1. Oszthatóság, legnagyobb közös osztó

Ebben a jegyzetben minden változó egész számot jelöl.

1.1. Definíció. *Azt mondjuk, hogy* a oszója b*-nek, vagy más szóval,* b osztható a*-val, ha létezik olyan* $x \in \mathbb{Z}$*, hogy* $b = ax$*. Ennek jelölése* $a|b$*.*

1.2. Tétel. *Legyen* $a, b, c \in \mathbb{Z}$*.*

1. $a|a$ *minden* a*-ra,*
2. *Ha* $a|b$ *és* $b|c$*, akkor* $a|c$*.*
3. *Ha* $a|b$ *és* $b|a$*, akkor* $a = \pm b$*.*
4. *Ha* $a|b$*, akkor* $a|bc$ *minden* $c \in \mathbb{Z}$*-re.*
5. *Ha* $a|b$ *és* $a|c$*, akkor* $a|bx + cy$ *minden* $x, y \in \mathbb{Z}$*-re.*
6. *Ha* $a|b$ *és* $a > 0$*,* $b > 0$*, akkor* $a \leq b$*.*
7. *Legyen* $m \neq 0$*. Ekkor* $a|b$*, akkor és csak akkor, ha* $ma|mb$*.*
8. *Ha* $a|b$*, akkor* $(-a)|b$*,* $a|(-b)$ *és* $(-a)|(-b)$*.*

1.3. Tétel (Maradékos osztás tétele). *Minden* $a > 0$ *és* $b \in \mathbb{Z}$*-hez létezik olyan, egyértelműen meghatározott* q *és* r *egész szám, amelyre*

$$b = aq + r, \qquad 0 \leq r < a.$$

1.4. Következmény. *Minden* a *és* b *egész számokhoz létezik olyan, egyértelműen meghatározott* q *és* r *egész szám, amelyre*

$$b = aq + r, \qquad 0 \leq |r| < a.$$

1.5. Definíció. *Azt mondjuk, hogy* d közös osztója *az* a *és* b *egész számoknak, ha* $d|a$ *és* $d|b$*. Azt mondjuk, hogy* g a legnagyobb közös oszója a*-nak és* b*-nek, ha* g *a közös osztók közül a legnagyobb, azaz, ha* d *közös osztója* a*-nak és* b*-nek, akkor* $d \leq g$*. Ennek jelölése* $g = (a, b)$*. Hasonlóan az* $a_1, \ldots, a_n$ *számok közös osztói közül a legnagyobbat, azaz a számok* legnagyobb közös oszóját $(a_1, \ldots, a_n)$ *jelöli.*

Bármely két egész számnak 1 és -1 is közös osztója. Mivel egy (nem nulla) egész számnak véges sok osztója van, ezért közös osztókból is csak véges sok van, ezért a legnagyobb közös osztó mindig egyértelműen definiált, és $(a, b) \geq 1$.

1.6. Tétel. *Minden* a *és* b *egész számokhoz léteznek olyan* x_0 *és* y_0 *egész számok, hogy*

$$(a, b) = ax_0 + by_0.$$

1.7. Következmény. *Minden* $a_1, \ldots, a_n$ *egész számokhoz léteznek olyan, egyértelműen meghatározott* x_i *egész számok, hogy*

$$(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n.$$

1.8. Tétel. *Az a és b egész számok bármely d közös osztójára $d|(a,b)$.*

1.9. Tétel. $(a,b) = (b,a) = (a,-b) = (|a|,|b|) = (a,b+ax)$ *minden x-re.*

1.10. Tétel.

1. *Minden m pozitív egészre $m(a,b) = (ma,mb)$.*
2. *Az a és b egész számok bármely d közös osztójára $\left(\frac{a}{d},\frac{b}{d}\right) = \frac{1}{d}(a,b)$.*
3. *Ha $g = (a,b)$, akkor $\left(\frac{a}{g},\frac{b}{g}\right) = 1$.*

1.11. Definíció. *Azt mondjuk, hogy a és b relatív prímek, ha $(a,b) = 1$.*

1.12. Tétel.

1. *Ha $(a,c) = 1$ és $(b,c) = 1$, akkor $(ab,c) = 1$.*
2. *Ha $c|ab$ és $(b,c) = 1$, akkor $c|a$.*

Euklideszi algoritmus: Adott a és b pozitív egész számokra ismételten alkalmazzuk a maradékos osztás tételét: osszuk el az a számot b-vel, majd b-t a maradékkal, stb. mindig az osztót a maradékkal. Azaz legyen

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b,\\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2,\\
r_2 &= r_3q_4 + r_4, & 0 < r_4 < r_3,\\
&\vdots\\
r_{i-2} &= r_{i-1}q_i + r_i, & 0 < r_i < r_{i-1},\\
r_{i-1} &= r_iq_{i+1}.
\end{aligned}$$

Az eljárás természetesen véges sok lépésben véget ér, az algoritmus végeredménye az utolsó nem nulla maradék, azaz r_i.

1.13. Tétel (euklideszi algoritmus). *Az a és b pozitív egész számok legnagyobb közös osztója az euklideszi algoritmussal kapott utolsó nem nulla maradék, azaz r_i. Továbbá a legnagyobb közös osztó mindig kifejezhető az $r_i = (a,b) = ax_0 + by_0$ alakban, ahol x_0 és y_0 megkapható úgy, hogy r_i-t kifejezzük az euklideszi algoritmus egyenleteit alkalmazva.*

2. Lineáris diofantoszi egyenletek

Az

$$ax + by = c \tag{2.1}$$

egyenletet, ahol $a, b, c \in \mathbb{Z}$, és ahol a megoldásokat is az egész számok körében keressük, *lineáris diofantoszi egyenletnek* vagy *lineáris diofantikus egyenletnek* hívjuk.

2.1. Tétel. *A (2.1) egyenletnek pontosan akkor létezik megoldása, ha $(a, b)|c$. Ekkor az egyenlet minden megoldása felírható az*

$$x = x_0 + k\frac{b}{(a,b)}, \qquad y = y_0 - k\frac{a}{(a,b)} \tag{2.2}$$

alakban, ahol $k \in \mathbb{Z}$ tetszőleges.

A (2.1) egyenletnek megoldási módszere: Legyen $d = (a, b)$. Az

$$au + bv = d$$

egyenlet egy u_0 és v_0 megoldását az euklideszi algoritmus segítségével határozhatjuk meg. Ekkor

$$x_0 = u_0\frac{c}{d}, \quad y_0 = v_0\frac{c}{d}$$

egy megoldása a (2.1) egyenletnek. Az összes megoldást a (2.2) képletet alkalmazva kaphatjuk.

3. Legkisebb közös többszörös, prímszámok

3.1. Definíció. *A h egész számot az a és b egész számok* közös többszörösének *nevezünk, ha $a|h$ és $b|h$. Az a és b szémok közös pozitív többszörösei közül a legkisebbet az a és b* legkisebb közös többszörösének *hívjuk, és $[a, b]$-vel jelöljük. Hasnlóan, az $a_1, \ldots, a_n$ számok közös pozitív többszörösei közül a legkisebbet, azaz a számok* legkisebb közös többszörösét $[a_1, \ldots, a_n]$ *jelöli.*

3.2. Tétel. *Az a és b egész számok bármely h közös többszörösére $[a, b]|h$.*

3.3. Tétel.

1. *Minden m pozitív egészre $m[a, b] = [ma, mb]$.*
2. *Minden pozitív egész a és b-re $(a, b)[a, b] = ab$.*

A következő tétel szerint több szám legnagyobb közös osztóját illetve legkisebb közös többszörösét vissza lehet vezetni két szám legnagyobb közös osztójának illetve legkisebb közös többszörösének kiszámítására.

3.4. Tétel. *Minden a, b, c egészre*

1. $(a, b, c) = ((a, b), c)$,
2. $[a, b, c] = [[a, b], c]$.

3.5. Definíció. *A $p > 1$ egész számot* prímszámnak *vagy* prímnek *nevezünk, ha p-nek nincs olyan d osztója, amelyre $1 < d < p$, azaz önmagán és az 1-en kívül nincs más pozitív osztója. Ha az n egész szám nem prím, akkor* összetett számnak *nevezzük.*

3.6. Tétel. *Minden $n > 1$ egész szám kifejezhető prímek (esetleg egytagú) szorzataként.*

Az előbbi tétel szerint tehát minden $n > 1$ egész szám felírható

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

alakban, ahol a p_i számok páronként különböző prímszámok, és $\alpha_i > 1$. Ezt az előállítást az n szám *törzstényezős alakjának* vagy *törzstényezős felbontásának* hívjuk.

3.7. Tétel. *Ha p prím és $p|ab$, akkor vagy $p|a$ vagy $p|b$. Ugyanígy, ha p prím és $p|a_1 a_2 \cdots a_n$, akkor valamely i-re $p|a_i$.*

3.8. Tétel (a számelmélet alaptétele). *Minden $n > 1$ egész szám felbontható prímszámok szorzatára, mégpedig a tényezők sorrendjétől eltekintve egyértelmű módon.*

3.9. Tétel. *Legyen $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ és $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$, ahol $0 \le \alpha_i$ és $0 \le \beta_i$, azaz tekintsük a és b törzstényezős alakját, ahol kölcsönösen felsoroljuk a másik számban szereplő minden prímszámot is 0 kitevővel. Ekkor*

$$(a, b) = p_1^{\min(\alpha_1, \beta_q)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)}$$

és

$$[a, b] = p_1^{\max(\alpha_1, \beta_q)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

3.10. Tétel (Euklidész). *A prímszámok száma végtelen, azaz a prímszámok $2, 3, 5, 7, \ldots$ sorozata végtelen.*

3.11. Tétel. *A prímszámok (növekvő) sorozatában két prímszám közötti távolság tetszőlegesen nagy lehet, azaz bármely k pozitív egész számhoz létezik k db egymás utáni összetett szám.*

Jelölje $\pi(n)$ az n-nél kisebb prímszámok számát.

3.12. Tétel (prímszámtétel).

$$\lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{\log n}} = 1,$$

nagy n-re $\pi(n)$ közelíthető a $\frac{n}{\log n}$ hányadossal.

4. Maradékosztályok

Legyen n pozitív egész rögzített ebben a szakaszban. Jelölje $\mathbb{Z}_n$ a modulo n ekvivalenciareláció ekvivalenciaosztályait, és jelölje $\bar{a}$ az a egész szám ekvivalenciaosztályát, azaz

$$\bar{a} = \{x \in \mathbb{Z} : \ x \equiv a \pmod{n}\}.$$

Ekkor $\mathbb{Z}_n$ számossága n, mégpedig

$$\mathbb{Z}_n = \{\bar{1}, \bar{2}, \ldots, \bar{n}\} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}.$$

Vezessük be az összeadás és a szorzás műveletét a $\mathbb{Z}_n$ halmazon:

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b}. \end{aligned}$$

Ez a definíció jól definiált, hiszen ha

$$a \equiv a' \pmod{n} \qquad \text{és} \qquad b \equiv b' \pmod{n},$$

akkor a kongruencia tulajdonságai alapján

$$a + b \equiv a' + b' \pmod{n} \qquad \text{és} \qquad a \cdot b \equiv a' \cdot b' \pmod{n}.$$

4.1. Tétel. *A $(\mathbb{Z}_n, +, \cdot)$ algebra kommutatív gyűrű.*

4.2. Tétel. *Ha p prím, akkor a $\mathbb{Z}_p$ maradékosztály-gyűrű test.*

4.3. Definíció. *Legyen R egy gyűrű, és jelölje 0 a gyűrű összeadásra vonatkozó egységelemét. Az $a \neq 0$ elemet* zérusosztónak *hívjuk, ha létezik olyan $b \neq 0$ elem, hogy $ab = 0$.*

Ha R test, akkor jelölje 1 a szorzásra vonatkozó egységelemet. Egy testben nincs zérusosztó, hiszen ha egy $a \neq 0$ elemre $ab = 0$ teljesül, akkor ebből $b = a^{-1}0 = 0$ következik.

4.4. Tétel. *Ha n összetett szám, akkor a $\mathbb{Z}_n$ maradékosztály-gyűrűben létezik zérusosztó, azaz $\mathbb{Z}_n$ nem test.*

Legyen k a modulo n redukált maradékosztályok száma, azaz $k = \varphi(n)$, és tekintsünk egy $a_1, a_2, \ldots, a_k$ redukált maradékrendszer modulo n, azaz

$$(a_i, n) = 1, \qquad i = 1, 2, \ldots, k,$$

és bármely m számhoz létezik olyan i, hogy $m \equiv r_i \pmod{n}$.

4.5. Tétel. *Egy redukált maradékrendszerhez tartozó $\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_k}\}$ maradékosztályok a szorzás műveletre vonatkozóan kommutatív csoportot alkotnak $\mathbb{Z}_n$-ben.*