b$  ugyanazt a maradékot adják  $m$ -mel osztva. ("a kongruens b-vel modulo m") Jelölés:  $a \equiv b \pmod{m}$  vagy  $a \equiv b \pmod{m}$ . Tehát  $a \equiv b \pmod{m} \iff m | a - b$ .

**Tétel 7**  $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{\frac{m}{(m, c)}}$

**Tétel 8 ((Kongruencia, mint ekvivalencia reláció, maradékosztályok)** Adott  $m$  modulusú kongruencia ekvivalencia reláció  $\mathbb{Z}$ -n. Az ennek megfelelő  $m$  darab ekvivalenciaosztályt maradékosztályoknak nevezzük mod  $m$ .

**Definíció 9 (Egyszerűen lineáris kongruencia)** Adott  $a, b, m$  mellett keressük az  $ax \equiv b \pmod{m}$  kongruencia  $x$  megoldásait.

**Tétel 9 (Lineáris kongruencia megoldhatósága, megoldások száma)**  $ax \equiv b \pmod{m}$  megoldható  $\iff (a, m) | b$ . Ugyanis  $ax \equiv b \pmod{m}$  megoldása az  $ax - b = my$  lineáris diofantoszi egyenlet megoldását jelenti. Megoldások számán a megoldásként szereplő maradékosztályok számát értjük. Ha egy maradékosztály egy eleme megoldás, akkor az összes eleme az. Ilyen értelemben  $(a, m)$  darab maradékosztály a megoldás.

**Tétel 10 (Kínai maradéktétel)** Az

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv c_k \pmod{m_k}$$

$$(m_i, m_j) = 1, \quad \text{ha } i \neq j$$

szimultán lineáris kongruencia rendszernek létezik egyértelmű megoldása mod  $m_1 \cdot m_2 \cdot \dots \cdot m_k$ .

## Számelméleti függvények

Legyen az  $n$  prímtényezői felbontása

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^r p_i^{\alpha_i}$$

Ekkor

1. Az  $n > 0$ -hez relatív prím,  $n$ -nél kisebb pozitív egészek száma (Euler-féle  $\varphi$ -függvény)

$$\varphi(n) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

2. Az  $n$  szám pozitív osztóinak száma

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1) = \prod_{i=1}^r (\alpha_i + 1)$$

3. Az  $n$  szám pozitív osztóinak összege

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

#### 4. Möbius függvény

$$\mu(n) = \begin{cases} 1 & \text{ha } n \text{ négyzetmentes és a prímtényezők száma páros} \\ -1 & \text{ha } n \text{ négyzetmentes és a prímtényezők száma páratlan} \\ 0 & \text{ha } n \text{ nem négyzetmentes} \end{cases}$$

**Tétel 11** (*Euler-Fermat tétel*) Ha  $(a, m) = 1$ , akkor  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . Spec. eset: Kis Fermat tétel: Ha  $p$  prím, akkor  $a^p \equiv a \pmod{p}$  bármely  $a$ -ra.

**Definíció 10** Az  $f(n)$  számelméleti függvényt multiplikatívnak nevezzük, ha  $\forall(a, b) = 1$  esetén  $f(a \cdot b) = f(a) \cdot f(b)$ .

**Definíció 11** Az  $f(n)$  számelméleti függvényt additívnak nevezzük, ha  $\forall(a, b) = 1$  esetén  $f(a + b) = f(a) + f(b)$ .

**Tétel 12** A  $\varphi(n), d(n), \sigma(n), \mu(n)$  multiplikatív számelméleti függvények.

**Definíció 12** (*Összegzési függvény*)

$$g(n) = \sum_{d|n} f(d)$$

**Tétel 13** A  $\varphi(n)$  összegzési függvénye  $g(n) = n$ .

A Möbius függvény összegzési függvénye  $n = 1$ -re 1, egyébként 0.

**Tétel 14** (*Möbius-féle megfordítási függvény*)

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