# Számelmélet

Dr. Tóth László
Pécsi Tudományegyetem

2006

**Bevezetés**

Ez az anyag tartalmazza a „Számelmélet” című VI. féléves tárgy kötelező elméleti anyagának a nagy részét. Tartalmaz továbbá olyan kiegészítő részeket is, amelyek nem kötelezőek, ezek ★ ★ jelek között szerepelnek. Az anyagban gyakorlatok és feladatok is vannak, amelyek egy része az előadásokon és a gyakorlati órákon feldolgozásra kerül. A gyakorlatok és feladatok előtt ▼ jel áll. A nehezebb feladatokat ▼▼ jelöli. A feladatokra vonatkozó útmutatások, eredmények és megoldások a fejezetek végén találhatók.

A jelen anyagrészhez szükséges a korábbi bevezető algebrai és számelméleti, valamint absztrakt algebrai fogalmak és eredmények ismerete.

A bizonyítások és a bizonyítás nélkül megadott tételek végét a □ jel mutatja.

Felhívom a figyelmet

– a definíciók pontos ismeretére (a fogalmak nevei **kövér betűkkel** szedettek),

– az egyes fogalmakra adott példákra (ezek általában • jel után szerepelnek); adjanak, keressenek további példákat az anyag jobb megértése érdekében,

– a Tételek pontos megfogalmazására és a bizonyításokra,

– a feladatok megoldására.

**További irodalom**

[FJ] Fehér János, Bevezetés az algebrába és a számelméletbe II., JPTE Pécs, 1995.

[FGy] Freud Róbert, Gyarmati Edit, Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000.

[M] Megyesi László, Bevezetés a számelméletbe, Polygon, Szeged, 1997.

[SzÁ] Szendrei Ágnes, Diszkrét matematika, Polygon, Szeged, 2000.

[SzJ] Szendrei János, Algebra és számelmélet, Nemzeti Tankönyvkiadó, Budapest, 1996.

## 1. Integritástartományok aritmetikája

### 1.1. Oszthatóság

A továbbiakban $(D,+,\cdot)$ egy integritástartományt jelöl, azaz egy egységelemes, kommutatív, zérusosztómentes gyűrűt, amelynek zéruseleme a 0, egységeleme az 1. Feltételezzük, hogy $D$ legalább kételemű (nem a zérusgyűrű), ekkor $0 \neq 1$.

**Definíció.** Legyen $(D,+,\cdot)$ egy integritástartomány és $a,b \in D$. Azt mondjuk, hogy $a$ **osztója** $b$-nek, jelölés: $a \mid b$, ha létezik $c \in D$ úgy, hogy $b = ac$. Ez egy reláció a $D$-n. Ha $a \mid b$, akkor $b$ **többszöröse** $a$-nak.

Ha $a \mid b$ és $a \neq 0$, akkor a fenti $c$ elem egyértelmű (▼ Igazoljuk!) és jelölés: $c = \frac{b}{a}$.

**Megjegyzések.** 1. Ez általánosítása az egész számok oszthatóságának, ahol $D = (\mathbb{Z},+,\cdot)$ az egész számok integritástartománya.

2. Ha integritástartomány helyett tetszőleges gyűrűben nézzük az oszthatóságot (elhagyva pl. a zérusosztómentességet vagy az egységelem létezését), akkor az nagyon bonyolulttá válik.

3. Ha testben nézzük, akkor triviálissá válik: ha $(K,+,\cdot)$ test, $a,b \in K$, akkor $a \mid b$ mindig igaz, ha $a \neq 0$, hiszen $b = ac \Leftrightarrow c = a^{-1}b$. Ha $a = 0$, akkor $0 \mid b$ csak $b = 0$-ra igaz.

**Példák.** • Jelölje $\mathbb{Z}[i] = \{a + bi : a,b \in \mathbb{Z}\}$ a Gauss-egészek halmazát, akkor $(\mathbb{Z}[i],+,\cdot)$ integritástartomány, ez a Gauss-egészek gyűrűje. Itt pl. $2 + i \mid 6 + 3i$ és $2 + 3i \mid -1 + 5i$, mert $-1 + 5i = (2 + 3i)(1 + i)$.

• A $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} : a,b \in \mathbb{Z}\}$ halmaz integritástartomány a komplex számok összeadására és szorzására nézve és itt pl. $2 + i\sqrt{5} \mid 9$. Valóban, $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

• Ka $K$ egy kommutatív test és $K[X]$ a $K$ feletti egyhatározatlanú polinomok halmaza, akkor $(K[X],+,\cdot)$ integritástartomány, ez a $K$ feletti polinomok gyűrűje. Ha pl. $K = \mathbb{Q}$, akkor $X - 1 \mid X^2 - 3X + 2$ és $2X + 1 \mid X^2 + \frac{1}{2}X$, mert $X^2 + \frac{1}{2}X = (2X + 1)\frac{1}{2}X$.

**Feladat.** ▼ Legyen $d \in \mathbb{Z} \setminus \{0,1\}$ rögzített négyzetmentes szám (azaz $d$ nem osztható egyetlen prím négyzetével sem ($d = 2,3,5,6,...,-1,-2,-3,-5,-6,...$) és $\mathbb{Z}[d] = \{a + b\sqrt{d} : a,b \in \mathbb{Z}\}$. Igazoljuk, hogy $(\mathbb{Z}[d],+,\cdot)$ integritástartomány.

**Megjegyzések.** 1. Ha $d > 0$, akkor $(\mathbb{Z}[d],+,\cdot)$ részgyűrűje $(\mathbb{R},+,\cdot)$-nak, ha $d < 0$, akkor $(\mathbb{Z}[d],+,\cdot)$ részgyűrűje $(\mathbb{C},+,\cdot)$-nak. Ez általánosítása a Gauss-egészek gyűrűjének, itt $d = -1$ és $\mathbb{Z}[i\sqrt{5}]$-nek, ahol $d = -5$.

2. A Gauss-egészekre, általánosabban a $\mathbb{Z}[d]$-beli valós, ill. komplex számokra értelmezett az osztás és azt, hogy igaz-e $z \mid w$ úgy vizsgálhatjuk, hogy elosztjuk a $w$ számot $z$-vel. Ehhez szorozzunk és osszunk a $z$ konjugáltjával, ahol $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ konjugáltja $\overline{z} = a - b\sqrt{d}$ (ez $d < 0$ esetén a komplex konjugált). Ha az eredmény $\mathbb{Z}[d]$-beli, akkor $z \mid w$ teljesül.

**Példa.** • Legyen $D = \mathbb{Z}[\sqrt{2}]$. Igaz-e, hogy $2 + 3\sqrt{2} \mid 22 + 5\sqrt{2}$ ? Nézzük:

$$\frac{22 + 5\sqrt{2}}{2 + 3\sqrt{2}} = \frac{(22 + 5\sqrt{2})(2 - 3\sqrt{2})}{(2 + 3\sqrt{2})(2 - 3\sqrt{2})} = \frac{14 - 56\sqrt{2}}{-14} = -1 + 4\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$

tehát igaz.

**Feladat.** ▼ Teljesül-e $z \mid w$, ha
a) $D = \mathbb{Z}[i]$, $z = 2 + i, w = 13 + 11i$,
b) $D = Z[i]$, $z = 2 - i, w = 13 + 11i$,
c) $D = \mathbb{Z}[i\sqrt{5}]$, $z = 3 + 2i\sqrt{5}, w = 36 - 5i\sqrt{5}$,
d) $D = \mathbb{Z}[\sqrt{3}]$, $z = 2 + 3\sqrt{3}, w = 13 + 2\sqrt{3}$.

**Tétel.** (Az oszthatóság tulajdonságai) Ha $(D,+,\cdot)$ integritástartomány és $a,b,c,d \in D$, akkor

1. $a \mid a$ (reflexivitás),
2. $a \mid b$ és $b \mid c \Rightarrow a \mid c$ (tranzitivitás),
3. $a \mid b$ és $a \mid c \Rightarrow a \mid b+c, a \mid b-c$,
4. $a \mid b$ és $a \mid b+c \Rightarrow a \mid c$,
5. $a \mid b$ és $c \mid d \Rightarrow ac \mid bd$,
6. $1 \mid a, a \mid 0$,
7. $0 \mid a \Leftrightarrow a = 0$,
8. $ac \mid bc, c \neq 0 \Rightarrow a \mid b$.

**Bizonyítás.** A definíció alapján, használva az integritástartományokra vonatkozó számítási szabályokat. Pl. 2. Ha $a \mid b$ és $b \mid c$, akkor létezik $d,e \in D$ úgy, hogy $b = ad, c = be$, innen $c = (ad)e = a(de)$, tehát $a \mid c$. ▼ Végezzük el a többi bizonyítását! □

**Megjegyzések.** 1. Az $\mid$ reláció általában nem szimmetrikus és nem antiszimmetrikus, pl. $(\mathbb{Z},+,\cdot)$-ban. ▼ Miért?

2. A 3. tulajdonság így általánosítható: $a \mid b_1, ..., a \mid b_k \Rightarrow a \mid x_1b_1 + ... + x_kb_k$ minden $x_1, ..., x_k \in D$ esetén. ▼ Igazoljuk!

**Definíció.** Ha $a,b \in D$, akkor azt mondjuk, hogy $a$ **asszociált** $b$-vel (vagy $b$-hez), ha $a \mid b$ és $b \mid a$, jelölés $a \sim b$. Ez is egy reláció a $D$-n.

**Tétel.** Ha $(D,+,\cdot)$ integritástartomány, akkor $\sim$ egy ekvivalenciareláció.

**Bizonyítás.** A definíció alapján. ▼ Végezzük el! □

Legyen $\tilde{a} = \{b \in D : a \sim b\}$ az $a$ **asszociáltsági osztály**a és $D/\sim = \{\tilde{a} : a \in D\}$ a megfelelő faktorhalmaz.

**Példa.** • $(\mathbb{Z},+,\cdot)$-ban $\tilde{1} = \{1,-1\}$, $\tilde{2} = \{2,-2\}$,...,$\tilde{a} = \{a,-a\}$ ha $a \neq 0$, $\tilde{0} = \{0\}$, továbbá $\mathbb{Z}/\sim = \{\{0\},\{1,-1\},\{2,-2\},...\}$.

Jelölje $U(D)$ a $D$ integritástartomány invertálható elemeinek (ezeket egységeknek is nevezzük) a halmazát. Tudjuk, hogy $(U(D),\cdot)$ Abel-csoport (lásd Absztrakt algebra anyag), ehhez elegendő, hogy $D$ kommutatív, egységelemes gyűrű legyen. Az egységek minden $D$-beli elemnek osztói, hiszen ha $u \in D$ egység, akkor $b = (bu^{-1})u$ alapján $u \mid b$ minden $b \in D$-re.

**Példa.** • $(\mathbb{Z},+,\cdot)$ egységei: $U(\mathbb{Z}) = \{-1,1\}$.
• $(\mathbb{Z}[i],+,\cdot)$ egységei: $U(\mathbb{Z}[i]) = \{-1,1,-i,i\}$. ▼ Igazoljuk!

**Feladat.** ▼ Melyek $\mathbb{Z}[\sqrt{d}]$ egységei, ha $d < 0$?

**Feladat.** ▼ Legyen $D$ egy integritástartomány és $a \in D$. Igazoljuk, hogy $a \mid 1$ akkor és csak akkor, ha $a$ egység.

**Tétel.** Legyen $(D,+,\cdot)$ egy integritástartomány és $a,b \in D$.

1. $a \sim b$ akkor és csak akkor, ha létezik olyan $u \in D$ invertálható elem, hogy $b = au$ (azaz $a$ és $b$ akkor és csak akkor asszociáltak, ha egymástól egy egységszorzóban különböznek).
2. $a \sim 1$ akkor és csak akkor, ha $a$ invertálható ($a \in U(D)$).

**Bizonyítás.** 1. Ha $a \sim b$, akkor $a \mid b, b \mid a$, ezért $\exists c,d \in D : b = ac, a = bd$ és innen $b = bdc$.

Ha $b = 0$, akkor $a = 0$ és $0 = 0 \cdot u$ igaz $u = 1$-re.

Ha $b \neq 0$, akkor $a \neq 0$ és $1 = dc$, tehát $c$ invertálható és $b = ac$.

Fordítva, ha feltételezzük, hogy $b = au$, $u \in U(D)$, akkor innen $a \mid b$ és $\exists u^{-1} = x \in D : bx = (au)x = a(ux) = a$, következik, hogy $b \mid a$, tehát $a \sim b$.

2. Az 1. azonnali következménye. □

**Feladat** ▼ Melyek $(\mathbb{Z}[i],+,\cdot)$-ban $1+2i$ és $3-4i$ asszociáltjai?

**Definíció.** Ha $a \mid b$, $a$ nem asszociált $b$-vel és $a$ nem asszociált az 1-gyel ($a \nsim b$, $a \nsim 1$), akkor azt mondjuk, hogy $a$ **valódi osztó**ja $b$-nek. Ellenkező esetben $a$ **nem valódi osztó**.

**Feladat.** ▼▼ Legyenek $a,b \in \mathbb{Z}$, legyen $\theta$ az $x^2+ax+b=0$ egyenlet egy gyöke és $\mathbb{Z}[\theta]=\{m+n\theta : m,n \in \mathbb{Z}\}$. Igazoljuk, hogy $(\mathbb{Z}[\theta],+,\cdot)$ az $\mathbb{C}$ részgyűrűje.

### 1.2. Kongruenciák

**Definíció.** Legyen $(D,+,\cdot)$ egy integritástartomány és $m \in D$ egy rögzített elem. Az $a,b \in D$ elemekre azt mondjuk, hogy $a$ kongruens $b$-vel modulo $m$, jelölés $a \equiv b \pmod m$, ha $m \mid a-b$. Ezt az $m$ modulusú **kongruenciareláció**nak nevezzük.

Ha $m \nmid a-b$, akkor ezt így írjuk: $a \not\equiv b \pmod m$ és azt mondjuk, hogy $a$ inkongruens $b$-vel modulo $m$.

Az $a$ elem akkor és csak akkor osztója $b$-nek, ha $b \equiv 0 \pmod a$. Az $m=0$ esetben $a \equiv b \pmod 0$ akkor és csak akkor igaz, ha $a-b=0$, azaz $a=b$. Ha $m=u$ egység, akkor $a \equiv b \pmod u$ teljesül minden $a,b \in D$-re.

**Tétel.** Ha $D$ egy integritástartomány és $m \in D$, akkor az $m$ modulusú kongruencia egy ekvivalenciareláció.

**Bizonyítás.** Minden $a \in D$-re $a \equiv a \pmod m$, mert $m \mid a-a=0$, tehát a reláció reflexív. Hasonlóan a definíció alapján azonnali, hogy a reláció szimmetrikus és tranzitív. ▼ Igazoljuk! □

**Definíció.** Ha $m \in D$ rögzített, akkor $D$-nek a $\pmod m$ kongruencia szerinti ekvivalenciaosztályait $\pmod m$ **maradékosztályok**nak nevezzük. Az egyes osztályok elemei az osztályok **reprezentánsai**.

Ha az $m$ modulus rögzített, akkor az $a$ elem reprezentálta maradékosztályt így jelöljük: $\widehat{a}$. Itt $\widehat{a}=\{d \in D : d \equiv a \pmod m\}$.

**Tétel.** Legyen $D$ egy integritástartomány. Ha $a \equiv b \pmod m$ és $c \equiv d \pmod m$, akkor $a+c \equiv b+d \pmod m$ és $ac \equiv bd \pmod m$, tehát azonos modulusú kongruenciákat össze lehet adni és össze lehet szorozni.

**Bizonyítás.** ▼ Igazoljuk! □

Az egész számokra vonatkozó kongruencia-tulajdonságok közül még továbbiak is érvényben maradnak, pl. ha $a \equiv b \pmod m$, akkor $a^k \equiv b^k \pmod m$, ahol $k \in \mathbb{N}^*$. ▼ Igazoljuk!

Ugyanakkor nem maradnak érvényben azok a kongruencia-tulajdonságok, amelyekben szerepel a legnagyobb közös osztó, ill. a legkisebb közös többszörös, mert ezek nem biztos, hogy léteznek az integritástartomány tetszőleges elemeire. Látni fogjuk, hogy az euklideszi gyűrű az az algebrai struktúra, amelyben igaz marad sok további számelméleti tulajdonság.

**Feladat.** ▼ Vizsgáljuk meg az egész számokra vonatkozó tanult kongruenciatulajdonságok közül melyek maradnak még érvényben?

**Definíció.** Jelölje $D_m$ a $D$ integritástartomány $\pmod m$ maradékosztályainak halmazát és $D_m$-en definiáljuk a $+$ és $\cdot$ műveleteket így:

$$\widehat{a}+\widehat{b}=\widehat{a+b}, \qquad \widehat{a}\widehat{b}=\widehat{ab}.$$

Ezek a definíciók nem függenek a választott reprezentánsoktól, azaz ha $\widehat{a}=\widehat{a'},\widehat{b}=\widehat{b'}$, akkor $\widehat{a}+\widehat{b}=\widehat{a'+b'}$ és $\widehat{a}\widehat{b}=\widehat{a'b'}$. Valóban, a feltételből $a \equiv a' \pmod m$, $b \equiv b' \pmod m$, és innen $a+b \equiv a'+b' \pmod m$, $ab \equiv a'b' \pmod m$, azaz $\widehat{a+b}=\widehat{a'+b'}$, $\widehat{ab}=\widehat{a'b'}$.

Igaz továbbá a következő

**Tétel.** Ha $D$ integritástartomány, akkor $(D_m, +, \cdot)$ egy kommutatív egységelemes gyűrű, ez a (mod $m$) **maradékosztálygyűrű**.

**Bizonyítás.** Belátható, hogy öröklődnek a tulajdonságok a zérusosztómentesség kivételével, $(D_m, +, \cdot)$ zéruseleme $\widehat{0}$, egységeleme pedig $\widehat{1}$ lesz. ▼ Írjuk le a részleteket! □

**Megjegyzések.** 1. Ha $D$ az egész számok gyűrűje, akkor a $(\mathbb{Z}_m, +, \cdot)$ maradékosztálygyűrűt kapjuk.

2. $D_m$-ben lehetnek zérusosztók, pl. $\mathbb{Z}_6$-ban $\widehat{2}$ és $\widehat{3}$ zérusosztók.

3. A $D_m$ maradékosztálygyűrű speciális esete a faktorgyűrű fogalmának, lásd Absztrakt algebra anyag. Valóban, ha $I = (m) = \{md : d \in D\}$ az $m$ által generált főideál, akkor $a \equiv b \pmod m \Leftrightarrow a - b \in I$.

### 1.3. Irreducibilis elemek és prímelemek

Legyen a továbbiakban is $(D, +, \cdot)$ egy integritástartomány.

**Definíció.** Legyen $p \in D, p \neq 0, p \nsim 1$. Azt mondjuk, hogy $p$ **irreducibilis elem**, ha $p$-nek nincs valódi osztója, azaz ha abból, hogy $a \mid p$ következik, hogy $a \sim 1$ vagy $a \sim p$.

**Példák.** • $(\mathbb{Z}, +, \cdot)$-ban az irreducibilis számok a $-2, 2, -3, 3, ..., -p, p, ...$ számok, ahol $p$ (pozitív) prímszám.

• a $(\mathbb{R}[X], +, \cdot)$ polinomgyűrűben $f$ pontosan akkor irreducibilis, ha $f$ elsőfokú polinom, vagy olyan másodfokú polinom, amelynek diszkriminánsa negatív.

Ha $a, b, c \in D$ és $c \mid a$ vagy $c \mid b$, akkor $c \mid ab$. Fordítva általában nem igaz.

**Definíció.** Legyen $p \in D, p \neq 0, p \nsim 1$. Azt mondjuk, hogy $p$ **prímelem**, ha abból, hogy $p \mid ab$ következik, hogy $p \mid a$ vagy $p \mid b$.

**Tétel.** Legyen $(D, +, \cdot)$ egy integritástartomány és $p \in D$. Ha $p$ prím, akkor $p$ irreducibilis.

**Bizonyítás.** Tegyük fel, hogy $p$ prím és $p = ab$. Akkor $p \mid ab$, innen feltétel szerint $p \mid a$ vagy $p \mid b$. Ha pl. $p \mid a$, akkor $a = px, x \in D$, $p = ab = pxb$, innen $p \neq 0$ miatt $xb = 1$, tehát $b$ egység és $p = ab$ így a fenti Tétel szerint következik, hogy $p \sim a$. □

A fordított állítás nem igaz.

**Példa.** • $D = (\mathbb{Z}[i\sqrt{5}]+, \cdot)$-ban $p = 3$ irreducibilis elem, de nem prímelem.

Valóban, az egységek (azok a $D$-beli elemek, melyek minden $D$-beli számnak osztói) itt is a $-1$ és a 1. ▼ Igazoljuk ezt! Megmutatjuk, hogy $p = 3$ irreducibilis. Tegyük fel, hogy $3 = (a+ib\sqrt{5})(c+di\sqrt{5})$. Mindkét oldal komplex konjugáltját véve $3 = (a-ib\sqrt{5})(c-di\sqrt{5})$, ahonnan $9 = (a^2 + 5b^2)(c^2 + 5d^2)$. Ha $a^2 + 5b^2 = 1$, akkor $a = \pm 1, b = 0$ és $a + bi\sqrt{5} = \pm 1$ egység. Ha $a^2 + 5b^2 = 3$, akkor $a, b$-re nem kapunk egész szám megoldást, ha pedig $a^2 + 5b^2 = 9$, akkor $c^2 + 5d^2 = 1$ és következik, hogy $c + di\sqrt{5} = \pm 1$ egység.

Most igazoljuk, hogy $p = 3$ nem prímelem. Itt $3 \mid 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, de $3 \nmid 2 + i\sqrt{5}$ és $3 \nmid 2 - i\sqrt{5}$. Valóban, ha pl. $3 \mid 2 + i\sqrt{5}$, akkor létezik $x, y \in \mathbb{Z}$ úgy, hogy $2 + i\sqrt{5} = 3(x + iy\sqrt{5})$, ahonnan $x = 2/3, y = 1/3$, ellentmondás.

Az irreducibilis elem és a prímelem fogalmak tehát általában (egy tetszőleges integritástartományban) nem esnek egybe. Ugyanakkor tudjuk, hogy az egész számok esetén – a $(\mathbb{Z}, +, \cdot)$ gyűrűben – ez a két fogalom egybeesik.

**Feladat.** ▼ Igazoljuk, hogy a $(\mathbb{Z}[i\sqrt{3}], +, \cdot)$ gyűrűben $z = 2$ irreducibilis elem, de nem prímelem.

### 1.4. Legnagyobb közös osztó és legkisebb közös többszörös

**Definíció.** Azt mondjuk, hogy az $a, b \in D$ elemeknek $d \in D$ egy **legnagyobb közös osztó**ja (lnko-ja), ha

i) $d$ közös osztó: $d \mid a, d \mid b$ és

ii) $a, b$ minden közös osztója $d$-nek is osztója : $d' \mid a, d' \mid b \Rightarrow d' \mid d$.

Jelölés: $d = (a, b) = lnko(a, b)$.

Hasonlóan definiálható az $a_1, ..., a_k \in D$ elemeknek a lnko-ja. ▼ Írjuk fel!

**Definíció.** Az $a, b \in D$ elemeknek $m \in D$ egy **legkisebb közös többszörös**e (lkkt-je), ha

i) $m$ közös többszörös: $a \mid m, b \mid m$ és

ii) $a, b$ minden közös többszöröse $m$-nek is többszöröse : $a \mid m', b \mid m' \Rightarrow m \mid m'$.

Jelölés: $m = [a, b] = lkkt[a, b]$.

Hasonlóan definiálható az $a_1, ..., a_k \in D$ elemeknek az lkkt-je. ▼ Írjuk fel!

Az lnko és az lkkt csak az asszociáltság erejéig vannnak meghatározva, feltéve, hogy léteznek.

**Példa.** • $(\mathbb{Z}, +, \cdot)$-ban $a = 4, b = 6$ esetén, $d = \pm 2, m = \pm 12$.

Példát mutatunk arra, hogy két elem lnko-ja nem mindig létezik. Szükségünk van a következőre:

Ha $z = x + iy\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$, akkor $N(z) = |z|^2 = x^2 + 5y^2$ a $z$ **normája**.

**Lemma.** Ha $z, w \in \mathbb{Z}[i\sqrt{5}]$ és $z \mid w$, akkor $N(z) \mid N(w)$.

**Bizonyítás.** Ha $z \mid w$, akkor $w = zt$, innen $N(w) = |w|^2 = |zt|^2 = |z|^2|t|^2 = N(z)N(t)$ és $N(z) \mid N(w)$, mert ezek (nemnegatív) egész számok. □

**Példa.** • $\mathbb{Z}[i\sqrt{5}]$-ben $a = 6$, $b = 2 + 2i\sqrt{5}$ esetén nem létezik lnko.

Valóban, $2 \mid 6$ és $2 \mid 2 + 2i\sqrt{5}$, tehát 2 közös osztó.

$6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, innen $1 + i\sqrt{5} \mid 6$, $1 + i\sqrt{5} \mid 2 + 2i\sqrt{5}$, tehát $1 + i\sqrt{5}$ is közös osztó.

Ha létezne $d = (a, b)$ lnko, akkor $d \mid 6, d \mid 2 + 2i\sqrt{5}$, és $2 \mid d, 1 + i\sqrt{5} \mid d$. Következik, hogy $N(d) \mid 36$, $N(d) \mid 24$, $4 \mid N(d)$, $6 \mid N(d)$, ezek egész számok, így $N(d) \mid (36, 24) = 12$, $12 = [4, 6] \mid N(d)$, innen $N(d) = x^2 + 5y^2 = 12$, de ennek nincs $x, y \in \mathbb{Z}$ megoldása.

**Tétel.** Legyen $D$ egy integritástartomány és tegyük fel, hogy bármely két elemnek létezik lnko-ja. Akkor tetszőleges $a, b, c, d \in D$ elemekre

1. $(a, b) \sim (b, a)$,
2. $((a, b), c) \sim (a, (b, c)$,
3. $(a, a) \sim a$, $(a, 0) \sim a$,
4. $(a, b) \sim a \Leftrightarrow a \mid b$,
5. $(a + bc, b) \sim (a, b)$,
6. $(a, b)c \sim (ac, bc)$,
7. ha $(a, b) \sim 1$, akkor $(a, bc) \sim (a, c)$,
8. ha $a \mid bc$ és $(a, b) \sim 1$, akkor $a \mid c$,
9. ha $d = (a, b)$, $d \neq 0$ és $a = da_1$, $b = db_1$, akkor $(a_1, b_1) \sim 1$.

**Bizonyítás.** 6. Ha $c = 0$, akkor a tulajdonság igaz. Legyen $c \neq 0$, $d = (a, b)$, $d' = (ac, bc)$. Kérdés: $dc \sim d'$?

Itt $d \mid a, d \mid b \Rightarrow dc \mid ac, dc \mid bc \Rightarrow dc \mid (ac, bc) = d'$.

Továbbá, $c \mid ac, c \mid bc \Rightarrow c \mid (ac, bc) = d' \Rightarrow \exists x : d' = xc$ és $xc = d' \mid ac, xc = d' \mid bc \Rightarrow x \mid a, x \mid b$, mert $c \neq 0$.

Innen $x \mid (a,b) = d$ és $d' = xc \mid dc$, kész.

7. Az $(a,b) \sim 1$ feltétel és az előző tulajdonságok alapján $(a,bc) \sim ((a,ac),bc) \sim (a,(ac,bc)) \sim (a,c(a,b)) \sim (a,c)$.

8. Ez a 7. speciális esete. Itt $a \mid bc$ miatt $a \sim (a,bc)$, továbbá 7. alapján $(a,bc) \sim (a,c)$, innen $a \sim (a,c)$, ahonnan $a \mid c$. □

**Feladat.** ▼ Igazoljuk, hogy ha $a,b,c \in D$, $(a,b) \sim 1$ és $(a,c) \sim 1$, akkor $(a,bc) \sim 1$ (feltéve, hogy léteznek az lnko-k).

**Megjegyzések.** 1. Az $a$ és $b$ elemek egy tetszőleges lnko-ját, feltéve, hogy létezik, $(a,b)$-vel jelöljük, annak ellénere, hogy ez nem egyértelműen meghatározott. Így az előbbi tételben ez is írható: $(a,b) = (b,a)$, $((a,b),c) = (a,(b,c)$, stb. Hasonlóan az lkkt $[a,b]$ jelölésére vonatkozóan.

2. $(\mathbb{Z},+,\cdot)$-ban $(a,b)$ és $[a,b]$ mindig a pozitív lnko-t, ill. lkkt-t jelöli $(a,b \neq 0)$, ezek mindig léteznek.

3. Ha $a$ és $b$ közül valamelyik 0, pl. ha $b = 0$, akkor az lnko és lkkt definíciói alapján következik, hogy létezik $(a,b)$, $[a,b]$ és $(a,0) \sim a$, $[a,0] \sim 0$.

**Feladat.** ▼ Igazoljuk, hogy $[[a,b],c] \sim [a,[b,c]]$. Adjuk meg az lkkt más tulajdonságait is!

**Tétel.** Ha $D$ integritástartomány és ha bármely két $a,b \in D$ elemnek létezik lnko-ja, akkor létezik lkkt-je is és

$$(a,b)[a,b] \sim ab.$$

★ **Bizonyítás.** Ha $a = 0$ vagy $b = 0$, akkor $[a,b] = 0$. Legyen $a,b \neq 0$ és $(a,b) = d$. Akkor $d \neq 0$, $a = da_1, b = db_1$, ahol $(a_1,b_1) = 1$.

Azt mutatjuk meg, hogy $m = da_1b_1$ az $a$ és $b$ lkkt-je (annak mintájára, hogy egész számok esetén $m = \frac{ab}{d} = da_1b_1$ lesz).

Itt $m = ab_1$, ahonnan $a \mid m$ és $m = ba_1$, ahonnan $b \mid m$, tehát $m$ közös többszörös.

Ha most $a \mid t, b \mid t$, akkor kérdés, hogy $m \mid t$ ? Legyen $t = ax$, $t = by$, innen $ax = by$, $da_1x = db_1y$ és $d \neq 0$-val osztva $a_1x = b_1y$. Továbbá, az lnko tulajdonsága szerint

$$(a_1x, b_1x) = x(a_1,b_1) = x, \qquad (a_1x,b_1x) = (b_1y,b_1x) = b_1(x,y),$$

ahonnan $b_1(x,y) = x$ és $b_1 \mid x$, $x = b_1z$. Innen $t = ax = ab_1z = mz$, tehát $m \mid t$. □★

**Tétel.** Legyen $D$ egy integritástartomány.

1) Ha $D$-ben bármely két elemnek létezik lnko-ja, akkor bármely $a_1,a_2,...,a_n \in D$ $(n \geq 3)$ elemeknek is létezik lnko-ja és

$$(a_1,a_2,...,a_n) \sim ((a_1,a_2,...,a_{n-1}),a_n).$$

2) Ha $D$-ben bármely két elemnek létezik lkkt-je, akkor bármely $a_1,a_2,...,a_n \in D$ $(n \geq 3)$ elemeknek is létezik lkkt-je és

$$[a_1,a_2,...,a_n] \sim [[a_1,a_2,...,a_{n-1}],a_n].$$

★ **Bizonyítás.** Lásd pl. [M], 13. old. ★

A következő Tétel megadja annak egy elegséges feltételét, hogy minden irreducibilis elem prímelem legyen (azaz, hogy az irreducibilis elemek egybeessenek a prímelemekkel).

**Tétel.** Ha egy $D$ integritástartományban bármely két elemnek létezik lnko-ja, akkor minden irreducibilis elem prímelem.

**Bizonyítás**. Tegyük fel, hogy $p$ irreducibilis elem és igazoljuk, hogy $p$ prímelem. Kérdés tehát: $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$?

Ha $p \mid a$, akkor kész. Ha $p \nmid a$, akkor kérdés: $p \mid b$? Itt $(p, a) \sim 1$, mert $p \nmid a$ és $p$ irreducibilis. Innen $p \mid ab, p \mid pb \Rightarrow p \mid (ab, pb) \sim (a, p)b \sim b \Rightarrow p \mid b$, kész. □

Kérdés ezek után, hogy mikor létezik az lnko?

**Definíció.** Ha $(a, b) \sim 1$, akkor azt mondjuk, hogy $a, b$ **relatív prímek**. Az $a_1, ..., a_k$ elemek **relatív prímek**, ha $(a_1, ..., a_k) \sim 1$ és **páronként relatív prímek**, ha $(a_i, a_j) \sim 1$ minden $i \neq j$-re. Ezt így is jelöljük: $(a, b) = 1$, ill. $(a_i, a_j) = 1$.

Azonnali, hogy ha $a_1, ..., a_k$ páronként relatív prímek, akkor relatív prímek, de fordítva nem. ▼ Adjunk erre példát!

**Feladat.** ▼ Igazoljuk, hogy az $F_n = 2^{2^n} + 1$, $n \geq 0$, ún. Fermat-számok páronként relatív prímek.

### 1.5. Gauss-gyűrűk

**Definíció.** A $(D, +, \cdot)$ integritástartomány **Gauss-gyűrű** (vagy **faktoriális gyűrű** vagy **irreducibilis faktorizációs gyűrű**), ha minden $a \in D, a \neq 0, a \nsim 1$ elem felbontható irreducibilis tényezők szorzatára és az asszociáltaktól eltekintve a felbontás egyértelmű, azaz

1) léteznek olyan $p_1, ..., p_r$ irreducibilis elemek, hogy $a = p_1 \cdots p_r$ és

2) ha ugyanakkor $a = q_1 \cdots q_s$ irreducibilis tényezők szorzata, akkor $r = s$ és a $p_1, ..., p_r$ és $q_1, ..., q_r$ elemek páronként asszociáltak.

**Tétel.** Legyen $(D, +, \cdot)$ egy integritástartomány. $D$ akkor és csak akkor Gauss-gyűrű, ha teljesül a fenti 1) és az alábbi $2^*$) tulajdonság:

$2^*$) $D$-ben minden irreduciblis elem prímelem.

**Bizonyítás.** Tegyük fel, hogy $D$ Gauss-gyűrű és igazoljuk a $2^*$) tulajdonságot. Legyen $q \in D$ irreducibilis és legyen $q \mid ab$. Kérdés, hogy $q \mid a$ vagy $q \mid b$?

Ha $a = 0$, akkor $q \mid a$ igaz, ha $b = 0$, akkor $q \mid b$ teljesül. Ha $a \sim 1$, akkor $q \mid b$ igaz, hasonlóan ha $b \sim 1$, akkor $q \mid a$. Ezért feltehetjük, hogy $a, b \neq 0$ és $a, b$ nem egységek.

Itt $q \mid ab$ alapján létezik $v \in D$ úgy, hogy $ab = qv$. Következik, hogy $v \neq 0$ és $v$ sem egység, mert $q$ irreducibilis.

Az $ab = qv$ elem 1) alapján felbontható irreducibilis elemek szorzatára és 2) szerint ez a felbontás egyértelmű, ezért $q$ egy asszociáltja elő kell forduljon az $a$ vagy a $b$ felbontásában. Így $q \mid a$ vagy $q \mid b$ következik.

Fordítva, ha feltételezzük, hogy teljesül 1) és $2^*$), akkor igazolható 2), lásd pl. [SzÁ], 143. old. □

A definíció alapján azonnali, hogy

**Következmény.** Ha $D$ Gauss-gyűrű, akkor minden $a \in D, a \neq 0$ elem felírható

$$a = ep_1^{k_1} \cdots p_t^{k_t}$$

alakban, ahol $e$ egység, $t \geq 0$, $k_i \geq 1$ egészek és $p_i$ páronként nem asszociált irreducibilis elemek. Itt $t = 0$ is megengedett, ekkor $a = e \sim 1$ egység. □

Továbbá a definíciókból azonnali az is, hogy

**Következmény.** Ha még $b = fp_1^{\ell_1} \cdots p_t^{\ell_t}$, ahol most $k_i, \ell_i \geq 0$, továbbá $a \neq 0, b \neq 0$, akkor

i) $a \mid b \Leftrightarrow k_i \leq \ell_i$ minden $i$-re,

ii)

$$(a, b) \sim p_1^{\min(k_1, \ell_1)} \cdots p_t^{\min(k_t, \ell_t)},$$

$$[a,b] \sim p_1^{\max(k_1,\ell_1)} \cdots p_t^{\max(k_t,\ell_t)},$$

tehát az lnko és lkkt létezik minden Gauss-gyűrűben. □

**Következmény.** Gauss-gyűrűkben minden irreducibilis elem prímelem, tehát az irreducibilis elem és a prímelem fogalmai egybeesnek.

**Bizonyítás.** Lásd a jelen szakasz Tételét vagy az 1.4. szakasz utolsó tételét. □

**Példák.** • $(\mathbb{Z},+,\cdot)$ Gauss-gyűrű,

2. $(K[X],+,\cdot)$ Gauss-gyűrű, ahol $K$ kommutatív test,

3. $(\mathbb{Z}[i\sqrt{5}],+,\cdot)$ nem Gauss-gyűrű, mert láttuk, hogy nem mindig létezik az lnko (és nem minden irreducibilis elem prímelem).

### 1.6. Főideálgyűrűk

**Definíció.** A $D$ integritástartomány **főideálgyűrű**, ha minden ideálja főideál, azaz ha minden $I \trianglelefteq D$ ideál esetén létezik $x \in D$ úgy, hogy $D = (x) = \{dx : d \in D\}$.

**Példák.** • $(\mathbb{Z},+,\cdot)$ főideálgyűrű, lásd Absztrakt algebra anyag.

• $(K[X],+,\cdot)$ főideálgyűrű, ahol $K$ kommutatív test, lásd Absztrakt algebra anyag.

Igazolható, hogy:

**Tétel.** Ha $D$ főideálgyűrű, akkor $D$ Gauss-gyűrű és minden $a,b \in D$ esetén

$$(a)+(b)=(d), \qquad (a)\cap(b)=(m),$$

ahol $d = \text{lnko}\,(a,b)$, $m = \text{lkkt}\,[a,b]$. □

A főideálgyűrűkkel részletesebben nem foglalkozunk.

### 1.7. Megoldások

1.1. Oszthatóság

▼ Teljesül-e $z \mid w$, ha

a) $D=\mathbb{Z}[i]$, $z=2+i, w=13+11i$,

b) $D=Z[i]$, $z=2-i, w=13+11i$,

c) $D=\mathbb{Z}[i\sqrt{5}]$, $z=3+2i\sqrt{5}, w=36-5i\sqrt{5}$,

d) $D=\mathbb{Z}[\sqrt{3}]$, $z=2+3\sqrt{3}, w=13+2\sqrt{3}$.

**Megoldás.** c)

$$\frac{36-5i\sqrt{5}}{3+2i\sqrt{5}} = \frac{(36-5i\sqrt{5})(3-2i\sqrt{5})}{(3+2i\sqrt{5})(3-2i\sqrt{5})} = \frac{58-87i\sqrt{5}}{29} = 2-3i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}],$$

teljesül.

▼ $(\mathbb{Z}[i],+,\cdot)$ egységei: $U(\mathbb{Z}[i]) = \{-1,1,-i,i\}$.

**Megoldás.** Legyen $z=a+bi \in \mathbb{Z}[i]$ egység. Akkor $z^{-1}=\frac{1}{z}=\frac{1}{a+bi}=\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i \in \mathbb{Z}[i]$ kell legyen. Itt $a,b\neq 0$ esetén $|a|<a^2+b^2$, $|b|<a^2+b^2$ és ekkor $z^{-1}\notin\mathbb{Z}[i]$. Ha $a=0$, akkor $z^{-1}=-\frac{1}{b}i\in\mathbb{Z}[i]$ alapján $b=\pm1$, hasonlóan, ha $b=0$.

▼ Melyek $\mathbb{Z}[\sqrt{d}]$ egységei, ha $d<0$?

**Megoldás.** Ha $d=-1$ (Gauss-egészek), akkor az egységek: $\pm1,\pm i$. Ha $d\leq -2$, akkor az egységek $\pm1$, lásd korábbi Feladat.

1.3. Irreducibilis elemek és prímelemek

▼ Igazoljuk, hogy a $(\mathbb{Z}[i\sqrt{3}],+,\cdot)$ gyűrűben $z=2$ irreducibilis elem, de nem prímelem.

**Megoldás.** Tegyük fel, hogy $2 = (a+bi\sqrt{3})(c+di\sqrt{3})$. Komplex konjugáltakat tekintve $2 = (a-bi\sqrt{3})(c-di\sqrt{3})$. Összeszorozva: $4 = (a^2+3b^2)(c^2+3d^2)$. Ha $a^2+3b^2 = 1$, akkor $a = \pm 1, b = 0$, az első tényező egység. Ha $a^2+3b^2 = 2$, ennek nincs megoldása. Ha $a^2+3d^2 = 4$, akkor $c^2+3d^2 = 1$, a második tényező egység. Tehát 2 irreducibilis. Továbbá, $2 \mid 4 = (1+i\sqrt{3})(1-i\sqrt{3})$ és ha 2 prím lenne, akkor osztója lenne valamelyik tenyezőnek, de ez ellentmondás, mert $\frac{1\pm i\sqrt{3}}{2} = \frac{1}{2} \pm \frac{1}{2}i\sqrt{3} \notin \mathbb{Z}[i\sqrt{3}]$.

## 2. Euklideszi gyűrűk

Az euklideszi gyűrű az az algebrai strukúra, amely eléggé speciális ahhoz, hogy igaz legyen benne az egész számok esetén megismert legtöbb számelméleti tulajdonság. Ugyanakkor az euklideszi gyűrű fogalma eléggé általános ahhoz, hogy magába foglalja az egész számok gyűrűjén kívül a kommutatív testek feletti polinomgyűrűket, a Gauss-egészek gyűrűjét, az Eisenstein-egészek gyűrűjét és másokat, és így ezek mindegyikében a szokásoshoz hasonló számelmélet építhető ki.

### 2.1. Euklideszi gyűrűk és tulajdonságaik

**Definíció.** A $D$ integritástartomány **euklideszi gyűrű**, ha van olyan $N : D \setminus \{0\} \to \mathbb{N}$ függvény, hogy minden $a, b \in D, b \neq 0$ esetén létezik $q, r \in D$ úgy, hogy

$$(*) \qquad \boxed{a = bq + r}\ , \text{ ahol } r = 0 \text{ vagy } N(r) < N(b).$$

Itt $N$ neve **euklideszi norma**, ennek más jelölése: $N(a) = ||a||$. A (*) egyenlőséget a **maradékos osztás képlet**ének nevezzük, $q$ az **osztási hányados**, $r$ az **osztási maradék**.

**Példák.** • $(\mathbb{Z}, +, \cdot)$ euklideszi gyűrű, ahol $N(x) = |x|$, a feltételek teljesülnek a maradékos osztás tétele szerint.

• $(K[X], +, \cdot)$ euklideszi gyűrű, ahol $K$ kommutatív test, itt $N(f) = \operatorname{gr} f$ az $f \neq 0$ foka, tudjuk, hogy a $K$ feletti polinomokra is igaz a maradékos osztás tétele.

• Minden $K$ test euklideszi gyűrű. Valóban, legyen $N : K \setminus \{0\} \to \mathbb{N}$, $N(x) = 1$ minden $x \in K, x \neq 0$ esetén. Ez euklideszi norma.

**Tétel.** Ha $D$ euklideszi gyűrű, akkor $D$ főideálgyűrű.

**Bizonyítás.** Legyen $I \trianglelefteq D$ tetszőleges ideál. Ha $I = \{0\}$, akkor $I = (0)$, kész. Ha $I \neq \{0\}$, akkor kérdés, hogy létezik-e $a \in D$ úgy, hogy $I = (a)$.

Legyen $A = \{N(x) : x \in I, x \neq 0\} \subseteq \mathbb{N}$ és $n = \min A$, továbbá legyen $a \in I, a \neq 0$ úgy, hogy $N(a) = n$. Igazoljuk, hogy $I = (a)$.

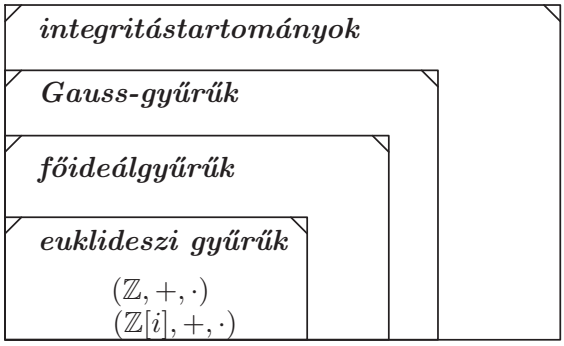
Itt $a \in I$ alapján $(a) \subseteq I$ azonnali.

Fordítva, ha $b \in I$, akkor $b = aq + r$ alakú, ahol $q, r \in D$ és $N(r) < N(a)$. Itt $r = b - aq \in I$, mert $I$ ideál.

Ha $N(r) \neq 0$, akkor ez ellentmond az $N(a)$ minimalitásának, ezért $N(r) = 0$, innen $r = 0$, $b = aq \in (a)$, $I \subseteq (a)$. $\square$

**Következmény.** 1) Ha $D$ euklideszi gyűrű, akkor $D$ Gauss-gyűrű.

2) Ha $D$ euklideszi gyűrű, akkor bármely két $a, b \in D$ elemnek létezik lnko-ja és lkkt-je, továbbá az irreducibilis elem és a prímelem fogalmak egybeesnek.




**1. ábra**

**Bizonyítás.** 1) Ha $D$ euklideszi gyűrű, akkor $D$ főideálgyűrű, az előző Tétel alapján. Továbbá minden főideálgyűrű Gauss-gyűrű az 1.6. szakasz Tétele szerint. Ezeket a kapcsolatokat szemlélteti az 1. ábra.

2) Ha $D$ euklideszi gyűrű, akkor $D$ Gauss-gyűrű az 1) pont szerint és Gauss-gyűrűben létezik az lnko és az lkkt, lásd 1.5. szakasz. □

**Feladat.** ▼ Hol helyezhetők el az 1. ábrán a $(\mathbb{Z}[i\sqrt{5}],+,\cdot)$ és a $(\mathbb{Z}[i\sqrt{3}],+,\cdot)$ gyűrűk?

Két elem legnagyobb közös osztójának létezése euklideszi gyűrűkben közvetlenül is belátható és fontos az a tény, hogy euklideszi gyűrűkben van olyan eljárás, amellyel meghatározható az lnko az elemek irreducibilis felbontása nélkül (ami általában nehéz feladat). Ez az eljárás az euklideszi algoritmus.

**Az euklideszi algoritmus.** Minden $D$ euklideszi gyűrűben létezik olyan véges algoritmus, amelynek segítségével meghatározható két elem lnko-ja.

Az euklideszi algoritmus lépései: Legyenek $a,b\in D$. Ha $b=0$, akkor $(a,0)=a$. ha $b\neq 0$, akkor a maradékos osztás képlete alapján:

$$a=bq_1+r_1,\quad r_1=0 \text{ vagy } N(r_1)<N(b).$$

Ha $r_1\neq 0$, akkor ismét a maradékos osztás képlete alapján:

$$b=r_1q_2+r_2,\quad r_2=0 \text{ vagy } N(r_2)<N(r_1).$$

Ismételve ezt kapjuk a $q_3,q_4,...\in D$ és az $r_3,r_4,...\in D$ elemeket, amelyekre

$$r_1=r_2q_3+r_3,\quad r_3=0 \text{ vagy } N(r_3)<N(r_2),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1},\quad r_{n-1}=0 \text{ vagy } N(r_{n-1})<N(r_{n-2}),$$

$$r_{n-2}=r_{n-1}q_n+r_n,\quad r_n=0 \text{ vagy } N(r_n)<N(r_{n-1}),$$

$$r_{n-1}=r_nq_{n+1},\quad r_{n+1}=0.$$

Az algoritmus akkor ér véget ha a kapott maradék nulla és ez véges sok lépés után bekövetkezik, hiszen $N(b)>N(r_1)>N(r_2)>...$ szigorúan csökkenő nemnegatív egészekből álló sorozat. Tegyük fel, hogy $r_1\neq 0, r_2\neq 0,...,r_n\neq 0$ és $r_{n+1}=0$. Megmutatjuk, hogy az $a$ és $b$ elemek (egy) legnagyobb közös osztója az utolsó nemnulla maradék, azaz $\boxed{(a,b)=r_n}$.

Az utolsó egyenletből $r_n\mid r_{n-1}$, az utolsó előttiből $r_n\mid r_{n-2}$ (lásd az oszthatóság tulajdonságait) és visszafelé haladva rendre kapjuk, hogy $r_n\mid r_{n-3},...,r_n\mid r_2, r_n\mid r_1, r_n\mid b, r_n\mid a$, tehát $r_n$ közös osztó. Ha pedig $c\mid a, c\mid b$, akkor az első egyenletből $c\mid r_1$, a másodikból $c\mid r_2$ és lefelé haladva következik, hogy $c\mid r_3,...,c\mid r_{n-2}, c\mid r_{n-1}, c\mid r_n$, azaz $c\mid r_n$. □

A fentiek alapján az is következik, hogy

**Tétel.** Ha $D$ euklideszi-gyűrű és $a,b\in D$, akkor léteznek olyan $u,v\in D$ elemek, hogy $(a,b)=au+bv$.

**Bizonyítás.** A fenti utolsó előtti egyenletből $(a,b)=r_n=r_{n-2}-r_{n-1}q_n=...$, haladjunk visszafelé. ▼ Írjuk le részletesen! □

**Feladatok.** ▼ 1. Alkalmazzuk az euklideszi algorimust az $a=33855, b=18870$ számokra és határozzunk meg olyan $x,y\in\mathbb{Z}$ számokat, amelyekre $33855x+18870y=d$, ahol $d=(33855,18870)$.

▼ 2. Alkalmazzuk az euklideszi algorimust az $f = 3X^3 - X^2 - 3X + 1, g = 2X^3 - 2X^2 - 3X + 3 \in \mathbb{Q}[X]$ polinomokra és határozzunk meg olyan $u, v \in \mathbb{Q}[X]$ polinomokat, amelyekre $fu + gv = d$, ahol $d = (f, g)$.

**Tétel.** (Kongruenciák tulajdonságai euklideszi gyűrűkben) Legyen $D$ egy euklideszi gyűrű, $a, b, c, d, m, m_1, m_2 \in D$, $m, m_1, m_2 \neq 0$ és $k \in \mathbb{N}^*$.

i) Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$, tehát azonos modulusú kongruenciákat össze lehet adni és össze lehet szorozni;

ii) Ha $a \equiv b \pmod{m}$, akkor $a + c \equiv b + c \pmod{m}$ és $ac \equiv bc \pmod{m}$, tehát egy kongruencia mindkét oldalához hozzá lehet adni ugyanazt az elemet és a kongruencia mindkét oldalát szorozni lehet ugyanazzal az elemmel;

iii) Ha $a \equiv b \pmod{m}$, akkor $a^k \equiv b^k \pmod{m}$, kongruenciát lehet hatványozni;

iv) Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{\frac{m}{d}}$, ahol $c \neq 0$ és $d = (c, m)$;

v) Ha $ac \equiv bc \pmod{m}$ és $(c, m) = 1$, akkor $a \equiv b \pmod{m}$, kongruenciát lehet egyszerűsiteni egy, a modulussal relatív prím elemmel és a modulus nem változik;

vi) Ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$, akkor $a \equiv b \pmod{[m_1, m_2]}$.

vii) Ha $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ és $m_1, m_2$ relatív prímek, akkor $a \equiv b \pmod{m_1 m_2}$.

**Bizonyítás.** Lényegében úgyanúgy, mint az egész számok esetén. Az i) tulajdonságot már láttuk az 1.2. szakaszban.

i) A feltétel szerint $m \mid a - b$ és $m \mid c - d$, ahonnan $m \mid (a - b) + (c - d) = (a + c) - (b + d)$, tehát $a + c \equiv b + d \pmod{m}$, valamint $m \mid c(a - b) + b(c - d) = ac - bd$, ahonnan $ac \equiv bd \pmod{m}$.

ii) Speciális esete i)-nek, ahol $d = c$.

iii) Az i) ismételt alkalmazásával ($c = a, d = b$), ha $a \equiv b \pmod{m}$, akkor $a^2 \equiv b^2 \pmod{m}$,...,$a^k \equiv b^k \pmod{m}$. Abból is következik, hogy minden $k \in \mathbb{N}^*$ számra $a - b \mid a^k - b^k$.

iv) A feltétel szerint $m \mid ac - bc = (a - b)c$, így $\frac{m}{d} \mid (a - b)\frac{c}{d}$. Itt $(\frac{m}{d}, \frac{c}{d}) = 1$ és kapjuk, hogy $\frac{m}{d} \mid a - b$, azaz $a \equiv b \pmod{\frac{m}{d}}$, lásd korábbi Tétel.

v) Az előző pont speciális esete, ha $d = (c, m) = 1$.

vi) Ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$, akkor $m_1 \mid a - b$ és $m_2 \mid a - b$, tehát $a - b$ közös többszöröse az $m_1$ és $m_2$ elemeknek és így $a - b$ többszöröse az $[m_1, m_2]$ lkkt-nek (az lkkt definíciója szerint).

vii) Speciális esete vi)-nak: ha $(m_1, m_2) = 1$, akkor $[m_1, m_2] = m_1 m_2$. □

**Tétel.** Legyen $D$ egy euklideszi gyűrű, $a, b, m \in D, a \neq 0, m \neq 0$.

1) Az $\boxed{ax \equiv b \pmod{m}}$ kongruenciának akkor és csak akkor van $x \in D$ megoldása, ha $(a, m) \mid b$.

2) Ha létezik $x_0$ megoldás, akkor az összes megoldás a következő alakú:

$$\boxed{x = x_0 + \frac{m}{(a, m)}t, \quad t \in D,}$$

ahol $\frac{m}{(a,m)}$ azt az $m_1 \in D$ elemet jelöli, amelyet az $m = m_1(a, m)$ egyenlőség határoz meg.

3) Ha $(a, m) = 1$, akkor létezik megoldás és egy megoldás van (mod $m$), azaz bármely két megoldás kongruens (mod $m$).

**Bizonyítás.** Legyen $(a, m) = d$, itt $d \neq 0$.

1) Tegyük fel, hogy $x = x_0$ megoldás, akkor $m \mid ax_0 - b$, ahonnan $ax_0 - b = km, k \in D$. Mivel $d \mid a$ és $d \mid m$ kapjuk, hogy $d \mid ax_0 - km = b$.

Fordítva, ha $d \mid b$, akkor legyen $b = de$. Tétel szerint létezik $u, v \in D$ úgy, hogy $(a, m) = d = au + mv$, innen $e$-vel szorozva $de = aue + mev$ és kapjuk, hogy $a(ue) \equiv b \pmod{m}$, tehát $x = ue$ megoldás.

2) Legyen $x_0$ egy rögzített megoldás és $x$ egy másik megoldás. Akkor $ax_0 \equiv b \pmod{m}$ és $ax \equiv b \pmod{m}$. Innen $a(x - x_0) \equiv 0 \pmod{m}$, azaz $a(x - x_0) = mk$, $k \in D$. Legyen $a = da_1$, $m = dm_1$, ahol $(a_1, m_1) = 1$. Kapjuk, hogy $da_1(x - x_0) = dm_1k$, $a_1(x - x_0) = m_1k$, mert $d \neq 0$. Innen $m_1 \mid a_1(x - x_0)$ és mivel $(a_1, m_1) = 1$ következik, hogy $m_1 \mid x - x_0$, $x \equiv x_1 \pmod{m_1}$, lásd az oszthatóság tulajdonságait.

3) Azonnali az előzőek alapján. □

**Tétel.** Legyen $D$ egy euklideszi gyűrű, $a, b, c \in D, a \neq 0, b \neq 0$.

1) Az $\boxed{ax + by = c}$ egyenletnek akkor és csak akkor van $x, y \in D$ megoldása, ha $(a, b) \mid c$.

2) Ha létezik $x_0, y_0$ megoldás, akkor az összes megoldás a következő alakú:

$$\boxed{x = x_0 + \frac{b}{(a,b)}t, \quad y = y_0 - \frac{a}{(a,b)}t, \quad t \in D.}$$

**Bizonyítás.** 1) Ha $ax + by = c$ teljesül valamely $x, y \in D$ elemekre, akkor $ax \equiv c \pmod{b}$, ennek a kongruenciának tehát van $x \in D$ megoldása. Az előző Tétel szerint következik, hogy $(a, b) \mid c$. Fordítva, ha $(a, b) \mid c$, akkor ismét e Tétel szerint van olyan $x \in D$, hogy $ax \equiv c \pmod{b}$, innen $ax - c = by$, $ax - by = c$, $y \in D$, tehát $x, -y$ megoldás.

2) Ha $x_0, y_0$ megoldás, akkor $ax_0 + by_0 = c$. Legyen $x, y$ egy tetszőleges megoldás. Akkor $ax + by = c$ és (*) $a(x - x_0) + b(y - y_0) = 0$. Továbbá $x_0$ és $x$ megoldásai az $ax \equiv c \pmod{b}$ kongruenciának és az előző Tétel szerint $x = x_0 + \frac{b}{(a,b)}t$. Ezt beírva (*)-ba $a\frac{b}{(a,b)}t + b(y - y_0) = 0$, innen $b$-vel egyszerűsítve $y = y_0 - \frac{a}{(a,b)}t$. Behelyettesítve ezeket az $x$ és $y$ értékeket az $ax + by = c$ egyenletbe kapjuk, hogy ezek valóban megoldások minden $t \in D$-re. □

Az 1.2. szakaszban láttuk, hogy ha $D$ integritástartomány, akkor $(D_m, +, \cdot)$ egy kommutatív egységelemes gyűrű, ennek neve a (mod $m$) maradékosztálygyűrű.

**Tétel.** Legyen $D$ egy euklideszi-gyűrű. A $(D_m, +, \cdot)$ maradékosztálygyűrű akkor és csak akkor test, ha $m$ irreducibilis elem (prímelem).

**Bizonyítás.** Tegyük fel, hogy $m$ irreducibilis elem és igazoljuk, hogy $D_m$ test. A kérdés az, hogy invertálható-e minden $\widehat{a} \in D_m$, $\widehat{a} \neq \widehat{0}$ elem, azaz létezik-e $\widehat{x} \in D_m$ úgy, hogy $\widehat{a}\widehat{x} = \widehat{1}$ ?

Az $\widehat{a} \neq \widehat{0}$ feltételből $a \not\equiv 0 \pmod{m}$, azaz $m \nmid a$. Mivel $m$ irreducibilis következik, hogy $(a, m) = 1$. Kapjuk, hogy az $ax \equiv 1 \pmod{m}$ kongruenciának van $x \in D$ megoldása, lásd korábbi Tétel, innen $\widehat{a}\widehat{x} = \widehat{1}$, amit igazolni kellett.

Fordítva, tegyük fel, hogy $D_m$ test és $m$ nem irreducibilis. Akkor $m$ felírható $m = m_1m_2$ alakban, ahol $m_1, m_2$ valódi osztók, azaz $m_1, m_2$ nem asszociáltak 1-gyel és nem asszociáltak $m$-mel. Tekintsük az $\widehat{m_1} \in D_m$ elemet, ahol $\widehat{m_1} \neq \widehat{0}$, mert $m \nmid m_1$. A feltétel szerint ennek létezik $\widehat{x} \in D_m$ inverze, amelyre $\widehat{m_1}\widehat{x} = \widehat{1}$. Innen $m \mid m_1x - 1$ és $m_1x - my = 1$ valamely $y \in D$-re. Mivel $m_1 = (m_1, m) \mid m_1x - my$ kapjuk, hogy $m_1 \mid 1$, ami ellentmondás. □

**Megjegyzés.** A bizonyítás második részében rövidebben: Ha $m = m_1m_2$, ahol $m_1, m_2$ valódi osztók, akkor $\widehat{m_1}, \widehat{m_2} \neq \widehat{0}$, de $\widehat{m_1}\widehat{m_2} = \widehat{m} = \widehat{0}$, azaz $\widehat{m_1}$ és $\widehat{m_2}$ zérusosztók. Következik, hogy $D_m$ nem test, mert tesben nincsenek zérusosztók. □

**Példa.** • A $\mathbb{Z}_m$ maradékosztálygyűrű akkor és csak akkor test, ha $m$ prímszám.

**Definíció.** Az $\widehat{a}$ (mod $m$) maradékosztály neve **redukált maradékosztály** (mod $m$), ha $(a,m)=1$. Ez az definíció nem függ a reprezentáns megválasztásától. Valóban, ha $\widehat{b}=\widehat{a}$, akkor $b\equiv a \pmod m$, ahonnan $b=a+km$, $k\in D$ és ha $(a,m)=1$, akkor $(b,m)=(a+km,m)=(a,m)=1$.

**Tétel.** A $\widehat{a}$ (mod $m$) maradékosztály akkor és csak akkor redukált maradékosztály, ha invertálható (egység) a $D_m$ maradékosztály-gyűrűben.

**Bizonyítás.** Ha $\widehat{a}$ (mod $m$) redukált maradékosztály, akkor $(a,m)=1$. Következik, hogy az $ax\equiv 1 \pmod m$ kongruenciának van megoldása, azaz van olyan $\widehat{x}\in D_m$, amelyre $\widehat{a}\widehat{x}=\widehat{1}$. Kapjuk, hog $\widehat{a}$ invertálható.

Fordítva, ha $\widehat{a}$ invertálható, akkor van olyan $x\in D$, hogy $\widehat{a}\widehat{x}=\widehat{1}$, $ax\equiv 1 \pmod m$ és innen $(a,m)\mid 1$, azaz $(a,m)=1$. □

A (mod $m$) redukált maradékosztályok $\{\widehat{a} : (a,m)=1\}$ halmaza tehát egyenlő az $U(D_m)$ halmazzal, lásd 1.1. szakasz.

**Következmény.** Ha $D$ euklideszi gyűrű, akkor a (mod $m$) redukált maradékosztályok Abel-csoportot alkotnak. □

★ **Tétel.** (Általánosított Euler-tétel) Legyen $D$ euklideszi gyűrű és tegyük fel, hogy az $(U(D_m),\cdot)$ csoport rendje véges, jelölje ezt $k=k(D_m)$. Akkor minden $a\in D$, $(a,m)=1$ elemre

$$a^k\equiv 1 \pmod m.$$

**Bizonyítás.** Alkalmazzuk a Lagrange-tételt az $(U(D_m),\cdot)$ csoportra. Kapjuk, hogy minden $\widehat{a}\in U(D_m)$ esetén $\widehat{a}^k=\widehat{1}$, azaz $\widehat{a^k}=\widehat{1}$, ami egyeértékű azzal, hogy $a^k\equiv 1 \pmod m$, ahol $(a,m)=1$. □

Ha $D=\mathbb{Z}$, akkor az egész számokra vonatkozó Eulet-tételt kapjuk. ★

### 2.2. A Gauss-egészek aritmetikája

**Tétel.** A Gauss-egészek $(\mathbb{Z}[i],+,\cdot)$ gyűrűje euklideszi gyűrű, ahol $N(z)=|z|^2=a^2+b^2$, $z=a+bi\in\mathbb{Z}[i]$.

**Bizonyítás.** Kérdés, hogy $\forall z,w\in\mathbb{Z}[i], w\neq 0:\ \exists\, q,r\in\mathbb{Z}[i]:\ z=qw+r$, ahol $r=0$ vagy $N(r)<N(w), r\neq 0$ ?

Ha a $q$-t már megválasztottuk, akkor $r=z-qw$ lesz. Ha $r=0$, akkor nincs mit bizonyítani, ha pedig $r\neq 0$, akkor kell, hogy

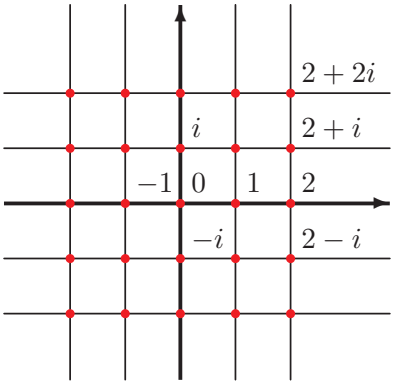
$$N(r)=N(z-qw)=|z-qw|^2<|w|^2,\quad \text{innen}\quad \left|\frac{z}{w}-q\right|^2<1,\quad \text{azaz}\quad \left|\frac{z}{w}-q\right|<1.$$

A Gauss-egészek a komplex számsíkon rácspontokat és egységoldalú rácsnégyzeteket határoznak meg, lásd 2. ábra. A $z/w$ komplex szám egy ilyen rácsnégyzetbe vagy annak oldalára esik. E rácsnégyzet két átellenes csúcsa köré rajzoljunk egy-egy egységkörívet, így következik, hogy $z/w$ távolsága e két csúcs valamelyikétől kisebb mint 1, lásd 3. ábra, tehát teljesül a fenti feltétel.

Másképp: itt $z/w$ egy komplex szám, legyen $z/w=u+iv$, ahol $u,v\in\mathbb{Q}$. Tekintsük az $u$ és $v$-hez legközelebb eső $x,y\in\mathbb{Z}$ számokat, amelyekre $|u-x|\le 1/2$, $|v-y|\le 1/2$, és legyen $q=x+iy\in\mathbb{Z}[i]$, lásd 4. ábra. Akkor

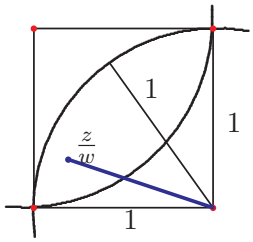
$$\left|\frac{z}{w}-q\right|^2=|(u-x)+i(v-y)|^2=(u-x)^2+(v-y)^2\le\frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1,$$

amit bizonyítani kellett. □

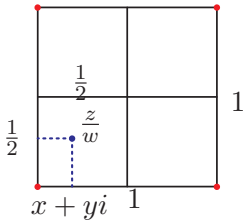



**2. ábra**. Gauss-egészek

**Megjegyzés.** A bizonyításból következik, hogy a $q$ hányados és az $r$ maradék nem egyértelmű, kivéve, ha $z/w$ rácspont, azaz $w \mid z$, ekkor $r = 0$ és $q = z/w$.




**3. ábra**




**4. ábra**

**Példa.** • Legyen $z = 3 - 17i$, $w = 3 + 2i$. Akkor

$$\frac{z}{w} = \frac{3-17i}{3+2i} = \frac{(3-17i)(3-2i)}{9+4} = -\frac{25}{13} - \frac{57}{13}i,$$

ahol $-\frac{25}{13} = -1,923...$, $-\frac{57}{13} = -4,384...$ és a legközelebbi egészeket választva: $x = -2, y = -4$, innen következik, hogy a $q = -2 - 4i$ választással $z = wq + r$, ahol $r = 1 - i$ és $N(r) = 2 < 13 = N(w)$. Vehető $q' = -2 - 5i$ is (készítsünk rajzot), ekkor $z = wq' + r'$, ahol $r' = -1 + 2i$ és $N(r') = 5 < 13 = N(w)$.

**Feladat.** ▼ Legyen $z = 6i$, $w = 2 + 2i$. Határozzuk meg az osztási hányadost és maradékot. Mutassuk meg, hogy ezek 4-féleképpen is megválaszthatók.

A Gauss-egészek tehát euklideszi-gyűrűt alkotnak az $N(z) = |z|^2 = a^2 + b^2$, $z = a + bi$ normára nézve, ahol $N(z) \geq 0$ egész szám. Azért előnyös normának az abszolút érték négyzetét venni, mert ez mindig nemnegatív egész szám, ugyanakkor $|z| = \sqrt{a^2 + b^2}$ lehet irracionális is.

Következik, hogy a Gauss-egészekre érvényesek mindazok a tulajdonságok, amelyeket euklideszi gyűrűkre mondtunk ki. Így az irreducibilis Gauss-egészek azonosak a prím Gauss-egészekkel, ezeket Gauss-prímeknek nevezzük. Bármely két Gauss-egésznek létezik lnko-ja és lkkt-je és az lnko meghatározható a euklideszi algoritmussal.

Nézzük a továbbiakban a Gauss-egészek speciális tulajdonságait. Már láttuk, hogy itt az egységek a $\pm 1, \pm i$, így egy $z \in \mathbb{Z}[i]$ asszociáltjai $z, -z, iz, -iz$. További tulajdonságokat rögzít a következő

**Tétel.** Legyenek $z, w \in \mathbb{Z}[i]$.

1. $N(z) = 0$ akkor és csak akkor, ha $z = 0$,

2. $N(z) = 1$ akkor és csak akkor, ha $z$ egység,
3. $N(zw) = N(z)N(w)$,
4. $z \mid N(z)$,
5. ha $z \mid w$, akkor $N(z) \mid N(w)$,
6. minden $w \neq 0$ számnak véges sok osztója van.

**Bizonyítás.** A definíciók alapján. Pl. 4. $z \mid z\overline{z} = |z|^2 = N(z)$, ahol $\overline{z}$ a $z$ komplex konjugáltja.

5. Ha $z \mid w$, akkor létezik $t \in \mathbb{Z}[i]$ úgy, hogy $w = zt$ és 3. alapján $N(w) = N(z)N(t)$, tehát $N(z)$ osztója $N(w)$-nek.

6. Ha $z \mid w$, akkor 5. alapján $N(z) \mid N(w)$, ahol $w \neq 0$ miatt $N(w) \neq 0$. Egy nemnulla egész számnak véges sok osztója van, ezért $N(z)$ és vele együtt $z$ is véges sok értéket vehet fel. □

**Feladatok.** ▼ 1. Igaz-e, hogy ha $N(z) \mid N(w)$, akkor $z \mid w$?

▼ 2. Igazoljuk, hogy ha $z_1$ és $z_2$ asszociáltak, akkor $N(z_1) = N(z_2)$. Igaz-e ez fordítva?

▼ 3. Vizsgáljuk meg, hogy lehet-e $\overline{z}$ (komplex konjugált) osztója $z$-nek.

▼ 4. a) Osztója-e $3 + 5i$-nek $4 + i$, ill. $4 - i$ ? b) Határozzuk meg $3 + 5i$ összes osztóját.

Kérdés, hogy mely $z = a + bi$ számok a Gauss-prímek?

**Példák.** • $15 = 3 \cdot 5$, $5 = (2 + i)(2 - i)$, $13 = (3 + 2i)(3 - 2i)$ nem Gauss-prímek,
• $1 + i$, $4 + i$, 3 Gauss-prímek.

Valóban, legyen $z \mid 1 + i$, akkor $N(z) \mid N(1 + i) = 2$, innen $N(2) = 1$ és $z$ egység, vagy $N(z) = 2$, innen $z = 1 + i, 1 - i, -1 + i, -1 - i$, amelyek $1 + i$ asszociáltjai, tehát $1 + i$-nek nincs valódi osztója.

**Feladat.** ▼ Igazoljuk, hogy $4 + i$ és 3 Gauss-prímek.

A továbbiakban meghatározzuk a Gauss-prímeket. A megkülönböztetés érdekében a $\mathbb{Z}[i]$-beli prímeket mindig Gauss-prímeknek nevezzük, a prím és prímszám pedig mindig $\mathbb{Z}$-beli prímet jelent. Használni fogjuk a következő tulajdonságot.

**Tétel.** Ha $z$ egy Gauss-prím, akkor létezik egy és csak olyan $p$ prímszám, hogy $z \mid p$.

**Bizonyítás.** Ha $z \in \mathbb{Z}[i]$ Gauss-prím, akkor $N(z) > 1$ és legyen $N(z)$ felbontása prímek szorzatára $N(z) = q_1 q_2 \cdots q_k$. Így $z \mid z\overline{z} = N(z) = q_1 q_2 \cdots q_k$ és mivel $z$ Gauss-prím következik, hogy $z \mid q_i$ valamely $i$-re.

Egyértelműség: tegyük fel, hogy $z \mid p$ és $z \mid q$, ahol $p \neq q$ prímek. Akkor $(p, q) = 1$ miatt léteznek $u, v \in \mathbb{Z}$ úgy, hogy $pu + qv = 1$ és következik, hogy $z \mid 1$, ami ellentmondás. □

Az előbbi Tétel szerint a Gauss-prímek maghatározásához elegendő a $p \in \mathbb{Z}$ prímek lehetséges $\mathbb{Z}[i]$-beli felbontásait tekinteni.

**Tétel.** A $p = 4k - 1$ alakú prímek $\mathbb{Z}[i]$-ben is prímek, tehát Gauss-prímek.

**Bizonyítás.** Tegyük fel, hogy $p = 4k - 1$ prím, de nem Gauss-prím. Akkor $p$ felírható $p = zt$ alakban, ahol $z, t \in \mathbb{Z}[i]$ nem egységek. Innen $N(p) = N(z)N(t)$, $p^2 = N(z)N(t)$, ahol $N(z) > 1, N(t) > 1$. Következik, hogy $N(z) = N(t) = p$. Legyen $z = a + bi$, akkor így $N(z) = a^2 + b^2 = p = 4k - 1$, de ez ellentmondás, mert két négyzetszám összege nem lehet $4k - 1$ alakú. Valóban, ha $a, b$ közül mindkettő páros vagy páratlan, akkor $a^2 + b^2 \equiv 0 \pmod 4$, ha pedig $a, b$ közül az egyik páros, a másik páratlan, pl. $a = 2x, b = 2y + 1$, akkor $a^2 + b^2 = 4x^2 + 4y^2 + 4y + 1 \equiv 1 \pmod 4$. □

**Tétel.** A $p = 4k + 1$ alakú prímek felbonthatók két nem asszociált, egymással konjugált Gauss-prím szorzatára.

A bizonyításhoz szükségünk van a következő lemmára.

**Lemma.** Ha $p = 4k + 1$ alakú prím, akkor az $x^2 \equiv -1 \pmod{p}$ kongruenciának van megoldása.

**A lemma bizonyítása.** A Wilson-tétel szerint minden $p$ prímre $(p-1)! \equiv -1 \pmod{p}$. Ha $p = 4k + 1$ alakú, akkor

$$(p-1)! = (4k)! = 1 \cdot 2 \cdot 3 \cdots (2k)(2k+1)(2k+2) \cdots (4k) =$$

$$= 1 \cdot 2 \cdot 3 \cdots (2k)(p-2k)(p-2k+1)(p-2k+2) \cdots (p-1) \equiv$$

$$\equiv 1 \cdot 2 \cdot 3 \cdots (2k)(-1)^{2k}(2k)(2k-1)(p-2k-2) \cdots 1 = ((2k)!)^2 \pmod{p},$$

tehát $x = (2k)!$ megoldás. □

**A Tétel bizonyítása.** Tegyük fel, hogy $p = 4k + 1$ prím és $p$ Gauss-prím. Akkor a Lemma alapján van olyan $x_0 \in \mathbb{Z}$ szám, hogy $x_0^2 \equiv -1 \pmod{p}$, azaz $p \mid x_0^2 + 1 = (x_0 + i)(x_0 - i)$ és innen $p \mid x_0 + i$ vagy $p \mid x_0 - i$, azaz $\frac{x_0}{p} + \frac{1}{p}i \in \mathbb{Z}[i]$ vagy $\frac{x_0}{p} - \frac{1}{p}i \in \mathbb{Z}[i]$, de ez ellentmondás, mert $\frac{1}{p} \notin \mathbb{Z}$.

Tehát $p$ felírható $p = z_1 z_2 \cdots z_\ell$ alakban, ahol $z_1, z_2, ..., z_\ell \in \mathbb{Z}[i]$ Gauss-prímek és $\ell \geq 2$. Akkor $N(p) = N(z_1)N(z_2) \cdots N(z_\ell)$, $p^2 = N(z_1)N(z_2) \cdots N(z_\ell)$, ahol $N(z_i) > 1$ minden $i$-re. Következik, hogy $\ell = 2$ és $N(z_1) = N(z_2) = p$, tehát $p = z_1 z_2$, ahol $z_1, z_2 \in \mathbb{Z}[i]$ prímek.

Megmutatjuk, hogy $z_1$ és $z_2$ egymás konjugáltjai. Itt $N(z_1) = |z_1|^2 = p$, innen $|z_1| = \sqrt{p}$, hasonlóan $|z_2| = \sqrt{p}$. Legyen

$$z_1 = \sqrt{p}(\cos\theta_1 + i\sin\theta_1), \quad z_2 = \sqrt{p}(\cos\theta_2 + i\sin\theta_2), \quad \theta_1, \theta_2 \in [0, 2\pi).$$

Akkor

$$z_1 z_2 = p(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)),$$

de $z_1 z_2 = p \in \mathbb{R}$, innen $\cos(\theta_1 + \theta_2) = 1$, $\sin(\theta_1 + \theta_2) = 0$ és következik, hogy $\theta_1 + \theta_2 = 0$, $\theta_2 = -\theta_1$, azaz $z_2 = \overline{z_1}$.

$z_1$ és $z_2$ nem asszociáltak. Valóban, ha $z_1 = z_2 u$ lenne, ahol $u$ egység, akkor $z_1 = \overline{z_1} u$ és a $z_1 = a + bi$ jelöléssel:

ha $u = 1$, akkor $a + bi = a - bi$, innen $b = 0$, $p = z_1 z_2 = a^2$ nem lehet prím, ellentmondás,

ha $u = -1$, akkor $a + bi = -a + bi$, innen $a = 0$, $p = z_1 z_2 = ib(-ib) = b^2$ nem lehet prím, ellentmondás,

ha $u = \pm i$, akkor hasonlóan ellentmondásra jutunk. □

A fentieken kivül még léteznek az $2 = (1+i)(1-i)$ felbontásából származó $1+i$ és $1-i$ Gauss-prímek, amelyek egymás asszociáltjai, mert $1 - i = -i(1 + i)$.

**Tétel.** A Gauss-prímek tehát a következők:

a) $u(1 + i)$, ahol $u \in \{1, -1, i, -i\}$ egység,

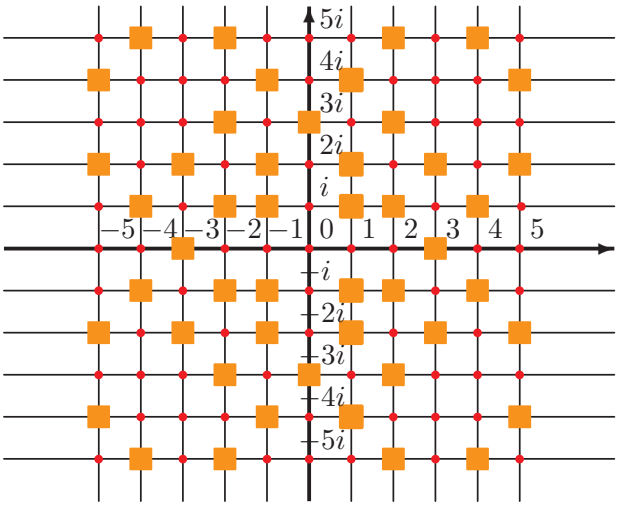
b) $up$, ahol $p = 4k - 1$ alakú prím ($p = 3, 7, 11, 19, 23, ...$) és $u$ egység,

c) $uz$, ahol $N(z) = 4k + 1$ alakú prím ($p = 5, 13, 17, 29, ...$) és $u$ egység. □

A $z = a + bi$, $|a|, |b| \leq 5$ Gauss-prímek a következők:

$-5-4i$, $-5-2i$, $-5+2i$, $-5+4i$, $-4-5i$, $-4-i$, $-4+i$, $-4+5i$, $-3-2i$, $-3$, $-3+2i$ $-2-5i$, $-2-3i$, $-2-i$, $-2+i$, $-2+3i$, $-2+5i$, $-1-4i$, $-1-2i$, $-1-i$, $-1+i$,$-1+2i$, $-1+4i$, $1-4i$, $1-2i$, $1-i$, $1+i$, $1+2i$, $1+4i$, $2-5i$, $2-3i$, $2-i$, $2+i$, $2+3i$, $2+5i$, $3-2i$, $3$, $3+2i$ $4-5i$, $4-i$, $4+i$, $4+5i$, $5-4i$, $5-2i$, $5+2i$, $5+4i$,

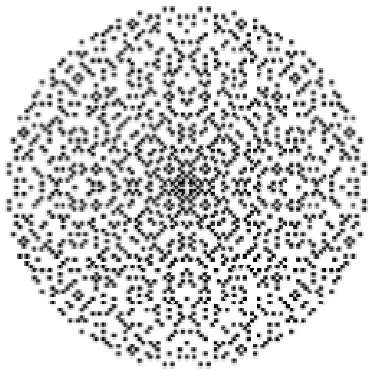
ezek láthatók az 5. ábrán.




**5. ábra.** Gauss-prímek

**Feladat.** ▼ Milyen szimmetriákat figyelhetünk meg az 5. ábrán?

A 6. ábrán kis fekete négyzetek jelzik azokat a Gauss-prímeket, amelyek normája $\leq 2500$ (abszolút értékük $\leq 50$).



**6. ábra.** Gauss-prímek

Foglaljuk össze, hogyan dönthető el egy $z \neq 0$ Gauss-egészről, hogy $z$ egység vagy Gauss-prím vagy Gauss-összetett? Erre ad választ a következő:

**Tétel.** Legyen $z = a + bi \in \mathbb{Z}[i], z \neq 0$.

1. eset. Ha $z = \pm 1, \pm i \;\Leftrightarrow\; N(z) = 1$, akkor $z$ egység.

2. eset. Ha $z = 1+i, 1-i, -1+i, -1-i \;\Leftrightarrow\; N(z) = 2$, akkor $z$ Gauss-prím.

3. eset. Ha $b = 0, |a| \geq 2$, tehát $z = a$ valós egész, $z \neq 0, \pm 1$, akkor

3.a) ha $z = a$ egy $4k-1$ alakú prím, akkor $z = a$ Gauss-prím,

3.b) ha $z = \pm 2$ vagy $z = \pm p$, ahol $p = 4k+1$ alakú prím, vagy $z$ összetett szám, akkor $z = a$ Gauss-összetett.

4. eset. Ha $b \neq 0$, tehát $z = a + bi$ nem valós szám és $N(z) = a^2 + b^2 \geq 3$, akkor

4.a) ha $N(z) = a^2 + b^2$ prímszám (ez csak $4k+1$ alakú lehet), akkor $z$ Gauss-prím,

4.b) ha $N(z)$ összetett szám, akkor $z$ Gauss-összetett.

**Feladatok.** ▼ 1. Gauss-prímek-e a következők: $-1-i$, $11i$, $2+7i$, $2-i$, $37$, $14+23i$, $-7+41i$.

▼ 2. Bontsuk fel Gauss-prímek szorzatára a következő számokat: $3+i$, $2+6i$, 10, 100, 200, 550, 600.

▼▼ 3. Mutassuk meg a Gauss-egészek és a Gauss-prímek alkalmazásával, hogy végtelen sok $4k+1$ alakú prímszám létezik.

Következményként kapjuk a következő tulajdonságot, amelynek állításában nem szerepelnek komplex számok.

**Tétel.** Minden $p = 4k+1$ alakú prím felírható két négyzetszám összegeként: $p = a^2+b^2$, ahol $a, b \in \mathbb{Z}$.

**Bizonyítás.** Ha $p = 4k+1$ alakú prím, akkor a Gauss-prímekre vonatkozó korábbi Tétel szerint $p = (a+ib)(a-ib) = a^2+b^2$. □

**Példák.** • $5 = 1^2+2^2$, $29 = 2^2+5^2$, $41 = 4^2+5^2$,

• a $3, 7, 11, 19$ prímek, ezek $p = 4k-1$ alakúak nem írhatók fel így, ugyanakkor pl. $20 = 2^2+4^2$, $45 = 3^2+6^2$.

Kérdés, hogy melyek azok a pozitív egészek, amelyek felírhatók két négyzetszám összegeként? Erre ad választ a következő tétel, amely szintén a Gauss-egészek segítségével igazolható, lásd pl. [FGy], 304. old. Itt csak annyit jegyzünk meg, hogy ha $n = x^2+y^2$, akkor $n = (x+iy)(x-iy)$ és innen már „látható" a Gauss-egészek szerepe.

★ **Tétel.** Az $n \in \mathbb{N}$ szám akkor és csak akkor írható fel $n = x^2+y^2$ alakban, ahol $x, y \in \mathbb{Z}$, ha $n$ kanonikus alakjában minden $4k-1$ alakú prím kitevője páros szám. □

A számelmélet nevezetes tétele a következő:

**Tétel.** (Lagrange) Minden $n$ pozitív egész szám felírható négy négyzetszám összegeként: $n = a^2+b^2+c^2+d^2$, ahol $a, b, c, d \in \mathbb{Z}$. □★

### 2.3. $\mathbb{Z}[\sqrt{2}]$ aritmetikája

Legyen $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Z}\}$, amely integritástartomány a valós számok összeadásával és szorzásával (részgyűrűje $(\mathbb{R}, +, \cdot)$-nak).

Ennek megfelelően értelme van az oszthatóságnak, az irreducibilis elem, a prímelem, az lnko, az lkkt fogalmainak.

Ha $z = a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ legyen $N(z) = |a^2-2b^2|$ a $z$ normája.

**Megjegyzések.** 1. $N(z)$ nemnegatív egész szám minden $z \in \mathbb{Z}[\sqrt{2}]$-re.

2. $N(z) = |(a+b\sqrt{2})(a-b\sqrt{2})|$.

3. Nem lenne célszerű az $|z|$ vagy az $|z|^2$ értékeket választani normának, mert ezek általában nem természetes számok, itt $|a+b\sqrt{2}|^2 = a^2+b^2+2ab\sqrt{2}$.

Igazoljuk, hogy

**Tétel.** $\mathbb{Z}[\sqrt{2}]$ euklideszi gyűrű a fenti $N(z) = |a^2-2b^2|$, $z = a+b\sqrt{2}$ normára nézve. □

Általánosabban, tekintsük a $\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} : a, b \in \mathbb{Z}\}$ integritástartományt, ahol $d \in \mathbb{Z}$, $d \neq 0, 1$ négyzetmentes szám, lásd 1.1. szakasz. Ha $z = a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ legyen $N(z) = |a^2-db^2|$.

**Tétel.** (A norma tulajdonságai) Ha $d \neq 0, 1$ tetszőleges rögzített négyzetmentes szám és $z, z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$, akkor

1. $N(z) = 0$ akkor és csak akkor, ha $z = 0$,
2. $N(z_1z_2) = N(z_1)N(z_2)$,
3. $N(z) = 1$ akkor és csak akkor, ha $z$ egység.

**Bizonyítás.** 1. Ha $z=0$, akkor $N(z)=0$ azonnali. Fordítva: $N(z)=|(a-b\sqrt{d})(a+b\sqrt{d})|=0 \Rightarrow a-b\sqrt{d}=0$ vagy $a+b\sqrt{d}=0$, innen $a=b\sqrt{d}$ vagy $a=-b\sqrt{d}$. Ha $b\neq 0$, akkor $\pm b\sqrt{d}$ irracionális szám és kapjuk, hogy $a$ irracionális, ami ellentmondás. Tehát $b=0$, ahonnan $a=\pm b\sqrt{d}=0$ és $z=0$ következik.

2. Legyen $z_1=a_1+b_1\sqrt{d}$, $z_2=a_2+b_2\sqrt{d}$. Akkor

$$z_1z_2=(a_1a_2+b_1b_2d)+(a_1b_2+a_2b_1)\sqrt{d},$$

innen

$$N(z_1z_2)=N((a_1a_2+b_1b_2d)+(a_1b_2+a_2b_1)\sqrt{d})=|(a_1a_2+b_1b_2d)^2-d(a_1b_2+a_2b_1)^2|=$$

$$=|a_1^2a_2^2+b_1^2b_2^2d^2-a_1^2b_2^2d-a_2^2b_1^2d|=|(a_1^2-db_1^2)(a_2^2-db_2^2)|=N(z_1)N(z_2).$$

3. Ha $N(z)=1$, akkor a $z=a+b\sqrt{d}$, $\overline{z}=a-b\sqrt{d}$ jelöléssel $N(z)=|z\overline{z}|=1$, innen $z(\pm\overline{z})=1$, tehát létezik $z$ inverze, ami $\pm\overline{z}\in\mathbb{Z}[\sqrt{d}]$.

Ha $z$ egység, akkor létezik $z^{-1}\in\mathbb{Z}[\sqrt{d}]$ úgy, hogy $zz^{-1}=1$, innen 2. alapján $N(z)N(z^{-1})=N(zz^{-1})=N(1)=1$, tehát $N(z)\mid 1$, $N(z)=1$. □

**Feladat.** ▼ Igazoljuk, hogy

a) $z\mid N(z)$,

b) ha $z\mid w$, akkor $N(z)\mid N(w)$.

A norma definíciója kiterjeszthető az $x+y\sqrt{d}$ alakú számokra, ahol $x$ és $y$ racionális számok. Ha $x,y\in\mathbb{Q}$ és $z=x+y\sqrt{d}$, legyen $N(z)=|x^2-dy^2|$.

**Tétel.** Ha $z_1=x_1+y_1\sqrt{d}$, $z_2=x_2+y_2\sqrt{d}$, ahol $x_1,y_1,x_2,y_2\in\mathbb{Q}$, akkor

$$N(z_1z_2)=N(z_1)N(z_2),$$

$$N(\frac{z_1}{z_2})=\frac{N(z_1)}{N(z_2)},\quad z_2\neq 0.$$

**Bizonyítás.** Az előző Tétel 2. pontjának bizonyítása érvényben marad racionális együtthatókra is, innen következik az első összefüggés.

Továbbá legyen $\frac{z_1}{z_2}=w$, ahol $w=x+y\sqrt{d}$, $x,y\in\mathbb{Q}$ alakú (▼ Írjuk ki részletesen!), innen $z_1=z_2w$ és az első összefüggés alapján $N(z_1)=N(z_2)N(w)$ és $N(\frac{z_1}{z_2})=N(w)=\frac{N(z_1)}{N(z_2)}$. □

**Tétel.** Ha $d=-2,-1,2,3$, akkor $Z[\sqrt{d}]$ euklideszi gyűrű az $N(z)=|a^2-db^2|$, $z=a+b\sqrt{d}$ normára nézve.

**Bizonyítás.** A Gauss-egészekre vonatkozó bizonyításhoz hasonlóan, ha $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$, $\beta\neq 0$, osszuk el $\alpha$-t $\beta$-val és kapjuk, hogy $\alpha/\beta=x+y\sqrt{d}$, ahol $x,y$ racionális számok. A legközelebbi $x_0$ és $y_0$ egészeket választva $|x-x_0|\leq 1/2$, $|y-y_0|\leq 1/2$.

Legyen $q=x_0+y_0\sqrt{d}$ és $r=\alpha-\beta q$. Ha $r\neq 0$, akkor $r=\beta(\frac{\alpha}{\beta}-q)$ alapján és használva az előző Tételt: $N(r)=N(\beta)N(\frac{\alpha}{\beta}-q)$. Itt $\frac{\alpha}{\beta}-q=(x-x_0)+(y-y_0)\sqrt{d}$ és $N(\frac{\alpha}{\beta}-q)=|(x-x_0)^2-d(y-y_0)^2|\leq(x-x_0)^2+|d|(y-y_0)^2\leq\frac{1}{4}+|d|\frac{1}{4}\leq\frac{1}{4}+\frac{3}{4}=1$. Az egyenlőség csak $d=3$ és $|x-x_0|=|y-y_0|=\frac{1}{2}$ esetén állhatna fenn, de valójában ekkor is szigorú az egyenlőtlenség, mert ekkor $|(x-x_0)^2-d(y-y_0)^2|=|\frac{1}{4}-3\cdot\frac{1}{4}|=|-\frac{1}{2}|=\frac{1}{2}<1$.

Kapjuk, hogy $N(r)<N(\beta)$. □

Ha $d=-1$, akkor visszakapjuk a Gauss-egészekre vonatkozó tulajdonságokat. Ha $d=2$, akkor kapjuk, hogy $\mathbb{Z}[\sqrt{2}]$ euklideszi gyűrű, lásd korábbi Tétel.

**Megjegyzések.** Az utóbbi Tétel szerint $\mathbb{Z}[i\sqrt{2}]$ és $\mathbb{Z}[\sqrt{3}]$ is euklideszi gyűrűk, ezekben is a szokásoshoz hasonló számelmélet építhető ki. Ugyanakkor $\mathbb{Z}[i\sqrt{3}]$ és $\mathbb{Z}[i\sqrt{5}]$ nem euklideszi gyűrűk (itt $d=-3$, ill. $d=-5$), mert nem is Gauss-gyűrűk, lásd 1.5. szakasz.

★ A Gauss-egészekhez képest különbség az, hogy $\mathbb{Z}[\sqrt{2}]$ elemei a valós tengelyen helyezkednek el, mégpedig sűrűn. Ez azt jelenti, hogy

**Tétel.** Minden $x$ valós szám tetszőlegesen kicsi környezetében van $\mathbb{Z}[\sqrt{2}]$-beli szám (sőt végtelen sok).

**Bizonyítás.** Legyen $x \in \mathbb{R}$ rögzített és tekintsük a következő sorozatot:

$$a_n = \left[\frac{x}{(\sqrt{2}-1)^n}\right](\sqrt{2}-1)^n, \quad n \geq 1$$

ahol [ ] az egészrészt jelöli. Akkor $a_n \in \mathbb{Z}[\sqrt{2}]$ minden $n \geq 1$-re és $\theta_n$-nel jelölve az $\frac{x}{(\sqrt{2}-1)^n}$ törtrészét kapjuk, hogy

$$a_n = \left(\frac{x}{(\sqrt{2}-1)^n} - \theta_n\right)(\sqrt{2}-1)^n = x - \theta_n(\sqrt{2}-1)^n.$$

Itt $0 \leq \theta_n < 1$ minden $n$-re és $0 < \sqrt{2}-1$, így $\lim_{n\to\infty} a_n = x$. □

**Tétel.** $\mathbb{Z}[\sqrt{2}]$-ben végtelen sok egység van.

**Bizonyítás.** Korábbi Tétel szerint $z = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ akkor és csak akkor egység, ha $N(z) = |x^2 - 2y^2| = 1$, azaz $x^2 - 2y^2 = 1$ vagy $x^2 - 2y^2 = -1$.

Legyen $z_1 = 3 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Akkor $N(z_1) = |9 - 8| = 1$, tehát $z_1$ egység. A norma tulajdonsága szerint $N(z_1^n) = (N(z_1))^n = 1^n = 1$ minden $n \geq 1$-re, tehát $z_n = z_1^n$ egység minden $n$-re. Mivel $z_1 < z_2 < ... < z_n < z_{n+1} < ...$ következik, hogy így végtelen sok egységet kaptunk. □

**Megjegyzések.** Igazolható, hogy $\mathbb{Z}[\sqrt{2}]$-ben minden egység $\pm z_0^n$, $n \in \mathbb{N}$ alakú, ahol $z_0 = 1 + \sqrt{2}$. Speciálisan $z_1 = 3 + 2\sqrt{2} = z_0^2$.

Az $x^2 - 2y^2 = 1$ és $x^2 - 2y^2 = -1$ diofántoszi egyenleteket Pell-egyenleteknek nevezzük.

Igazolható, hogy a $\mathbb{Z}[\sqrt{2}]$-beli prímek a következők, az asszociáltaktól eltekintve:

**Tétel.** A $8k \pm 3$ alakú prímek $\mathbb{Z}[\sqrt{2}]$-ben is prímek, a $8k \pm 1$ alakú prímek pedig két $\mathbb{Z}[\sqrt{2}]$-beli prím szorzatára bomlanak és ezeken kívül $\mathbb{Z}[\sqrt{2}]$-ben prím még a $\sqrt{2}$. □

**Példák.** • $z = 5$ és $z = 11$ prímek $\mathbb{Z}[\sqrt{2}]$-ben,

• $3 + \sqrt{2}$ és $3 - \sqrt{2}$ prímek $\mathbb{Z}[\sqrt{2}]$-ben, mert $(3+\sqrt{2})(3-\sqrt{2}) = 7$ egy $8k-1$ alakú prím.

★

### 2.4. Az Eisenstein-egészek aritmetikája

Legyen $\varrho = \frac{-1+i\sqrt{3}}{2} = \cos(2\pi/3) + i\sin(2\pi/3)$ harmadrendű egységgyök, amelyre $\varrho^3 = 1$ és $\varrho^2 + \varrho + 1 = 0$.

Jelölés: $\mathbb{Z}[\varrho] = \{a + b\varrho : a, b \in \mathbb{Z}\}$, amely integritástartomány a komplex számok összeadására és szorzására nézve. ▼ Igazoljuk!

Ezt az Eisenstein-egészek gyűrűjének nevezzük (másképp: Eisenstein-Jacobi-egészek vagy Euler-egészek). A továbbiakban az E-egész elnevezést használjuk. Az E-egészek egy paralelogramma-rácsot (pontosabban rombusz-rácsot) alkotnak a komplex számsíkban, lásd a 7. ábrát.

**Definíció.** Ha $\alpha = a + b\varrho = (a - \frac{b}{2}) + \frac{b\sqrt{3}}{2}i$ egy E-egész, akkor ennek normája az abszolút érték négyzete: $N(\alpha) = |\alpha|^2 = (a - \frac{b}{2})^2 + \frac{3b^2}{4} = a^2 + b^2 - ab$, amely nemnegatív egész szám.

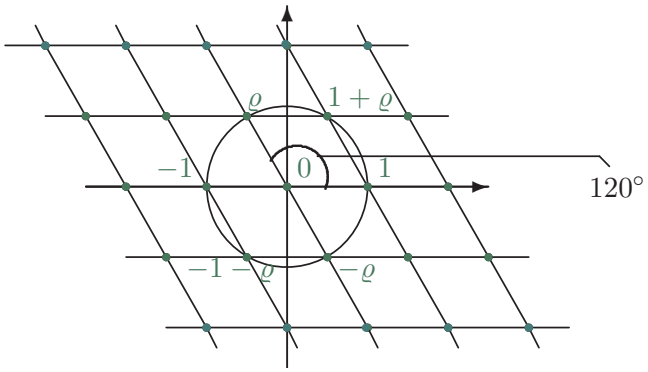
**Tétel.** Az E-egészek euklideszi gyűrűt alkotnak erre a normára nézve.

**Bizonyítás.** A Gauss-egészekre vonatkozó bizonyításhoz hasonlóan. Kérdés, hogy $\forall \alpha, \beta \in \mathbb{Z}[\varrho], \beta \neq 0: \ \exists\, q, r \in \mathbb{Z}[\varrho] : \alpha = q\beta + r$, ahol $r = 0$ vagy $N(r) < N(\beta), r \neq 0$ ?

Ha a $q$-t már megválasztottuk, akkor $r = \alpha - q\beta$ lesz. Ha $r = 0$, akkor nincs mit bizonyítani, ha pedig $r \neq 0$, akkor szükséges, hogy

$$N(r) = N(\alpha - q\beta) = |\alpha - q\beta|^2 < |\beta|^2, \quad \text{innen} \quad \left|\frac{\alpha}{\beta} - q\right|^2 < 1, \quad \text{azaz} \quad \left|\frac{\alpha}{\beta} - q\right| < 1.$$

Az $\alpha/\beta$ komplex szám most vagy egy egységoldalú rombusz belsejébe vagy annak oldalára esik és mindig van olyan csúcs, amelytől $\alpha/\beta$ távolsága kisebb mint 1, tehát teljesül a fenti feltétel. □




**7. ábra** E-egészek

**Tétel.** Legyenek $\alpha, \beta \in \mathbb{Z}[\varrho]$.
1. $N(\alpha) = 0$ akkor és csak akkor, ha $\alpha = 0$,
2. $N(\alpha) = 1$ akkor és csak akkor, ha $\alpha$ egység,
3. $N(\alpha\beta) = N(\alpha)N(\beta)$,
4. $\alpha \mid N(\alpha)$,
5. ha $\alpha \mid w$, akkor $N(\alpha) \mid N(\alpha)$,
6. minden $\alpha \neq 0$ E-számnak véges sok osztója van.

**Bizonyítás.** A Gauss-egészekre vonatkozó megfelelő Tétel bizonyításához hasonlóan. ▼ Végezzük el! □

**Tétel.** Az E-egészek gyűrűjében az egységek a következők: $1, -1, \varrho, -\varrho, 1 + \varrho, -1 - \varrho$, ezek éppen a hatodrendű egységgyökök (lásd 7. ábra).

**Bizonyítás.** Az előző Tétel szerint $\alpha = a + b\varrho$ akkor és csak akkor egység, ha $N(\alpha) = 1$, azaz $|\alpha| = 1$, tehát $\alpha$ távolsága az origótól 1, ez pedig éppen a megadott számokra teljesül.

Másképp: $N(\alpha) = 1$ akkor és csak akkor, ha $(a - \frac{b}{2})^2 + \frac{3b^2}{4} = 1$. Ha itt $|b| \geq 2$, akkor $\frac{3b^2}{4} \geq 3$ és nem kapunk megoldást. Tehát $b \in \{-1, 0, 1\}$ kell legyen. Ha $b = -1$, akkor $(a + \frac{1}{2})^2 + \frac{3}{4} = 1$, $|a + \frac{1}{2}| = \frac{1}{2}$, innen $a = 0$ vagy $a = -1$. Hasonlóan a $b = 0$ és $b = -1$ esetekben. □

Az E-egészek $\mathbb{Z}[\varrho]$ euklideszi gyűrűjében az irreducibilis elemek azonosak a prím elemekkel, ezeket E-prímeknek nevezzük. A Gauss-prímekre vonatkozó megfelelő tulajdonságokhoz hasonlóan igazolhatók a következők, a bizonyításokat csak vázoljuk. ▼ Egészítsük ki ezeket!

**Tétel.** Ha $\alpha$ egy E-prím, akkor létezik egy és csak olyan $p$ prímszám, hogy $\alpha \mid p$.

**Bizonyítás.** Ha $\alpha \in \mathbb{Z}[\varrho]$ E-prím, akkor $N(\alpha) > 1$ és legyen $N(\alpha)$ felbontása prímek szorzatára $N(\alpha) = q_1 q_2 \cdots q_k$. Így $\alpha \mid N(\alpha) = q_1 q_2 \cdots q_k$ és mivel $\alpha$ E-prím következik, hogy $\alpha \mid q_i$ valamely $i$-re.

▼ Igazoljuk az egyértelműséget! □

**Tétel.** A $p = 3k-1$ alakú prímek $\mathbb{Z}[\varrho]$-ban is prímek, tehát E-prímek.

**Bizonyítás.** Tegyük fel, hogy $p = 3k-1$ prím, de nem E-prím. Akkor $p$ felírható $p = \alpha\beta$ alakban, ahol $\alpha, \beta \in \mathbb{Z}[\varrho]$ nem egységek. Innen $p^2 = N(\alpha)N(\beta)$, $N(\alpha) = N(\beta) = p$. Legyen $\alpha = a+b\varrho$, akkor így $4N(\alpha) = (2a-2)^2+3b^2 = p = 3k-1$ alakú, de ez ellentmondás, mert $(2a-2)^2 + 3b^2 \equiv 0$ vagy $1 \pmod 3$. □

**Tétel.** A $p = 3k+1$ alakú prímek felbonthatók két nem asszociált, egymással konjugált E-prím szorzatára.

★ **Bizonyítás.** Használjuk a következő tulajdonságot:

Ha $p = 3k+1$ alakú prím, akkor az $x^2 \equiv -3 \pmod p$ kongruenciának van megoldása, lásd később a négyzetes maradékokra vonatkozó szakaszt.

Tegyük fel, hogy $p = 3k+1$ prím és $p$ E-prím. Akkor a Lemma alapján van olyan $x_0 \in \mathbb{Z}$ szám, hogy $x_0^2 \equiv -3 \pmod p$, azaz $p \mid x_0^2+3 = (x_0+i\sqrt{3})(x_0-i\sqrt{3}) = (x_0+1+2\varrho)(x_0-1-2\varrho)$ és innen $p \mid (x_0+1+2\varrho)$ vagy $p \mid (x_0-1-2\varrho)$, de ez ellentmondás.

Tehát $p$ felírható $p = \alpha_1\alpha_2\cdots z_\ell$ alakban, ahol $\ell = 2$ kell legyen és így $p = \alpha_1\alpha_2$, ahol $\alpha_1, \alpha_2$ E-prímek. □★

A fentieken kivül még létezik az $3 = (-1)(i\sqrt{3})^2$ felbontásából származó $i\sqrt{3} = 1+2\varrho$ E-prím (és ennek asszociáltjai).

**Tétel.** Az E-prímek a következők:

a) $u(1+2\varrho)$, ahol $u \in \{1, -1, \varrho, -\varrho, 1+\varrho, -1-\varrho, \}$ egység,

b) $up$, ahol $p = 3k-1$ alakú prím ($p = 2, 5, 11, 17, 23, 29, ...$) és $u$ egység,

c) $uz$, ahol $N(z) = 3k+1$ alakú prím ($p = 7, 13, 19, 31, ...$) és $u$ egység. □

**Feladatok.** ▼ 1. Igazoljuk, hogy ha $\alpha \in \mathbb{Z}[\varrho]$ és $N(\alpha)$ prím, akkor $\alpha$ prím. Igaz-e fordítva?

▼ 2. Melyek az $i\sqrt{3} = 1+2\varrho$ asszociáltjai?

▼ 3. E-prímek-e a következők: $\alpha_1 = 2+3\varrho$, $\alpha_2 = 3+\varrho$, $\alpha_3 = 5+8\varrho$.

Az E-egészek alkalmazásával igazolható, hogy az $x^3+y^3 = z^3$ egyenletnek nem léteznek $x, y, z \in \mathbb{Z} \setminus \{0\}$ megoldásai. Ez a Fermat-Wiles tétel speciális esete. Az az erősebb állítás is igaz, hogy az adott egyenletnek nincsenek $x, y, z \in \mathbb{Z}[\varrho] \setminus \{0\}$ megoldásai, lásd [FGy], 327. old.

Itt csak annyit jegyzünk meg, hogy ha $x^3+y^3 = z^3$, akkor $x^3 = z^3-y^3 = (z-y)(z-y\varrho)(z-y\varrho^2) = (z-y)(z-y\varrho)(z+y+y\varrho)$, ahonnan már látható, hogyan is jelennek itt meg az $E$-egészek.

### 2.5. Megoldások

2.1. Euklideszi gyűrűk és tulajdonságaik

▼ Hol helyezhetők el az 1. ábrán a $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ és a $(\mathbb{Z}[i\sqrt{3}], +, \cdot)$ gyűrűk?

**Válasz.** Ezek nem Gauss-gyűrűk.

▼ Alkalmazzuk az euklideszi algorimust az $a = 33855, b = 18870$ számokra és határozzunk meg olyan $x, y \in \mathbb{Z}$ számokat, amelyekre $33855x+18870y = d$, ahol $d = (33855, 18870)$.

**Válasz.** $(a, b) = 555$.

▼ Alkalmazzuk az euklideszi algorimust az $f = 3X^3 - X^2 - 3X + 1, g = 2X^3 - 2X^2 - 3X + 3 \in \mathbb{Q}[X]$ polinomokra és határozzunk meg olyan $u, v \in \mathbb{Q}[X]$ polinomokat, amelyekre $fu + gv = d$, ahol $d = (f, g)$.

**Válasz.** $(f, g) = X - 1$.

2.2. A Gauss-egészek aritmetikája

▼ Igaz-e, hogy ha $N(z) \mid N(w)$, akkor $z \mid w$?

**Megoldás.** Nem igaz, pl. $z = 1 + 2i, w = -1 + 2i$-re $N(z) = N(w) = 1 + 4 = 5$, de $z \nmid w$, mert $\frac{-1+2i}{1+2i} = \frac{3+4i}{5} \notin \mathbb{Z}[i]$. Másképp, ha $w = zt$ lenne, akkor $N(w) = N(z)N(t)$, innen $N(t) = 1$, tehát $t$ egység. Akkor $w = zt$, ahol $t = \pm 1, \pm i$, de ez nem igaz.

▼ Igazoljuk, hogy ha $z_1$ és $z_2$ asszociáltak, akkor $N(z_1) = N(z_2)$. Igaz-e ez fordítva?

**Megoldás.** Fordítva nem igaz, pl. $3 + 2i$ és $-3 + 2i$ nem asszociáltak, de $N(3 + 2i) = N(-3 + 2i) = 9 + 4 = 13$.

▼ Vizsgáljuk meg, hogy lehet-e $\overline{z}$ (komplex konjugált) osztója $z$-nek.

**Megoldás.** Ha $z = a + bi, \overline{z} = a - bi$ és ha $z \mid \overline{z}$, akkor $z = \overline{z}t$, $N(z) = N(\overline{z})N(t)$, innen $N(t) = 1$, tehát $t = e$ egység és $z = \overline{z}e$.

Ha $e = 1$, akkor $z = \overline{z}$, innen $z \in \mathbb{Z}$. Ha $e = -1$, akkor $z = -\overline{z}$, $a + ib = -a + ib$, innen $a = 0$ és $z = bi$, ahol $b \in \mathbb{Z}$. Hasonlóan, $e = \pm i$-re kapjuk, hogy $z = a + ai$, ill. $z = a - ai$, ahol $a \in \mathbb{Z}$.

▼ a) Osztója-e $3 + 5i$-nek $4 + i$, ill. $4 - i$ ? b) Határozzuk meg $3 + 5i$ összes osztóját.

**Megoldás.** a) $\frac{3+5i}{4+i} = \frac{(3+5i)(4-i)}{17} = 1 + i$, ezért $4 + i \mid 3 + 5i$. $\frac{3+5i}{4-i} = \frac{(3+5i)(4+i)}{17} = \frac{7+23i}{17}$, tehát $4 - i \nmid 3 + 5i$.

b) Ha $z \mid w = 3 + 5i$, akkor $N(z) \mid N(w) = 9 + 25 = 34$. Itt 34 pozitív osztói $1, 2, 17, 34$. Ha $N(z) = 1$, akkor $z$ egység: $z = \pm 1, \pm i$. Ha $N(z) = 2$, akkor $z = z_1 = 1 + i$ vagy asszociáltjai: $-z_1 = -1 - i, iz_1 = -1 + i, -iz_1 = 1 - i$. Ha $N(z) = 17$, akkor $z = z_2 = 4 + i$ vagy ennek asszociáltjai: $-z_2 = -4 - i, iz_2 = -1 + 4i, -iz_2 = -1 - 4i$, továbbá $z = z_3 = 1 + 4i$ vagy ennek asszociáltjai: $-z_3 = -1 - 4i, iz_3 = -4 + i, -iz_3 = 4 - i$. Ha $N(z) = 34$, akkor $z = w = 3 + 5i$ vagy ennek asszociáltjai: $-w = -3 - 5i, iw = -5 + 3i, -iw = 5 - 3i$, továbbá $z = z_4 = 5 + 3i$ vagy ennek asszociáltjai: $-z_4 = -5 - 3i, iz_4 = -3 + 5i, -iz_4 = 3 - 5i$. Ellenőrízhető - lásd a) pont - hogy ezek közül csak $1, z_1 = 1 + i, z_2 = 4 + i, w = 3 + 5i$ és ezek asszociáltjai osztók.

▼ Igazoljuk, hogy $4 + i$ és 3 Gauss-prímek.

**Megoldás.** Ha $z \mid 4 + i$, akkor $N(z) \mid N(4 + i) = 17$. Innen $N(z) = 1$ és $z$ egység, vagy $N(z) = 17$, innen $z = 4 + i$ és asszociáltjai vagy $z = 1 + 4i$ és asszociáltjai, de ellenőrízhető, hogy $1 + 4i \nmid 4 + i$. Tehát $4 + i$-nek nincs valódi osztója.

Ha $z = a + bi \mid 3$, akkor $N(z) \mid N(3) = 9$. Innen $N(z) = 1$ és $z$ egység, vagy $N(z) = a^2 + b^2 = 3$, ennek nincs megoldása, vagy $N(z) = 9$, innen $z = 3$ és asszociáltjai, tehát 3-nak nincs valódi osztója.

▼ Milyen szimmetriákat figyelhetünk meg az 5. ábrán?

**Megoldás.** Ha $z = a + bi$ prím, $b \neq 0$, akkor $\overline{a + bi} = a - bi$, $-a + bi$ és $-a - bi$ is prímek, mert mindegyik normája $a^2 + b^2 = N(z)$, tehát a Gauss-prímek a komplex számsíkban a tengelyekre nézve és az origóra nézve szimmetrikusan helyezkednek el.

▼ Bontsuk fel Gauss-prímek szorzatára a következő számokat: $3 + i$, $2 + 6i$, 10, 100, 200, 550, 600.

**Megoldás.** $(3+i)(3-i) = 9+1 = 10$ összetett, ezért $3+i$ nem Gauss-prím. A felbontás:

$3+i=(2-i)(1-i)$, ahol $2-i$ Gauss-prím, mert $(2-i)(2+i)=4+1=5$ prím és $1-i$ is Gauss-prím.

$2+6i=2(1+3i)=-(1+i)(1-i)(1-2i)(1-i)=-(1+i)^2(1-i)(1-2i)$, ahol $(1-2i)(1+2i)=1+4=5$ prím, ezért $1-2i$ Gauss-prím, tehát a felbontás: $2+6i=-(1+i)^2(1-i)(1-2i)$.

▼▼ Mutassuk meg a Gauss-egészek és a Gauss-prímek alkalmazásával, hogy végtelen sok $4k+1$ alakú prímszám létezik.

**Megoldás.** Tegyük fel, hogy véges sok $4k+1$ alakú prím van: $p_1, p_2, ..., p_n$. Legyen $x=(2p_1p_2\cdots p_n)^2+1$. Akkor $x$-nek létezik $q$ prímosztója, amely biztosan páratlan.

Tegyük fel, hogy $q=4k-1$ alakú, akkor következik, hogy $q$ Gauss-prím. Legyen $a=2p_1p_2\cdots p_n$. Így $q \mid x=a^2+1=(1+ia)(1-ia)$ és innen $q \mid 1+ia$ vagy $q \mid 1-ia$. Kapjuk, hogy $\frac{1}{q}+\frac{a}{q}i \in \mathbb{Z}[i]$ vagy $\frac{1}{q}-\frac{a}{q}i \in \mathbb{Z}[i]$, ami ellentmondás.

Tehát $q=4k+1$ alakú, azaz $q=p_i$ valamely $i$-re, innen $q \mid 1$, ami ismét ellentmondás.

2.4. Az Eisenstein-egészek aritmetikája

▼ Igazoljuk, hogy ha $\alpha \in \mathbb{Z}[\varrho]$ és $N(\alpha)$ prím, akkor $\alpha$ prím. Igaz-e fordítva?

**Megoldás.** Ha $N(\alpha)=p$ prím és $\alpha=\alpha_1\alpha_2$, akkor $p=N(\alpha)=N(\alpha_1)N(\alpha_2)$, innen $N(\alpha_1)=1$ vagy $N(\alpha_2)=1$, tehát $\alpha_1$ vagy $\alpha_2$ egység és $\alpha$ E-prím.

Fordítva nem igaz, mert pl. 5 E-prím, de $N(5)=25$ nem prím.

▼ E-prímek-e a következők: $\alpha_1=2+3\varrho$, $\alpha_2=3+\varrho$, $\alpha_3=5+8\varrho$.

**Megoldás.** $N(\alpha_1)=4-6+9=7$ prím, ezért $\alpha$ E-prím. $N(\alpha_3)=25-40+64=49$ nem prím, ezért $\alpha$ E-prím.

**★ 2.6. További feladatok**

▼▼ 1. Legyen $d \geq 3$ egy páratlan négyzetmentes szám. Igazoljuk, hogy $\mathbb{Z}[i\sqrt{d}]$ nem Gauss-gyűrű.

**Megoldás.** $(1+i\sqrt{d})(1-i\sqrt{d})=1+d$ páros szám, ezért $2 \mid (1+i\sqrt{d})(1-i\sqrt{d})$, de $2 \nmid (1+i\sqrt{d})$ és $2 \nmid (1-i\sqrt{d})$. Következik, hogy $2 \in \mathbb{Z}[i\sqrt{d}]$ nem prímelem. Igazoljuk, hogy 2 irreducibilis. Valóban, legyen $2=(a+bi\sqrt{d})(x+yi\sqrt{d})$, akkor normára térve $4=(a^2+db^2)(x^2+dy^2)$. Ha itt $a^2+db^2=1$, akkor $b=0$ és $a=\pm 1$, tehát $a+bi\sqrt{d}=\pm 1$ egység. Ha $a^2+db^2=2$, akkor nincs $a,b \in \mathbb{Z}$ megoldás. Ha itt $a^2+db^2=4$, akkor $x^2+dy^2=1$, innen $x+yi\sqrt{d}=\pm 1$ egység.

▼▼ 2. Igazoljuk, hogy $\mathbb{Z}[i\sqrt{6}]$ nem Gauss-gyűrű.

**Megoldás.** Mutassuk meg, hogy 6-nak $6=2\cdot 3=i\sqrt{6}(-i\sqrt{6})$ két, irreducibilis számokra való felbontása.

▼▼ 3. Igazoljuk, hogy $\mathbb{Z}[\sqrt{26}]$ nem Gauss-gyűrű.

**Megoldás.** Mutassuk meg, hogy 26-nak $26=2\cdot 13=\sqrt{26}\sqrt{26}$ két, irreducibilis számokra való felbontása. ★

## 3. Az egész számok számelmélete

A továbbiakban az egész számok számelméletével foglalkozunk. A 3.1. és 3.2. szakaszokban összefoglaljuk az egész számok oszthatóságára és kongruenciájára vonatkozó fogalmak és tulajdonságok közül azokat, amelyek csak az egész számokra érvényesek, illetve amelyeket nem érintettünk az első két fejezetben.

### 3.1. Oszthatóság, kongruenciák

Az oszthatósági feladatok megoldása során gyakran alkalmazzuk a következő tulajdonságokat.

**Tétel.** Legyenek $a, b \in \mathbb{Z}$ és $n \in \mathbb{N}^*$. Akkor
i) $a - b \mid a^n - b^n$,
ii) ha $n$ páratlan, akkor $a + b \mid a^n + b^n$,
iii) ha $n$ páros, akkor $a + b \mid a^n - b^n$.

**Bizonyítás.** Azonnali az $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$,
$a^{2k+1} + b^{2k+1} = (a + b)(a^{2k} - a^{2k-1}b + ... - ab^{2k-1} + b^{2k})$ és
$a^{2k} - b^{2k} = (a + b)(a^{2k-1} - a^{2k-2}b + ... + ab^{2k-2} - b^{2k-1})$ azonosságok alapján. □

**Tétel.** (A maradékos osztás tétele $\mathbb{Z}$-ben) Ha $a, b \in \mathbb{Z}, a \neq 0$, akkor léteznek az egyértelműen meghatározott $q \in \mathbb{Z}$ és $r \in \mathbb{Z}$ számok úgy, hogy $b = qa + r$, ahol $0 \leq r < |a|$.

**Tétel.** Legyenek $a, b, m \in \mathbb{Z}, m \geq 1$. Az $a \equiv b \pmod m$ kongruencia akkor és csak akkor teljesül ha $a$ és $b$ $m$-mel osztva ugyanazt a maradékot adja.

**Bizonyítás.** A definíció alapján $a \equiv b \pmod m \Leftrightarrow m \mid a - b$. Legyen $a = mq + r, b = mq' + r'$, ahol $0 \leq r < m, 0 \leq r' < m$. Ha $a \equiv b \pmod m$, akkor $m|a-b = m(q-q') + (r-r')$ és így $m|r - r'$. De $0 \leq |r - r'| < m$ és következik, hogy $r = r'$.
Ha $r = r'$, akkor azonnali, hogy $m|a - b$, azaz $a \equiv b \pmod m$. □

A kongruenciák műveleti tulajdonságainak alkalmazásaként tekintsük a következő példákat.

**Példák.** • 1. Igazoljuk, hogy $641 \mid F_5 = 2^{2^5} + 1$.
Valóban, $641 = 640 + 1 = 5 \cdot 2^7 + 1$, így $5 \cdot 2^7 \equiv -1 \pmod{641}$ és ezt negyedik hatványra emelve: $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$. Másrészt, $641 = 625 + 16 = 5^4 + 2^4$, ahonnan $2^4 \equiv -5^4 \pmod{641}$. Összeszorozva ez utóbbi két kongruenciát $5^4 \cdot 2^{32} \equiv -5^4 \pmod{641}$, s osztva $5^4$-nel, ahol $(5^4, 641) = 1$, kapjuk, hogy $2^{32} + 1 = 2^{2^5} + 1 \equiv 0 \pmod{641}$.
• 2. Ha $f$ egy egész együtthatós polinom és $x \equiv y \pmod m$, akkor $f(x) \equiv f(y) \pmod m$.
Valóban, legyen $f = a_0X^n + a_1X^{n-1} + ... + a_{n-1}X + a_n$. Mivel $x \equiv y \pmod m$, kapjuk, hogy $x^k \equiv y^k \pmod m$ minden $k \in \{0, 1, 2, ..., n\}$-re és összegezve $f(x) \equiv f(y) \pmod m$.
• 3. Vezessük le a 11-re vonatkozó következő oszthatósági szabályt. Egy tízes számrendszerbeli szám akkor osztható 11-gyel ha a páratlan helyein álló számjegyek összegéből kivonva a páros helyeken álló számjegyek összegét 11-gyel osztható számot kapunk. Legyen

$$n = a_0a_1...a_{k-1}a_{k(10)} = a_0.10^k + a_1.10^{k-1} + ... + a_{k-1}.10 + a_k$$

egy adott szám. Mivel $10 \equiv -1 \pmod{11}$, kapjuk, hogy $10^i \equiv (-1)^i \pmod{11}$, s innen

$$n = \sum_{i=0}^{k} a_{k-i}10^i \equiv \sum_{i=0}^{k}(-1)^i a_i (\bmod 11).$$

**Definíció.** Az egész számok egy $T$ rendszere **teljes maradékrendszer** $\pmod m$, ha minden $x \in \mathbb{Z}$ esetén létezik egy és csak egy $T$-beli $a$ szám úgy, hogy $x \equiv a \pmod m$.

Következik, hogy ha $T$ teljes maradékrendszer (mod $m$), akkor $T$ tartalmaz egy és csak egy elemet minden maradékosztályból (mod $m$). Így

**Tétel.** Az egész számok egy $T$ rendszere akkor és csak akkor teljes maradékrendszer (mod $m$), ha $T$ elemeinek a száma $m$ és ezek páronként inkongruensek (mod $m$). □

Teljes maradékrendszer (mod $m$) például a $0, 1, 2, ..., m-1$, ennek neve **legkisebb nemnegatív teljes maradékrendszer** (mod $m$) és a következő, **legkisebb abszolútértékű teljes maradékrendszer** (mod $m$), amely $-\frac{m-1}{2}, ..., -2, -1, 0, 1, 2, ..., \frac{m-1}{2}$, ha $m$ páratlan és $-(\frac{m}{2}-1), ..., -2, -1, 0, 1, 2, ..., \frac{m}{2}-1, \frac{m}{2}$, ha $m$ páros.

Gyakran használjuk a következő tulajdonságot:

**Tétel.** Ha $r_1, r_2, ..., r_m$ egy teljes maradékrendszer (mod $m$) és $a, b \in \mathbb{Z}, (a, m) = 1$, akkor $ar_1 + b, ar_2 + b, ..., ar_m + b$ is teljes maradékrendszer (mod $m$).

**Bizonyítás.** Azt kell igazolnunk, hogy az $ar_i + b$ számok páronként inkongruensek (mod $m$). Valóban, ha $ar_i + b \equiv ar_j + b$ (mod $m$), akkor $a(r_i - r_j) \equiv 0$ (mod $m$), de $(a, m) = 1$, így $r_i - r_j \equiv 0$ (mod $m$), azaz $r_i \equiv r_j$ (mod $m$), ahonnan $r_i = r_j$. □

**Definíció.** Az $\widehat{a}$ (mod $m$) maradékosztály neve **redukált maradékosztály** (mod $m$), ha $(a, m) = 1$. Ez a definíció nem függ a reprezentáns megválasztásától, lásd 2.1. szakasz. A (mod $m$) redukált maradékosztályok számát $\phi(m)$-mel jelöljük, ez az **Euler-függvény** (más jelölés: $\varphi(m)$).

**Példa.** • $m = 12$ esetén a (mod 12) redukált maradékosztályok: $\widehat{1}, \widehat{5}, \widehat{7}, \widehat{11}$ és ezek száma $\phi(12) = 4$.

$\phi(m)$ azoknak a számoknak a száma (mod $m$), amelyek $m$-hez relatív prímek. A legkisebb nemnegatív teljes maradékrendszert tekintve így $\phi(m)$ azoknak az $x$ számoknak a száma, amelyekre $0 \leq x \leq m-1$ és $(x, m) = 1$.

**Feladat.** ▼ Mennyi $\phi(6), \phi(7), \phi(24), \phi(p^a)$, ahol $p$ prím?

Igazolható, hogy ha $n$ kanonikus alakja $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$, akkor

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_r}\right).$$

**Definíció.** Az egész számok egy $R$ rendszere **redukált maradékrendszer** (mod $m$), ha minden $x \in \mathbb{Z}, (x, m) = 1$ szám esetén létezik egy és csak egy $R$-beli $a$ szám úgy, hogy $x \equiv a$ (mod $m$). Következik, hogy $R$ akkor redukált maradékrendszer (mod $m$) ha $R$ minden redukált maradékosztályból (mod $m$) tartalmaz egy és csak egy elemet. Ez a következőképpen is megfogalmazható:

**Tétel.** Az egész számok egy $R$ rendszere akkor és csak akkor redukált maradékrendszer (mod $m$), ha

i) $R$ elemeinek a száma $\phi(m)$,

ii) $R$ elemei páronként inkongruensek (mod $m$),

iii) $R$ minden eleme relatív prím $m$-hez. □

**Tétel.** Ha $r_1, r_2, ..., r_{\phi(m)}$ redukált maradékrendszer (mod $m$) és $a \in \mathbb{Z}, (a, m) = 1$, akkor $ar_1, ar_2, ..., ar_{\phi(m)}$ is redukált maradékrendszer (mod $m$).

**Bizonyítás.** Alkalmazzuk az előző Tételt. Az $ar_i$ elemek száma $\phi(m)$ és ezek páronként inkongruensek (mod $m$). Valóban, ha $ar_i \equiv ar_j$ (mod $m$), akkor $a$-val osztva, ahol $(a, m) = 1$, kapjuk, hogy $r_i \equiv r_j$ (mod $m$), ahonnan $r_i = r_j$. Továbbá minden $ar_i$ elem relatív prím $m$-mel, hiszen $(r_i, m) = 1$ és $(a, m) = 1$ alapján $(ar_i, m) = 1$. □

**Tétel.** (Euler kongruencia tétele) Ha $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor

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

**Bizonyítás.** Legyen $r_1, r_2, ..., r_{\phi(m)}$ egy redukált maradékrendszer (mod $m$). Tétel szerint akkor $ar_1, ar_2, ..., ar_{\phi(m)}$ is redukált maradékrendszer (mod $m$) és így minden $ar_i$-hez létezik egy és csak egy $r_j$ úgy, hogy $ar_i \equiv r_j \pmod{m}$, továbbá különböző $ar_i$-khez különböző elemek tartoznak az eredeti redukált maradékrendszerből. Kapjuk, hogy $ar_1 \equiv s_1 \pmod{m}$, $ar_2 \equiv s_2 \pmod{m}$, $ar_{\phi(m)} \equiv s_{\phi(m)} \pmod{m}$, ahol $s_1, s_2, ..., s_{\phi(m)}$ az $r_1, r_2, ..., r_{\phi(m)}$ egy permutációja. Összeszorozva ezeket a kongruenciákat:

$$a^{\phi(m)} r_1 r_2 ... r_{\phi(m)} \equiv r_1 r_2 ... r_{\phi(m)} (\mathrm{mod} m),$$

majd egyszerűsítve $r_1 r_2 ... r_{\phi(m)}$-mel, amely $m$-hez relatív prím, kapjuk, hogy $a^{\phi(m)} \equiv 1 \pmod{m}$. □

**Tétel.** (Fermat kongruencia tétele vagy kis Fermat tétel)

a) Ha $p$ prímszám, $a \in \mathbb{Z}$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

b) Ha $p$ prímszám és $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{p}$.

**Bizonyítás.** a) Azonnal következik az Euler tételből, ahol $m = p$ és $\phi(p) = p - 1$.

b) Ha $p \nmid a$, azaz ha $(a, p) = 1$, akkor az a) pont szerint $a^{p-1} \equiv 1 \pmod{p}$ és $a$-val szorozva $a^p \equiv a \pmod{p}$. Ha $p|a$, akkor $p \mid a^p$, így $p \mid a^p - a$, tehát a kongruencia ebben az esetben is igaz. □

**Példa.** • Ha $n \in \mathbb{Z}$ nem osztható 11-gyel, akkor $n^5 - 1$ vagy $n^5 + 1$ osztható 11-gyel. Valóban, a Fermat-tétel szerint ($a = n, p = 11$): $n^{10} \equiv 1 \pmod{11}$, ahonnan $11|n^{10} - 1 = (n^5 - 1)(n^5 + 1)$ és mivel 11 prím, kapjuk, hogy $11|n^5 - 1$ vagy $11|n^5 + 1$.

A Fermat-tétel fordítottja nem igaz. Ha $a^n \equiv a \pmod{n}$ valamely $a \in \mathbb{Z}$ számra, akkor nem következik, hogy $n$ prímszám.

**Példa** • Ha $a = 2$ és $n = 341 = 11 \cdot 31$, akkor $2^{341} \equiv 2 \pmod{341}$. Valóban, $2^{10} = 1024 \equiv 1 \pmod{11}$, közvetlen számítással vagy a Fermat tétel alapján, ahonnan $2^{340} \equiv 1 \pmod{11}$. Továbbá, $2^{10} = 1024 \equiv 1 \pmod{31}$, $2^{340} \equiv 1 \pmod{31}$ és kapjuk, hogy $2^{340} \equiv 1 \pmod{11 \cdot 31}$, tehát $2^{341} \equiv 2 \pmod{341}$.

A 2.1. szakaszban euklideszi gyűrűkre bizonyított tétel alapján kapjuk a következő tételt.

**Tétel.** Legyenek $a, b \in \mathbb{Z}$, $m \in \mathbb{N}^*$, $m \nmid a$ és legyen $d = (a, m)$.

1) Az $\boxed{ax \equiv b \,(\mathrm{mod}\ m)}$ (1) kongruenciának akkor és csak akkor van $x \in \mathbb{Z}$ megoldása, ha $d \mid b$.

2) Ha létezik $x_0$ megoldás, akkor az összes megoldás a következő alakú:

$$\boxed{x = x_0 + \frac{m}{d}t, \quad 0 \le t \le d - 1.} \tag{2}$$

3) Ha $d = 1$, akkor létezik megoldás és egy megoldás van (mod $m$), azaz bármely két megoldás kongruens (mod $m$). □

Az $ax \equiv b \pmod{m}$ (1) kongruenciát a következőképpen tudjuk megoldani. Ha $(a, m) = d \mid b$, akkor (1)-nek van megoldása és előbb megoldjuk az

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{3}$$

kongruenciát, amelynek mindig 1 megoldása van. (1)-nek pedig $d$ megoldása van, amelyeket a fenti (2) képlet szerint írhatunk fel.

Ha (3)-ban a modulus kicsi, akkor ennek megoldását próbálgatással kaphatjuk meg. Ellenkező esetben célszerű más megoldási módot keresni.

**Tétel.** Ha $(a, m) = 1$, akkor az (1) kongruencia egyetlen megoldása $x \equiv a^{\phi(m)-1}b \pmod{m}$.

**Bizonyítás.** Hogy egyetlen megoldás van, az következik az előbbi Tételből. Ha $x \equiv a^{\phi(m)-1}b \pmod{m}$, akkor $x$ valóban megoldás, hiszen az Euler-tétel szerint $ax \equiv a^{\phi(m)}b \equiv b \pmod{m}$. □

**Megjegyzés.** Nagy $m$ esetén e tétel alkalmazása meglehetősen sok számolással jár. Egy más, és talán a legjobb általános módszer az euklidészi algoritmus alkalmazása: Ha adott az (1) kongruencia, akkor meghatározzuk a $d = (a, m)$ értéket és egyúttal olyan $u$ és $v$ egész számokat, melyekre $au + mv = d$, lásd 2.1. szakasz. Innen $\frac{a}{d}u + \frac{m}{d}v = 1$, $\frac{a}{d}u \equiv 1 \pmod{\frac{m}{d}}$ és $b/d$-vel szorozva $\frac{a}{d}(bu/d) \equiv b/d \pmod{\frac{m}{d}}$, azaz $x = bu/d$ a (3) kongruencia egy megoldása és innen meghatározható (1) összes megoldása.

**Példák.** • 1. Oldjuk meg a $13x \equiv 5 \pmod{29}$ kongruenciát.

Mivel $(13, 29) = 1$, a kongruencia megoldható, 1 megoldása van (mod 29), s ez $x \equiv 16 \pmod{29}$, mely megkapható próbálgatással, de ez hosszadalmas.

Az előbbi Tétel alkalmazásával $x \equiv 13^{\phi(29)-1} \cdot 5 = 13^{27} \cdot 5 = 169^{13} \cdot 13 \cdot 5 = (6 \cdot 29 - 5)^{13} \cdot 13 \cdot 5 \equiv -5^{13} \cdot 65 \equiv -25^6 \cdot 5(2 \cdot 29 + 7) \equiv -(29 - 4)^6 \cdot 5 \cdot 7 \equiv -4^6 \cdot 35 \equiv -4^6 \cdot 6 \equiv -(2^5)^2 \cdot 24 \equiv -3^2(-5) \equiv 45 \equiv 16 \pmod{29}$, de látjuk, hogy ez is is hosszadalmas számításokat igényel.

Másképp, az euklidészi algoritmus segítségével: $29 = 2 \cdot 13 + 3$,
$13 = 4 \cdot 3 + 1$,
$3 = 3 \cdot 1 + 0$,
és innen $1 = 13 - 4 \cdot 3 = 13 - 4(29 - 2 \cdot 13) = 9 \cdot 13 - 4 \cdot 29$. Kapjuk, hogy $13 \cdot 9 \equiv 1 \pmod{29}$, 5-tel szorozva $13 \cdot 45 \equiv 5 \pmod{29}$, $13 \cdot 16 \equiv 5 \pmod{29}$, tehát $x \equiv 16 \pmod{29}$.

Sok esetben gyorsabban célba érünk, ha a kongruenciához hozzáadjuk a modulust vagy annak alkalmas többszörösét, illetve a kongruenciát szorozzuk vagy osztjuk egy alkalmas számmal (osztás esetén ez legyen relatív prím a modulussal). Itt például 3-mal szorozva $39x \equiv 15 \pmod{29}$, $10x \equiv 15 \pmod{29}$, amit 5-tel osztva $2x \equiv 3 \pmod{29}$, majd 15-tel szorozva $30x \equiv 45 \pmod{29}$, $x \equiv 16 \pmod{29}$.

• 2. Oldjuk meg a $21x \equiv 14 \pmod{35}$ kongruenciát.

Most $(21, 35) = 7|14$, a kongruencia tehát megoldható és 7 megoldás van (mod 35). Felírva a (3)-nak megfelelő $3x \equiv 2 \pmod{5}$ kongruenciát, ennek egyedüli megoldása $x \equiv 4 \pmod{5}$ és innen $x \equiv 4, 9, 14, 19, 24, 29, 34 \pmod{35}$.

**Feladat.** ▼ Oldjuk meg a következő kongruenciákat:
a) $26x \equiv 6 \pmod{68}$, b) $19x \equiv 11 \pmod{24}$, c) $36x \equiv 7 \pmod{20}$.

**Tétel.** (Wilson-tétel) Ha $p$ prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

★ **Bizonyítás.** Ellenőrízhető, hogy a tétel igaz $p = 2$ és $p = 3$ esetén. Legyen $p > 3$ és $H = \{2, 3, 4, ..., p-2\}$. Megmutatjuk, hogy minden $a \in H$-ra létezik egy és csak egy $a' \in H$ úgy, hogy $a' \neq a$ és $aa' \equiv 1 \pmod{p}$. Valóban, tekintsük az $T = \{0, 1, 2, ..., p-1\}$ legkisebb nemnegatív (mod $p$) teljes maradékrendszert. Tétel szerint létezik egy és csak egy $x \in T$ úgy, hogy $ax \equiv 1 \pmod{p}$. Itt $x \neq 0, x \neq 1, x \neq p-1, x \neq a$. Ha például $x = a$ lenne, akkor $a^2 \equiv 1 \pmod{p}$, ahonnan $p|(a-1)(a+1)$, s mivel $p$ prím kapjuk, hogy $p|a-1$

vagy $p|a+1$, ami ellentmondást jelent.

Ugyanakkor így különböző $a$ értékekhez különböző $a'$ értékek tartoznak és a $H$ halmaz elemei párba állíthatók úgy, hogy minden párban az elemek szorzata 1-gyel kongruens (mod $p$). Összeszorozva ezeket a kongruenciákat: $(p-2)! \equiv 1 \pmod{p}$ és innen $(p-1)! = (p-1)(p-2)! \equiv p-1 \equiv -1 \pmod{p}$. □

**Megjegyzés.** Igaz a fordított állítás is: Ha $n \in \mathbb{N}^*$ és $(n-1)! \equiv -1 \pmod{n}$, akkor $n$ prímszám. Valóban, ha $n$ nem lenne prím, akkor létezne $k|n, 1 < k < n$. Az $n|(n-1)!+1$ feltételből $k|(n-1)!+1$ és mivel $k \leq n-1$, ezért $k|(n-1)!$, ahonnan $k|1$, ami ellentmondás. ★

A továbbiakban lineáris kongruenciarendszerekkel foglalkozunk, ezek általános alakja a következő :

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ a_kx &\equiv b_k \pmod{m_k}. \end{aligned}$$

Ahhoz, hogy ennek a rendszernek legyen megoldása szükséges, hogy az egyes kongruenciáknak legyenek megoldásaik és ezeket a megoldásokat tekintve egy

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

alakú (4) kongruenciarendszert kapunk. Ilyen rendszerre vonatkozik az alábbi tétel.

**Tétel.** (Kínai maradéktétel) Ha az $m_1, m_2, ..., m_k$ modulusok páronként relatív prímek és $c_1, c_2, ..., c_k$ tetszőleges egész számok, akkor a (4) rendszernek létezik megoldása és egy megoldás van (mod $m_1m_2...m_k$).

**Bizonyítás.** Legyen $m = m_1m_2...m_k$ és tekintsük az

$$\frac{m}{m_i}x \equiv 1 \pmod{m_i} \tag{5}$$

kongruenciákat, $1 \leq i \leq k$. Mivel $(\frac{m}{m_i}, m_i) = 1$, Tétel alapján (5)-nek létezik megoldása, legyen egy megoldás $x = e_i$. Így

$$\frac{m}{m_j}e_j \equiv \begin{cases} 1 \pmod{m_i}, \text{ ha } j = i, \\ 0 \pmod{m_i}, \text{ ha } j \neq i. \end{cases} \tag{6}$$

Legyen most

$$x_0 = \sum_{j=1}^{k} \frac{m}{m_j}e_jc_j.$$

(6) alapján kapjuk, hogy minden $i$-re $x_0 \equiv c_i \pmod{m_i}$, tehát $x_0$ megoldása a (4) rendszernek. Ha $x_0'$ egy másik megoldás, akkor $m_i|x_0 - c_i$ és $m_i|x_0' - c_i$, ahonnan $m_i|x_0 - x_0'$ minden $i$-re, s kapjuk, hogy $m_1m_2...m_k = m|x_0 - x_0'$, azaz $x_0 \equiv x_0' \pmod{m}$. □

**Feladatok**

▼ 1. Oldjuk meg a következő kongruenciarendszereket:

a) $x \equiv 3 \pmod{5}$, $x \equiv 1 \pmod{6}$, $x \equiv 2 \pmod{7}$;

b) $5x \equiv 3 \pmod{7}$, $3x \equiv 7 \pmod{8}$.

▼ 2. Határozzuk meg azokat a 4-jegyű számokat, amelyek 72-vel osztva 46 maradékot, 127-tel osztva pedig 97 maradékot adnak.

### 3.2. Elsőfokú diofántoszi egyenletek

Az elsőfokú kongruenciák szoros kapcsolatban vannak a kétismeretlenes elsőfokú (lineáris) **diofántoszi egyenlet**ekkel, amelyek általános alakja

$$ax + by = c,$$

ahol az $a, b, c$ együtthatók egész számok és az $x, y$ ismeretleneket is a $\mathbb{Z}$ halmazban keressük.

A 2.1. szakaszban bizonyított tételből kapjuk:

**Tétel.** Legyenek $a, b, c \in \mathbb{Z}, a \neq 0, b \neq 0$.

1) Az $\boxed{ax + by = c}$ egyenletnek akkor és csak akkor van $x, y \in \mathbb{Z}$ megoldása, ha $(a, b) \mid c$.

2) Ha létezik $x_0, y_0$ megoldás, akkor végtelen sok megoldás van és az összes megoldás a következő alakú:

$$\boxed{x = x_0 + \frac{b}{(a,b)}t, \quad y = y_0 - \frac{a}{(a,b)}t, \quad t \in \mathbb{Z}.}$$

Kérdés, hogyan határozható meg egy $x_0, y_0$ megoldás? Erre módszer az euklidészi algoritmus alkalmazása: meghatározzuk a $d = (a, b)$ értéket és egyúttal olyan $u$ és $v$ egész számokat, melyekre $au + mv = d$. Innen $c/d$-vel szorozva $a\frac{cu}{d} + b\frac{cv}{d} = c$, ami azt mutatja, hogy $x_0 = \frac{cu}{d}$, $y = \frac{cv}{d}$ egy megoldás.

Egy másik megoldási módszert illusztrál a következő példa.

**Példa.** • Oldjuk meg az előbbi $13x \equiv 5 \pmod{29}$ kongruenciát úgy, hogy elsőfokú diofantoszi egyenletre vezetjük vissza. A megfelelő egyenlet $13x - 29y = 5$, fejezzük ki $x$-et: $x = \frac{29y+5}{13} = 2y + \frac{3y+5}{13}$, ahol legyen $\frac{3y+5}{13} = z \in \mathbb{Z}$. Kapjuk a $3y + 5 = 13z$ egyenletet, melyből fejezzük ki az $y$-t: $y = \frac{13z-5}{3} = 4z - 2 + \frac{z+1}{3}$, s innen $\frac{z+1}{3} = t \in \mathbb{Z}, z + 1 = 3t$, újabb egyenlet, ahonnan $z = 3t - 1$. Visszahelyettesítve, $y = 12t - 4 - 2 + t = 13t - 6, x = 26t - 12 + 3t - 1 = 29t - 13$. Tehát az eredeti egyenlet megoldása $x = 29t - 13, y = 13t - 6$, ahol $t \in \mathbb{Z}$, a kongruencia megoldása pedig $x \equiv -13 \equiv 16 \pmod{29}$.

**Megjegyzés.** Ez a módszer minden $ax + by = c$ diofántoszi egyenlet megoldására alkalmazható, rendre az abszolútértékben kisebb együtthatójú ismeretlent fejezzük ki és belátható, hogy ekkor véges sok lépés után eredményre jutunk.

**Feladatok**

▼ 1. Oldjuk meg: a) 18x+5y=2, b) 36x+15y=51.

▼ 2. Igazoljuk, hogy az $a_1x_1 + a_2x_2 + ... + a_kx_k = c$ diofántoszi egyenletnek akkor és csak akkor van megoldása ha $(a_1, a_2, ..., a_k)|c$.

### 3.3. Magasabbfokú kongruenciák

**Definíció.** Tekintsük az $f = a_0X^n + a_1X^{n-1} + ... + a_{n-1}X + a_n$ egész együtthatós polinomot és az $f(x) \equiv 0 \pmod{m}$ kongruenciát, ahol $m \in \mathbb{N}^*$. Ezt **$n$-edfokú kongruenciá**nak nevezzük, ha $a_0 \not\equiv 0 \pmod{m}$, azaz, ha $m \nmid a_0$, és ennek **megoldás**a minden olyan $x = x_0 \in \mathbb{Z}$ szám, melyre $f(x_0) \equiv 0 \pmod{m}$ fennáll.

Ha $x_0$ megoldás és $x \equiv x_0 \pmod{m}$, akkor $x$ is megoldása az adott kongruenciának, hiszen $f(x) \equiv f(x_0) \equiv 0 \pmod{m}$. Így, ha $x_0$ megoldás, akkor az $\widehat{x_0}$ maradékosztály (mod $m$) minden eleme megoldás, tehát végtelen sok megoldás van. Ezért elegendő egy teljes maradékrendszer, például a legkisebb nemnegatív teljes maradékrendszer elemeit vizsgálni.

**Példák.** • A $3x^2+2x-1 \equiv 0 \pmod 5$ másodfokú kongruenciának $x=2$ és $x=4$ megoldása, így megoldás minden $x=2+5k$ és $x=4+5k, k \in \mathbb{Z}$ szám és más megoldás nincs (erről behelyettesítéssel győződhetünk meg).

• A $3x^3+3x^2+1 \equiv 0 \pmod 6$ harmadfokú kongruenciának nincs megoldása, mert minden $x \in \mathbb{Z}$-re $3x^3+3x^2=3x^2(x+1)$ osztható 6-tal, de $6 \nmid 1$.

**Definíció.** Az $f(x) \equiv 0 \pmod m$ kongruencia **megoldásai számá**nak a páronként inkongruens (mod $m$) megoldások számát nevezzük. Két kongruenciát **egyenértékű**nek nevezünk, ha megoldáshalmazaik egyenlőek.

Egy kongruenciát célszerű redukálni, azaz minden együtthatóját helyettesíteni a vele kongruens (mod $m$) legkisebb nemnegatív, illetve legkisebb abszolútértékű számmal.

**Példa.** • Redukálva az $x^4+12x^3+7x^2-8x+2 \equiv 0 \pmod 6$ kogruenciát kapjuk a vele egyenértékű $x^4+x^2-2x+2 \equiv 0 \pmod 6$ kongruenciát.

Ha a modulus kis szám, akkor egy kongruencia megoldásait megkaphatjuk próbálgatással.

**Tétel.** Minden $n$-edfokú $p$ prímmodulusú kongruencia egyenértékű egy legfeljebb $(p-1)$-edfokú kongruenciával.

**Bizonyítás.** Legyen $f(x) \equiv 0 \pmod p$ egy $n$-edfokú $p$ prímmodulusú kongruencia. Ha az $f$ polinomot elosztjuk a $g=x^p-x$ polinommal, akkor $f=(x^p-x)q(x)+r(x)$, ahol az $r$ maradék egy, legfeljebb $(p-1)$-edfokú polinom. Megmutatjuk, hogy az $f(x) \equiv 0 \pmod p$ kongruencia egyenértékű az $r(x) \equiv 0 \pmod p$ kongruenciával. Valóban, a kis Fermat-tétel szerint $x^p-x \equiv 0 \pmod p$ minden $x \in \mathbb{Z}$-re, így $f(x) \equiv r(x) \pmod p$. □

**Megjegyzések.** 1. Megtörténhet, hogy $r$ egy $k$-adfokú ($k \leq p-1$) polinom és az $r(x) \equiv 0 \pmod p$ kongruencia $k$-nál alacsonyabb fokú, ha $r$-ben a legmagasabbfokú tagok együtthatói $p$ többszörösei.

2. Ha $p \nmid a_0$, akkor $x \equiv 0 \pmod p$ nem megoldás és $x^{p-1}-1$-gyel osztva az adott kongruencia egy, legfeljebb $(p-2)$-edfokú kongruenciára redukálható.

**Példa.** • Oldjuk meg a $3x^{14}+4x^{13}+4x^7+3x^3+4x^2+2x \equiv 0 \pmod 5$ kongruenciát.

A Fermat-tétel szerint $x^5 \equiv x \pmod 5$, innen $x^7 \equiv x^3 \pmod 5$, $x^{10} \equiv x^2 \pmod 5$, $x^{13} \equiv x^5 \equiv x \pmod 5$, $x^{14} \equiv x^2 \pmod 5$ és kapjuk, hogy $3x^2+4x+4x^3+3x^3+4x^2+2x \equiv 0 \pmod 5$, $7x^3+7x^2+6x \equiv 0 \pmod 5$, $2x^3+2x^2+x \equiv 0 \pmod 5$, amelynek megoldásai $x \equiv 0,1,3 \pmod 5$.

**Tétel.** (Lagrange) Az $f(x) \equiv 0 \pmod p$ $n$-edfokú ($n \geq 1$), $p$ prímmodulusú kongruenciának legfeljebb $n$ megoldása van.

**Bizonyítás.** $n$ szerinti indukcióval bizonyítunk. Ha $n=1$, akkor az $a_0x+a_1 \equiv 0 \pmod p$, $(a_0,p)=1$ elsőfokú kongruenciának egy megoldása, korábbi Tétel szerint. Tegyük fel, hogy az állítás igaz minden legfeljebb $(n-1)$-edfokú kongruenciára és nem igaz minden $n$-edfokú kongruenciára, azaz létezik olyan $f(x) \equiv 0 \pmod p$ $n$-edfokú kongruencia, amelynek legalább $(n+1)$ (mod $p$) inkongruens megoldása van: $x_1, x_2, ..., x_n, x_{n+1}$.

Az $f$ polinomot $(x-x_1)$-gyel osztva $f=(x-x_1)g(x)+c$, ahol $g$ $(n-1)$-edfokú polinom és $c=f(x_1) \equiv 0 \pmod p$, így $f(x) \equiv (x-x_1)g(x) \pmod p$. Minden $i \in \{2,3,...,n,n+1\}$-re $f(x_i) \equiv (x_i-x_1)g(x_i) \equiv 0 \pmod p$, de $x_i \not\equiv x_1 \pmod p$, ahonnan $g(x_i) \equiv 0 \pmod p$. Kapjuk, hogy $x_2, x_3, ..., x_n, x_{n+1}$ megoldásai a legfeljebb $(n-1)$-edfokú $g(x) \equiv 0 \pmod p$ kongruenciának, ami ellentmond az indukciós feltevésnek és ezzel a bizonyítás kész. □

**Megjegyzés.** Összetett modulus esetén a fenti Lagrange-tétel állítása nem igaz, például az $x^3+5x \equiv 0 \pmod 6$ kogruencia megoldásai $x \equiv 0,1,2,3,4,5 \pmod 6$ és ezek száma nagyobb mint 3.

**Tétel.** Ha az $f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n \equiv 0 \pmod{p}$ $p$ prímmodulusú kongruenciának $(n+1)$ inkongruens megoldása van (mod $p$), akkor $p \mid a_i$ minden $i \in \{0, 1, ..., n\}$-re.

**Bizonyítás.** Következik az előbbi tételből. Ha létezne $a_i \not\equiv 0 \pmod{p}$, $0 \leq i \leq n-1$, akkor az adott kongruencia legalább elsőfokú és legfeljebb $n$-edfokú lenne és következne, hogy legfeljebb $n$ megoldása van, ami ellentmondás. Ha $a_i \equiv 0 \pmod{p}$, $0 \leq i \leq n-1$, akkor következik, hogy $a_n \equiv 0 \pmod{p}$. □

**Példa.** • Ha az $f(x) = x^{p-1} - 1 - (x-1)(x-2)...(x-p+1) \equiv 0 \pmod{p}$ $p \geq 3$ prímmodulusú kongruenciát tekintjük, akkor ez legfeljebb $(p-2)$-edfokú, hiszen az $x^{p-1}$ és $-x^{p-1}$ tagok összege nulla. Továbbá a Fermat-tétel alkalmazásával $f(1) \equiv f(2) \equiv ... \equiv f(p-1) \equiv 0 (\text{mod } p)$, tehát van $p-1$ inkongruens megoldás (mod $p$), és az előbbi Tételből kapjuk, hogy minden együttható osztható $p$-vel, azaz

$S_1 = 1 + 2 + ... + (p-1) \equiv 0 \pmod{p}$,

$S_2 = 1 \cdot 2 + 1 \cdot 3 + ... + (p-1)p \equiv 0 \pmod{p}$,

.....

$S_{p-2} = \frac{(p-1)!}{1} + \frac{(p-1)!}{2} + ... + \frac{(p-1)!}{p-1} \equiv 0 \pmod{p}$,

$S_{p-1} = 1 \cdot 2 \cdot 3...(p-1) + 1 \equiv 0 \pmod{p}$.

Az utolsó kongruencia éppen a Wilson-tétel.

★Továbbá, a Viéte-képletek szerint $g(x) = (x-1)(x-2)...(x-p+1) = x^{p-1} - S_1x^{p-2} + S_2x^{p-3} - ... - S_{p-2}x + (p-1)!$, ahonnan $x = p$-re: $g(p) = (p-1)! = p^{p-1} - S_1p^{p-2} + S_2p^{p-3} - ... - S_{p-2}p + (p-1)!$. Következik, hogy $p^{p-1} - S_1p^{p-2} + S_2p^{p-3} - ... - S_{p-2}p = 0$, ahol, ha $p \geq 5$, akkor az utolsó tag kivételével minden tag osztható $p^3$-nal, de így ez az utolsó tagra is igaz.

Ezzel igazoltuk a következő eredményt:

**Tétel.** (Wolstenholme) Ha $p \geq 5$ prímszám, akkor

$$S_{p-2} = (p-1)!(1 + \frac{1}{2} + ... + \frac{1}{p-1}) \equiv 0 \pmod{p^2}. \quad \square\bigstar$$

### 3.4. Másodfokú kongruenciák, négyzetes maradékok

Most a másodfokú kongruenciákat vizsgáljuk.

A másodfokú kongruenciák általános alakja $ax^2 + bx + c \equiv 0 \pmod{m}$, ahol $m \nmid a$. Ezek visszavezethetők $x^2 \equiv d \pmod{n}$ alakú kongruenciákra és így elegendő ez utóbbiakkal foglalkoznunk. Valóban, $4a$-val szorozva: $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}$, $(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}$, s a $2ax + b = y, b^2 - 4ac = d, 4am = n$ jelölésekkel az $y^2 \equiv d \pmod{n}$ kongruenciához jutunk.

Vizsgáljuk először az $x^2 \equiv -1 \pmod{p}$ kongruenciát, ahol $p$ prím.

**Tétel.** Az $x^2 \equiv -1 \pmod{p}$ kongruenciának, ahol $p$ prím, akkor és csak akkor létezik $x \in \mathbb{Z}$ megoldása, ha $p = 2$ vagy ha $p \equiv 1 \pmod{4}$.

**Bizonyítás.** Ha $p = 2$, akkor választható $x = 1$ és $1 \equiv -1 (\text{mod } 2)$. Legyen $p \equiv 1 \pmod{4}$, azaz $p = 4k+1$ alakú, ahol $k \in \mathbb{N}$. Láttuk a 2.2. szakaszban, hogy akkor $x = (2k)!$ megoldás.

Most legyen $p \equiv 3 \pmod{4}$, azaz $p = 4k + 3$ alakú, ahol $k \in \mathbb{N}$ és tegyük fel, hogy létezik $x \in \mathbb{Z}$ úgy, hogy $x^2 \equiv -1 \pmod{p}$. Mindkét oldalt $\frac{p-1}{2} = 2k + 1$ hatványra emelve: $x^{p-1} \equiv -1 \pmod{p}$. Itt $p \nmid x$, hiszen ellenkező esetben következne, hogy $p| - 1$, ami ellentmondás. A Fermat-tétel szerint így $x^{p-1} \equiv 1 \pmod{p}$ és következik, hogy $-1 \equiv 1 \pmod{p}$, azaz $p|2$, ami ellentmondás. □

**Definíció.** Azt mondjuk, hogy az $a$ szám **négyzetes (kvadratikus) maradék** (mod $m$) ha az $x^2 \equiv a \pmod m$ kongruenciának van megoldása és **négyzetes (kvadratikus) nemmaradék** (mod $m$) ha ennek a kongruenciának nincs megoldása.

**Példa.** • $a = -1$ négyzetes maradék (mod $p$), $p$ prím, ha $p = 2$ vagy $p \equiv 1 \pmod 4$ és négyzetes nemmaradék (mod $p$), ha $p \equiv 3 \pmod 4$.

Ha $a$ négyzetes maradék (mod $p$), $p > 2$ pím és $(a, p) = 1$, akkor az $x^2 \equiv a \pmod p$ kongruenciának 2 megoldása van. Valóban, definíció alapján van egy $x_0$ megoldás, de akkor $-x_0$ is megoldás és ezek különbözőek, mert $x_0 \equiv -x_0 \pmod p$ akkor és csak akkor, ha $2x_0 \equiv \pmod p$, ami lehetetlen, mert $(p, 2) = (a, p) = 1$. Ugyanakkor a Lagrange-tétel szerint legfeljebb 2 megoldás van.

Az $x^2 \equiv -1 \pmod p$, $p \equiv 1 \pmod 4$ kongruencia megoldásai $x \equiv \pm(\frac{p-1}{2})! \pmod p$, lásd az előbbi Tétel bizonyítását.

Megjegyezzük, hogy $p = 2$ esetén az $x^2 \equiv 1 \pmod 2$ kongruenciának egy megoldása van: $x \equiv 1 \pmod 2$.

**Tétel.** Ha $p > 2$ prímszám, akkor minden (mod $p$) redukált maradékrendszer $\frac{p-1}{2}$ számú (mod $p$) négyzetes maradékot tartalmaz, amelyek kongruensek az

$$1^2, 2^2, 3^2, ..., (\frac{p-1}{2})^2$$

számokkal, és $\frac{p-1}{2} \pmod p$ négyzetes nemmaradékot tartalmaz.

**Bizonyítás.** Legyen $(a, p) = 1$. Az $a$ akkor és csak akkor négyzetes maradék (mod $p$), ha kongruens egy redukált maradékrendszer (mod $p$) valamely elemének a négyzetével. Válasszuk a legkisebb abszolútértékű redukált maradékrendszert: $-\frac{p-1}{2}, ..., -2, -1, 1, 2,$ $..., \frac{p-1}{2}$, így $a$ kongruens az $1^2, 2^2, 3^2, ...., (\frac{p-1}{2})^2$ számok valamelyikével. Ezek inkongruensek (mod $p$), mert ha $x^2 \equiv y^2 \pmod p$, ahol $1 \le y < x \le \frac{p-1}{2}$, akkor $p|x^2 - y^2 = (x - y)(x + y)$, tehát $p|x - y$ vagy $p|x + y$, ami lehetetlen, mert $1 \le x - y, x + y \le p - 1$. □

**Tétel.** (Euler-lemma) Ha $p > 2$ prímszám és $(a, p) = 1$, akkor

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p, \text{ ha } a \text{ négyzetes maradék (mod } p), \\ -1 \pmod p, \text{ ha } a \text{ négyzetes nemmaradék (mod } p). \end{cases}$$

**Bizonyítás.** Ha $a$ négyzetes maradék, akkor $a \equiv y^2 \pmod p$ valamely $y$-ra, ahol $(y, p) = 1$. Itt $(p - 1)/2$-hatványra emelve $a^{(p-1)/2} \equiv y^{p-1} \equiv 1 \pmod p$, használva a Fermat-tételt. A négyzetes maradékok, ezek száma $(p - 1)/2$, tehát mind megoldásai az $x^{(p-1)/2} \equiv 1$ kongruenciának és más megoldások nem lehetnek, mert a Lagrange-tétel szerint a megoldások száma legfeljebb $(p - 1)/2$.

Ha $a$ négyzetes nemmaradék, akkor az előbbiek szerint $a^{(p-1)/2} \not\equiv 1 \pmod p$. Ugyanakkor a Fermat-tétel szerint $a^{p-1} \equiv 1 \pmod p$, ahonnan $p|a^{(p-1)/2} - 1$ vagy $p|a^{(p-1)/2} + 1$ és kapjuk, hogy $a^{(p-1)/2} \equiv -1 \pmod p$. □

**Példa.** • Vizsgáljuk meg, hogy $a = 13$ négyzetes maradék-e (mod 17).

$13^{\frac{17-1}{2}} \equiv 13^8 \equiv (-4)^8 \equiv (4^2)^4 \equiv 16^4 \equiv (-1)^4 \equiv 1 \pmod{17}$, így kapjuk, hogy 13 négyzetes maradék (mod 17), tehát az $x^2 \equiv 13 \pmod{17}$ kongruencia megoldható és két megoldása $x \equiv 8 \pmod{17}$, $x \equiv -8 \equiv 9 \pmod{17}$, ami ellenőrzéssel kapható meg.

**Definíció.** Ha $p > 2$ prímszám és $(a, p) = 1$, akkor az $(\frac{a}{p})$ **Legendre-szimbólum**ot (olvasd „a per p" Legendre-szimbólum) a következőképpen definiáljuk:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ ha } a \text{ négyzetes maradék (mod } p), \\ -1, \text{ ha } a \text{ négyzetes nemmaradék (mod } p). \end{cases}$$

**Tétel.** (A Legendre-szimbólum tulajdonságai) Ha $p > 2$ prímszám és $(a, p) = (b, p) = 1$, akkor

1) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p$; $\quad (\frac{a^2}{p}) = 1$; $\quad (\frac{1}{p}) = 1$;

2) Ha $a \equiv b \pmod p$, akkor $(\frac{a}{p}) = (\frac{b}{p})$;

3) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$; $\quad (\frac{a^2b}{p}) = (\frac{b}{p})$;

4)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ ha } p = 4k+1 \text{ alakú}, \\ -1, \text{ ha } p = 4k-1 \text{ alakú}. \end{cases}$$

**Bizonyítás.** 1) és 2) az Euler-lemma és a definíció azonnali következménye.

3) Az 1) alkalmazásával $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \pmod p$, azaz $p|(\frac{ab}{p}) - (\frac{a}{p})(\frac{b}{p}) \in \{-2, 0, 2\}$, és mivel $p > 2$ kapjuk, hogy $(\frac{ab}{p}) - (\frac{a}{p})(\frac{b}{p}) = 0$.

4) Következik 1)-ből és a jelen szakasz első Tételéből is. □

**Megjegyzés.** A fenti 3) tulajdonság szerint egy $p > 2$ prímre vonatkozó két négyzetes maradék (két négyzetes nemmaradék) szorzata négyzetes maradék, egy négyzetes maradék és egy négyzetes nemmaradék szorzata pedig négyzetes nemmaradék. □

**Példa.** • Határozzuk meg a négyzetes maradékokat (mod 17).

Ezek száma $\frac{17-1}{2} = 8$. Biztosan ilyenek az $1, 4, 9, 16$ teljes négyzetek és ezek szorzatai: $4 \cdot 9 \equiv 36 \equiv 2 \pmod{17}$, $4 \cdot 2 \equiv 8 \pmod{17}$, $2 \cdot 16 \equiv 32 \equiv 15 \pmod{17}$, $2 \cdot 15 \equiv 30 \equiv 13 \pmod{17}$, s ez már 8 érték, a négyzetes maradékok (mod 17) tehát $1, 2, 4, 8, 9, 13, 15, 16$, a négyzetes nemmaradékok (mod 17) pedig $3, 5, 6, 7, 10, 11, 12, 14$.

**Megjegyzés.** Az előző Tétel 3) pontja általánosításaként következik, hogy

$$\left(\frac{a_1 a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_k}{p}\right),$$

ahol $a_1, a_2, ..., a_k$ relatív prímek $p$-vel. Így, ha $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, akkor $(\frac{a}{p})$ kiszámítása visszavezethető $(\frac{p_i}{p})$ és $(\frac{-1}{p})$ kiszámítására. Ez utóbbit megadja az előbbi Tétel 4) pontja, nézzük most a $(\frac{q}{p})$ kiszámítási lehetőségeit, ahol $p$ és $q$ különböző prímek. Erre vonatkozik a nevezetes négyzetes (kvadratikus) reciprocitási tétel.

**Tétel.** (A négyzetes reciprocitás tétele) Ha $p, q \geq 3$ különböző prímszámok, akkor

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

azaz

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), \text{ ha } p \text{ vagy } q \text{ } 4k+1 \text{ alakú}, \\ -\left(\frac{q}{p}\right), \text{ ha } p \text{ és } q \text{ } 4k-1 \text{ alakú}. \end{cases} \quad \square$$

**Példák.** • 1. Határozzuk meg a $(\frac{990}{3719})$ Legendre-szimbólum értékét, ahol 3719 prímszám.

$990 = 2 \cdot 3^2 \cdot 5 \cdot 11$ és kapjuk, hogy $(\frac{990}{3719}) = (\frac{2}{3719})(\frac{3^2}{3719})(\frac{5}{3719})(\frac{11}{3719})$. Itt $(\frac{2}{3719}) = 1$, mert $3719 \equiv -1 \pmod 8$, lásd Tétel, $(\frac{3^2}{3719}) = 1$, továbbá alkalmazva a reciprocitási tételt $(\frac{5}{3719}) = (\frac{3719}{5}) = (\frac{743 \cdot 5 + 4}{5}) = (\frac{4}{5}) = 1$, ahol $5 \equiv 1 \pmod 4$ és $(\frac{11}{3719}) = -(\frac{3719}{11}) = -(\frac{1}{11}) = -1$, ahol $11 \equiv -1 \pmod 4$, $3719 \equiv -1 \pmod 4$. Így $(\frac{990}{3719}) = -1$, azaz 990 négyzetes nemmaradék (mod 3719).

★ • 2. Határozzuk meg a $(\frac{3}{p})$ és $(\frac{-3}{p})$ Legendre-szimbólumok értékét, ahol $p > 3$ prímszám.

A kvadratikus reciprocitás tétele szerint $(\frac{3}{p}) = (\frac{p}{3})$, ha $p \equiv 1 \pmod 4$ és $(\frac{3}{p}) = -(\frac{p}{3})$, ha $p \equiv -1 \pmod 4$. A következő eseteket tekintjük: I. $p \equiv 1 \pmod{12}$, ekkor $(\frac{3}{p}) = (\frac{p}{3}) = (\frac{1}{3}) = 1$; II. $p \equiv 5 \pmod{12}$, ekkor $(\frac{3}{p}) = (\frac{p}{3}) = (\frac{2}{3}) = -1$; III. $p \equiv 7 \pmod{12}$, most $(\frac{3}{p}) = -(\frac{p}{3}) = -(\frac{1}{3}) = -1$; végül IV. $p \equiv 11 \pmod{12}$, ekkor $(\frac{3}{p}) = -(\frac{p}{3}) = -(\frac{-1}{3}) = 1$.

Azt kapjuk, hogy $(\frac{3}{p}) = 1$ ha $p \equiv \pm 1 \pmod{12}$ és $(\frac{3}{p}) = -1$ ha $p \equiv \pm 5 \pmod{12}$.

Továbbá $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p})$ és a Lagrange-szimbólum tulajdonságai alapján $(\frac{-3}{p}) = 1$ ha $p \equiv 1, -5 \pmod{12}$ és $(\frac{3}{p}) = -1$ ha $p \equiv -1, 5 \pmod{12}$. ★

### 3.5. A rend és a primitív gyök fogalma

Szükségünk van a következő fogalmakra és tulajdonságokra.

**Definíció.** Legyen $m \in \mathbb{N}^*, a \in \mathbb{Z}, (a, m) = 1$. Az $a$ **rendje** (mod $m$) az a legkisebb $k \in \mathbb{N}^*$ szám, amelyre $a^k \equiv 1 \pmod m$, jelölés $k = o_m(a) = o(a)$, ha $m$ rögzített. Azt is mondjuk, hogy $a$ a $k = o(a)$ kitevőhöz tartozik (mod $m$). Euler tétele szerint ha $(a, m) = 1$, akkor $a^{\phi(m)} \equiv 1 \pmod m$, így minden $a$-nak létezik rendje és $o_m(a) \leq \phi(m)$.

Megjegyezzük még, hogy ha $a \equiv b \pmod m$, akkor $o_m(a) = o_m(b)$. Ha $(a, m) > 1$, akkor nincs olyan $k \in \mathbb{N}^*$, melyre $a^k \equiv 1 \pmod m$, ekkor nem definiáljuk a rend fogalmát.

**Megjegyzés.** Tekintsük a (mod $m$) redukált maradékosztályok $R_m = U(Z_m)$ multiplikatív csoportját, amelynek rendje (a csoport elemeinek a száma) éppen $\phi(m)$ az Euler-függvény. Ha $(x, m) = 1$, akkor az $\widehat{x} \in R_m$ redukált maradékosztály rendje - úgy, ahogy a csoportok esetén definiáltuk - egyenlő az $x \in \mathbb{Z}$ szám rendjével a fenti definíció szerint.

**Tétel.** (A rend tulajdonságai) Ha $(a, m) = (b, m) = 1$ és $n, s, t \in \mathbb{N}^*$, akkor

1) $a^n \equiv 1 \pmod m$ akkor és csak akkor ha $o(a)|n$,

2) $o(a)|\phi(m)$,

3) $a^s \equiv a^t \pmod m$ akkor és csak akkor ha $s \equiv t \pmod{o(a)}$,

★ 4) $o(a^n) = \frac{o(a)}{(o(a), n)}$,

5) $o(ab) \leq [o(a), o(b)]$ és ha $(o(a), o(b)) = 1$, akkor $o(ab) = o(a)o(b)$. ★

**Bizonyítás.** 1) Ha $a^n \equiv 1 \pmod m$ és $n = o(a)q + r, 0 \leq r < o(a)$, akkor $a^n = (a^{o(a)})^q a^r \equiv a^r \pmod m$, így $a^r \equiv 1 \pmod m$ és a definíció alapján következik, hogy $r = 0$, azaz $o(a)|n$. Fordítva, ha $o(a)|n$, akkor $a^n = (a^{o(a)})^{n/o(a)} \equiv 1 \pmod m$.

2) Következik az Euler tételből és az 1) tulajdonságból.

3) Feltehető, hogy $s \geq t$, ekkor $a^s \equiv a^t \pmod m \Leftrightarrow a^{s-t} \equiv 1 \pmod m \Leftrightarrow o(a)|s - t \Leftrightarrow s \equiv t \pmod{o(a)}$, felhasználva (1)-et.

★ 4) Legyen $o(a) = k$ és $o(a^n) = l$, továbbá $(k, n) = d$, így $k = dk_1, n = dn_1, (k_1, n_1) = 1$ és $(a^n)^{k_1} = a^{dn_1 k_1} = (a^k)^{n_1} \equiv 1 \pmod m$, ahonnan 1) alkalmazásával $l|k_1$.

Másrészt, $(a^n)^l = a^{nl} \equiv 1 \pmod m$, s innen szintén 1) alapján $k|nl, dk_1|dn_1 l, k_1|n_1 l$, s mivel $(k_1, n_1) = 1$ következik, hogy $k_1|l$. Az előbbiek szerint $l = k_1 = \frac{k}{d} = \frac{k}{(k,n)}$, amit bizonyítani kellett.

5) Legyen $o(a) = k$ és $o(b) = j$, akkor

$$(ab)^{[k,j]} = (a^k)^{\frac{[k,j]}{k}}(b^j)^{\frac{[k,j]}{j}} \equiv 1 \pmod{m},$$

ahol a kitevők egész számok és kapjuk, hogy $o(ab) \leq [k,j]$, pontosabban $o(ab)|[k,j] = [o(a), o(b)]$.

Most tegyük fel, hogy $(k,j) = 1$. Akkor $(ab)^{o(ab)} \equiv 1 \pmod{m}$, s hatványozva: $(ab)^{ko(ab)} = (a^k)^{o(ab)}b^{ko(ab)} \equiv b^{ko(ab)} \equiv 1 \pmod{m}$ és $(ab)^{jo(ab)} = a^{jo(ab)}(b^j)^{o(ab)} \equiv a^{jo(ab)} \equiv 1 \pmod{m}$. Így $o(b) = j|ko(ab), o(a) = k|jo(ab), j|o(ab), k|o(ab)$, mert $(k,j) = 1$ és innen $[k,j] = kj|o(ab)$.

A fentiek szerint $o(ab) = kj$. ★ □

**Tétel.** Ha $p$ prímszám, akkor minden olyan $k \in \mathbb{N}^*$ szám esetén, amelyre $k \mid p-1$ létezik olyan $a$ szám, melyre $o_p(a) = k$ és az ilyen $a$ számok száma (mod $p$) egyenlő $\phi(k)$-val.

★ **Bizonyítás.** Tekintsük az $1, 2, ..., p-1$ redukált maradékrendszert (mod $p$), jelölje ezt $R$, s legyen $f(d)$ azoknak az $a \in R$ elemeknek a száma, melyekre $o_p(a) = d$, ahol $d|\phi(p) = p-1$. Az $R$ minden elemének van rendje és a rend osztója $p-1$-nek, így $\sum_{d|p-1} f(d) = p-1$. Használva, hogy $\sum_{d|p-1} \phi(d) = p-1$ így $\sum_{d|p-1}(\phi(d) - f(d)) = 0$. Azt fogjuk megmutatni, hogy $f(d) \leq \phi(d)$, azaz $\phi(d) - f(d) \geq 0$ minden $d|p-1$ esetén. Ebből következni fog, hogy $\phi(d) - f(d) = 0, f(d) = \phi(d)$ minden $d|p-1$ esetén.

Tegyük fel, hogy $f(d) \geq 1$, tehát hogy létezik $a_0 \in R, o_p(a_0) = d$. Ekkor $a_0^d \equiv 1 \pmod{p}$, azaz $a_0$ megoldása az

$$x^d \equiv 1 \pmod{p} \tag{1}$$

kongruenciának. Akkor $1, a_0, a_0^2, ..., a_0^{d-1}$ mind megoldásai az (1) kongruenciának és páronként inkongruensek (mod $p$), lásd az előző Tételt. Így ezek adják (1) összes megoldásait, mert a Lagrange-tétel szerint a megoldások száma legfeljebb $d$.

Most legyen egy tetszőleges $a \in R$, amelyre $o_p(a) = d$. Akkor $a$ megoldása (1)-nek, tehát létezik $j, 0 \leq j \leq d-1$ úgy, hogy $a \equiv a_0^j \pmod{p}$. Az előző Tétel. /4) szerint $d = o_p(a) = o_p(a_0^j) = \frac{d}{(d,j)}$, ahonnan $(j,d) = 1$, tehát $j$ éppen $\phi(d)$ értéket vesz fel és így $f(d) = \phi(d)$.

Ezzel igazoltuk, hogy ha $f(d) \geq 1$, akkor $f(d) = \phi(d)$. Ha $f(d) = 0$, akkor nyilván $f(d) < \phi(d)$ és kapjuk, hogy $f(d) \leq \phi(d)$ igaz $p-1$ minden $d$ osztójára és ezzel a bizonyítás teljes. □★

**Definíció.** Legyen $(a,m) = 1$. Azt mondjuk, hogy $a$ **primitív gyök** (mod $m$) ha $o_m(a) = \phi(m)$.

Az előző Tételből a $k = p-1$ választással azonnal következik:

**Tétel.** Ha $p$ prímszám, akkor létezik primitív gyök (mod $p$) és a primitív gyökök száma (mod $p$) éppen $\phi(p-1)$.

**Példa.** • Határozzuk meg a primitív gyököket (mod 17).

Ezek száma $\phi(17-1) = \phi(16) = \phi(2^4) = 2^4(1-\frac{1}{2}) = 8$. Vegyük sorra az $1, 2, 3, ..., 16$ számokat és vizsgáljuk ezek rendjét (mod 17). A rend 16-nak osztója, tehát $1, 2, 4, 8, 16$ lehet. A jelen szakasz második Tétele szerint $\phi(1) = 1$ olyan szám van, amelynek a rendje 1 és ez az $a = 1$; $\phi(2) = 1$ olyan szám van, amelynek a rendje 2 és ez az $a = 16$, mert $16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$; $\phi(4) = 2$ olyan szám van, amelyek rendje 4 és ezek az $a = 4$ és $a = 13$, meghatározásuk történhet a következőképpen: olyan $a$-kat keresünk, amelyekre $a^4 \equiv 1 \pmod{17}$, azaz $17|a^4 - 1 = (a^2-1)(a^2+1)$ és $a^2 \not\equiv 1 \pmod{17}$, azaz $17 \not| a^2 - 1$,

ahonnan $17|a^2+1$. Biztosan jó $a=4$ és $a=-4$, ahol $-4\equiv 13 \pmod{17}$ és több nincs. Hasonlóképpen $\phi(8)=4$ olyan szám van, amelyek rendje 8 és ezek $a=2,15,8,9$. A többi szám rendje 16, ezek lesznek a primitív gyökök (mod 17): $a=3,5,6,7,10,11,12,14$.

Vajon minden $m$-re létezik primitív gyök (mod $m$)? Erre válasz a következő tétel, amelyet bizonyítás nélkül adunk meg.

**Tétel.** Akkor és csak akkor létezik primitív gyök (mod $m$), ha $m=1, m=2, m=4, m=p^a$ vagy $m=2p^a$ alakú, ahol $p\geq 3$ prímszám és $a\in\mathbb{N}$. □

Innen azonnal kapjuk a jelen szakasz első Tétele /3 alapján:

**Tétel.** Ha $(g,m)=1$ és $g$ primitív gyök (mod $m$), akkor $g, g^2, g^3, ..., g^{\phi(m)}$ egy redukált maradékrendszer (mod $m$).

**Definíció.** Ha $(a,m)=1$ és ha $g$ primitív gyök (mod $m$), akkor azt a $j\in\{1,2,...,\phi(m)\}$ kitevőt, amelyre $g^j\equiv a \pmod{m}$ az $a$ szám $g$ alapú **indexé**nek nevezzük (mod $m$), jelölés $j=\operatorname{ind}_g a \pmod{m} = \operatorname{ind}_g a$. Az előző Tétel. szerint minden $m$-hez relatív prím számnak létezik indexe és

$$g^{\operatorname{ind}_g a}\equiv a \pmod{m}.$$

**Tétel.** (Az index tulajdonságai) Ha $(a,m)=(b,m)=1, k\geq 1$ és $g$ egy primitív gyök (mod $m$), akkor

1) $\operatorname{ind}_g ab \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(m)}$,

2) $\operatorname{ind}_g a^k \equiv k \operatorname{ind}_g a \pmod{\phi(m)}$,

★ 3)

$$o_m(a)=\frac{\phi(m)}{(\operatorname{ind}_g a, \phi(m))}. \quad ★$$

**Bizonyítás.** 1) A definíció alapján $g^{\operatorname{ind}_g ab}\equiv ab \pmod{m}$. Ugyanakkor $g^{\operatorname{ind}_g a}\equiv a \pmod{m}$, $g^{\operatorname{ind}_g b}\equiv b \pmod{m}$, s ezeket összeszorozva $g^{\operatorname{ind}_g a+\operatorname{ind}_g b}\equiv ab \pmod{m}$. Kapjuk, hogy $g^{\operatorname{ind}_g ab}\equiv g^{\operatorname{ind}_g a+\operatorname{ind}_g b} \pmod{m}$, ahonnan $\operatorname{ind}_g ab \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(m)}$, lásd a szakasz első Tétele /3).

★ 3) Alkalmazzuk a szakasz első Tétele /4) pontját az $a=g, n=\operatorname{ind}_g a$ választással, ahol $o_m(g)=\phi(m)$. Kapjuk, hogy $o_m(g^{\operatorname{ind}_g a})=o_m(a)=\frac{\phi(m)}{(\operatorname{ind}_g a,\phi(m))}$. ★ □

Az indexre vonatkozó fenti szabályok emlékeztetnek a logaritmussal való számolás szabályaira, ezért az indexet **diszkrét logaritmus**nak is szokás nevezni.

**Példa.** • Készítsünk indextáblázatot (mod 17) ha $g=3$, amely a legkisebb pozitív primitív gyök (mod 17).

Sorra kiszámítjuk $3, 3^2, 3^3, ..., 3^{16}$-nak 17-tel való osztási maradékait: $3\equiv 3 \pmod{17}$, $3^2\equiv 9 \pmod{17}$, $3^3\equiv 27\equiv 10 \pmod{17}$, $3^4\equiv 3\cdot 3^3\equiv 3\cdot 10\equiv 30\equiv 13 \pmod{17}$, $3^5\equiv 3\cdot 3^4\equiv 3\cdot 13\equiv 39\equiv 5 \pmod{17}$,... és az eredményeket a következő táblázatba foglaljuk:

| Index | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Szám | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

Például $\operatorname{ind}_3 9=2, \operatorname{ind}_3 11=7$.

Célszerű a táblázatot $a$ értékei szerint is átrendezni:

| Szám | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Index | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |

Például $\operatorname{ind}_3 11 = 7, \operatorname{ind}_3 14 = 9$. Hasonló indextáblázatok készíthetők más modulus és más $g$ értékekkel is.

### 3.6. Binom kongruenciák

**Definíció. Binom (kéttagú) kongruenciák**nak nevezzük az $ax^k \equiv b \pmod m$ alakú kongruenciákat.

Ezek visszavezethetők

$$(*) \qquad x^k \equiv c \pmod m$$

alakú kongruenciákra, így elegendő ez utóbbiakkal foglalkoznunk. Valóban, legyen $(a, m) = d, a = da_1, m = dm_1, (a_1, m_1) = 1$, így annak szükséges feltétele, hogy legyen megoldás az, hogy $d|b, b = db_1$, és ekkor $da_1x^k \equiv db_1 \pmod{dm_1}$, $a_1x^k \equiv b_1 \pmod{m_1}$, amelyet $a_1^{\phi(m_1)-1}$-nel szorozva és használva az Euler tételt $x^k \equiv a_1^{\phi(m_1)-1}b_1 \pmod{m_1}$, amely (*) alakú kongruencia.

Először azt az esetet vizsgáljuk amikor $m = p$ prímszám. A $c$ helyett $a$-t írva nézzük tehát az

$$x^k \equiv a \pmod p$$

alakú kongruenciákat.

**Tétel.** Legyen $p$ prímszám, $(a, p) = 1$ és $d = (k, p-1)$. Akkor az $x^k \equiv a \pmod p$ kongruenciának

a) van megoldása és a megoldások száma $d$, ha $a^{\frac{p-1}{d}} \equiv 1 \pmod p \Leftrightarrow d|\operatorname{ind}_g a$,

b) nincs megoldása, ha $a^{\frac{p-1}{d}} \not\equiv 1 \pmod p \Leftrightarrow d \not| \operatorname{ind}_g a$,

ahol $g$ tetszőleges primitív gyök (mod $p$).

**Bizonyítás.** A megoldást keressük $x \equiv g^{\operatorname{ind}_g x} \pmod p$ alakban. Így $g^{k \operatorname{ind}_g x} \equiv g^{\operatorname{ind}_g a} \pmod p$ és a 3.5. szakasz első Tétel /3) szerint ez egyenértékű a következővel:

$$k \operatorname*{ind}_g x \equiv \operatorname*{ind}_g a \pmod{p-1}.$$

Ez $\operatorname{ind}_g x$-ben egy elsőfokú kongruencia és a megoldhatóság feltétele az, hogy

$$d = (k, p-1) | \operatorname*{ind}_g a,$$

és ekkor $\operatorname{ind}_g x$-re $d$ megoldás van, ami $x$-re is $d$ inkongruens megoldást ad (mod $p$).

★ Most igazoljuk, hogy a $d|\operatorname{ind}_g a$ feltétel egyenértékű az $a^{\frac{p-1}{d}} \equiv 1 \pmod p$ feltétellel:

$$d = (k, p-1) | \operatorname*{ind}_g a \Leftrightarrow (k, p-1) | (\operatorname*{ind}_g a, p-1) \Leftrightarrow \frac{p-1}{(\operatorname{ind}_g a, p-1)} | \frac{p-1}{(k, p-1)}$$

$$\Leftrightarrow o_p(a) | \frac{p-1}{(k, p-1)} = \frac{p-1}{d} \Leftrightarrow a^{\frac{p-1}{d}} \equiv 1 \pmod p,$$

használva az index tulajdonságait és a 20.3. szakasz első Tétel 1) pontját. ★ □

**Példa.** Oldjuk meg az $x^{11} \equiv 6 \pmod{17}$ binom kongruenciát a (mod 17) indextáblázatokat használva.

Az előző Tétel bizonyítási módszere szerint mindkét oldalt a $g = 3$ primitív gyök hatványaként felírva:

$$3^{11 \operatorname{ind}_3 x} \equiv 3^{\operatorname{ind}_3 6} \pmod{17},$$

ahonnan $11 \operatorname{ind}_3 x \equiv \operatorname{ind}_3 6 \pmod{16}$. A táblázat szerint $\operatorname{ind}_3 6 = 15$, így $11 \operatorname{ind}_3 x \equiv 15 \pmod{16}$. Itt $(11, 16) = 1$, tehát ennek az $\operatorname{ind}_3 x$-ben lineáris kongruenciának 1 megoldása van: $-5 \operatorname{ind}_3 x \equiv 15 \pmod{16}$, s $-5$-tel osztva $\operatorname{ind}_3 x \equiv -3 \equiv 13 \pmod{16}$. A táblázatból kapjuk, hogy $x \equiv 12 \pmod{17}$. □

Igazolható a következő tétel.

**Tétel.** Ha $p > 2$ prímszám, $k \in \mathbb{N}^*, p \nmid k, (a, p) = 1$ és $i \in \mathbb{N}^*$, akkor az $x^k \equiv a \pmod{p^i}$ prímhatványmodulusú kongruenciának akkor és csak akkor van megoldása, ha az $x^k \equiv a \pmod{p}$ prímmodulusú kongruenciának van megoldása és ekkor a megoldások száma $d = (k, p-1)$. □

**Feladat.** ▼ A (mod 17) indextáblázatokat használva oldjuk meg az alábbi kongruenciákat:

a) $7x^{10} \equiv 12 \pmod{17}$, b) $x^9 \equiv 4 \pmod{17}$, c) $9x \equiv 14 \pmod{17}$, d) $5^x \equiv 12 \pmod{17}$, e) $5 \cdot 6^x \equiv 7 \pmod{17}$.

### 3.7. Számelméleti függvények

**Definíció. Számelméleti függvény**nek nevezünk minden $f : \mathbb{N}^* \to \mathbb{C}$ függvényt, ahol $\mathbb{C}$ a komplex számok halmaza, a számelméleti függvények halmazát $\mathcal{F}$-fel jelöljük.

Ez az definíció megegyezik a komplex számsorozatok definíciójával. Elsősorban azok a függvények érdekelnek bennünket, amelyek valamely számelméleti fogalomhoz kapcsolódnak.

Ilyen számelméleti függvények például a $\tau$ és $\phi$, ahol $\tau(n) = \sum_{d|n} 1$ az $n$ szám pozitív osztóinak a száma, $\phi$ az Euler-függvény, lásd 3.1. szakasz. Ilyen a $\sigma$ függvény is, ahol $\sigma(n) = \sum_{d|n} d$ az $n$ pozitív osztóinak az összege.

**Definíció.** Legyen $f \in \mathcal{F}$ egy számelméleti függvény. Azt mondjuk, hogy

i) $f$ **multiplikatív**, ha minden $m, n \in \mathbb{N}^*, (m, n) = 1$ esetén $f(mn) = f(m)f(n)$,

ii) $f$ **teljesen multiplikatív** ha minden $m, n \in \mathbb{N}^*$ számpárra $f(mn) = f(m)f(n)$.

Ha $f$ teljesen multiplikatív, akkor $f$ multiplikatív és fordítva nem.

**Tétel.** Ha $f \in \mathcal{F}$ nem azonosan nulla multiplikatív függvény, akkor $f(1) = 1$.

**Bizonyítás.** Létezik olyan $n_0 \in \mathbb{N}$, amelyre $f(n_0) \neq 0$ és így a multiplikativitás alapján $f(n_0) = f(1 \cdot n_0) = f(1)f(n_0)$, ahonnan $f(1) = 1$. □

Legyen a továbbiakban $n > 1$ kanonikus alakja

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}.$$

**Tétel.** Ha $f$ multiplikatív függvény, akkor $f$ értékeit elegendő a prímhatványokra ismerni:

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) ... f(p_r^{a_r}).$$

**Bizonyítás.** Valóban, a multiplikativitás alapján

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2} ... p_r^{a_r}) = f(p_1^{a_1}) f(p_2^{a_2}) f(p_3^{a_3} ... p_r^{a_r}) = ... = f(p_1^{a_1}) f(p_2^{a_2}) ... f(p_r^{a_r}). \square$$

**Tétel.** Ha $f$ teljesen multiplikatív függvény, akkor $f$ értékeit elegendő a prímszámokra ismerni:

$$f(n) = f(p_1)^{a_1} f(p_2)^{a_2} ... f(p_r)^{a_r}.$$

**Bizonyítás.** Ha $p^a$ prímhatvány, akkor $f(p^a) = f(p)f(p^{a-1}) = (f(p))^2 f(p^{a-2}) = ... = (f(p))^a$ és alkalmazzuk az előző Tételt. □

**Definíció.** Ha $f \in \mathcal{F}$, akkor a

$$g(n) = \sum_{d|n} f(d), \quad n \in \mathbb{N}^*$$

képlettel definiált $g$ függvényt, ahol az összegzés $n$ pozitív $d$ osztóira vonatkozik, az $f$ **összegzési függvény**ének nevezzük.

**Tétel.** Ha $f$ multiplikatív függvény, akkor $f$ összegzési függvénye is multiplikatív.

Ez az állítás következik az alábbi általánosabb tételből.

**Tétel.** Ha $f$ és $g$ multiplikatív függvények és

$$h(n) = \sum_{d|n} f(d)g(n/d), \quad n \in \mathbb{N}^*,$$

akkor $h$ is multiplikatív.

**Bizonyítás.** Legyen $m, n \in \mathbb{N}^*, (m, n) = 1$, akkor az $mn$ minden $d$ osztója felírható egyértelműen $d = d_1 d_2$ alakban, ahol $d_1|m, d_2|n$. Így

$$h(mn) = \sum_{d|mn} f(d)g(n/d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2)g(mn/d_1 d_2).$$

Itt $(d_1, d_2) = 1$ és $(m/d_1, n/d_2) = 1$, és használva, hogy $f$ és $g$ multiplikatív kapjuk, hogy

$$h(mn) = \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2)g(m/d_1)g(n/d_2)$$

$$= \sum_{d_1|m} f(d_1)g(m/d_1) \sum_{d_2|n} f(d_2)g(n/d_2) = h(m)h(n).\square$$

Ha ebben a Tételben $g(n) = 1, n \in \mathbb{N}^*$, akkor $h$ az $f$ összegzési függvénye és az ezt megelőző Tételt kapjuk.

Ha $s \in \mathbb{R}$ adott szám, akkor legyen $\sigma_s(n) = \sum_{d|n} d^s$ az $n$ pozitív osztóinak $s$-edik hatványösszege. Ha $s = 1$, akkor $\sigma_1(n) = \sigma(n) = \sum_{d|n} d$ az $n$ osztóinak összege, ha pedig $s = 0$, akkor $\sigma_0(n) = \tau(n)$ az $n$ osztóinak száma.

**Tétel.** A $\sigma_s, \sigma, \tau$ függvények multiplikatívak és

$$\sigma_s(n) = \frac{p_1^{s(a_1+1)} - 1}{p_1^s - 1} ... \frac{p_r^{s(a_r+1)} - 1}{p_r^s - 1}, \quad s \neq 0,$$

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} ... \frac{p_r^{a_r+1} - 1}{p_r - 1},$$

$$\tau(n) = (a_1 + 1)...(a_r + 1).$$

**Bizonyítás.** Az $f(n) = n^s$ függvény multiplikatív (sőt teljesen multiplikatív) és így ennek összegzési függvénye, a $\sigma_s$ is multiplikatív Tétel szerint. Elegendő $\sigma_s(p^a)$ meghatározása, ahol $p^a$ egy prímhatvány. Azt kapjuk, hogy

$$\sigma_s(p^a) = 1 + p^s + p^{2s} + ... + p^{as} = \frac{p^{s(a+1)} - 1}{p^s - 1}, \quad s \neq 0,$$

a mértani sorozat összegzési képlete szerint. Ha $s = 0$, akkor $\sigma_0(p^a) = \tau(p^a) = a + 1$. □

A $\sigma_s, \sigma, \tau$ függvények nem teljesen multiplikatívak, például $\tau(4) = 3 \neq 2 \cdot 2 = \tau(2)\tau(2)$.

**Definíció.** Az $n \in \mathbb{N}^*$ számot **tökéletes szám**nak nevezzük ha $n$ egyenlő az önmagánál kisebb pozitív osztóinak összegével, azaz ha $\sigma(n) = 2n$.

Például $n = 6$ és $n = 28$ tökéletes számok, mert $6 = 1+2+3$ és $28 = 1+2+4+7+14$, illetve $\sigma(6) = 1+2+3+6 = 2 \cdot 6 = 12$ és $\sigma(28) = 1+2+4+7+14+28 = 2 \cdot 28 = 56$.

**Tétel.** (Euklidész) Ha $2^k - 1$ prímszám, akkor $n = 2^{k-1}(2^k - 1)$ tökéletes szám.

**Bizonyítás.** A $\sigma$ függvény multiplikativitása alapján
$\sigma(n) = \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)(1 + 2^k - 1) = 2^k(2^k - 1) = 2n$.
□

**Tétel.** (Euler) Ha $n$ páros tökéletes szám, akkor $n = 2^{k-1}(2^k - 1)$ alakú, ahol $2^k - 1$ prímszám.

★ **Bizonyítás.** Legyen $n = 2^a m$, ahol $a \geq 1$ és $m$ páratlan. Így $\sigma(n) = \sigma(2^a m) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m)$ és innen $\sigma(n) = 2n$ alapján $(2^{a+1} - 1)\sigma(m) = 2^{a+1}m$. Következik, hogy $2^{a+1} - 1 | 2^{a+1}m$ és mivel $(2^{a+1} - 1, 2^{a+1}) = 1$ kapjuk, hogy $2^{a+1} - 1 | m$, azaz $m = (2^{a+1} - 1)m_1$, amit visszahelyettesítve: $(2^{a+1} - 1)\sigma(m) = (2^{a+1} - 1)2^{a+1}m_1$, ahonnan $\sigma(m) = 2^{a+1}m_1$. Az $m_1$ és $m$ osztói $m$-nek, $m_1 < m$ és $m_1 + m = m_1 + (2^{a+1} - 1)m_1 = 2^{a+1}m_1 = \sigma(m)$. Így $m$-nek $m_1$-en és $m$-en kívül nincs más osztója és kapjuk, hogy $m_1 = 1$ és $m = 2^{a+1} - 1$ prímszám. Tehát az $a = k - 1$ jelöléssel $n = 2^{k-1}(2^k - 1)$, ahol $2^k - 1$ prímszám. □★

Így $n$ akkor és csak akkor páros tökéletes szám, ha $n = 2^{p-1}M_p$ alakú, ahol $M_p$ Mersenne-prím. További tökéletes számok $n = 2^3 M_5 = 496, 2^6 M_7 = 8128$. Jelenleg (2006. április) 43 tökéletes szám ismert annak megfelelően, hogy 42 Mersenne-prímet ismerünk. Nem tudjuk, hogy létezik-e végtelen sok Mersenne-féle prímszám, így azt sem tudjuk, hogy van-e végtelen sok tökéletes szám. Arra a kérdésre sem ismerjük a választ, hogy létezik-e páratlan tökéletes szám.

Most az Euler-féle $\phi$ függvényt vizsgáljuk.

**Tétel.** a) A $\phi$ függvény multiplikatív, azaz minden $m, n \in \mathbb{N}^*, (m, n) = 1$ esetén $\phi(mn) = \phi(m)\phi(n)$.

b) Ha $n$ kanonikus alakja $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$, akkor

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_r}\right).$$

**Bizonyítás.** a) Rendezzük az $1, 2, 3, ..., mn$ számokat a következő táblázatba:

| | | | | |
|---|---|---|---|---|
| $1$ | $2$ | $3$ | ... | $m$ |
| $m+1$ | $m+2$ | $m+3$ | ... | $2m$ |
| $2m+1$ | $2m+2$ | $2m+3$ | ... | $3m$ |
| ... | ... | ... | ... | ... |
| $(n-1)m+1$ | $(n-1)m+2$ | $(n-1)m+3$ | ... | $nm$ |

Számoljuk le kétféleképpen a táblázat $mn$-hez relatív prím $k$ számait. Ezek száma egyrészt $\phi(mn)$, az Euler függvény definíciója szerint.

Másrészt, $(k, mn) = 1 \Leftrightarrow (k, m) = 1$ és $(k, n) = 1$ (lásd Tétel). Válasszuk ki először az $m$-hez relatív prímeket. A táblázat mindegyik sora egy-egy teljes maradékrendszer (mod $m$), így mindegyik sor $\phi(m)$ számú $m$-hez relatív prím számot tartalmaz úgy, hogy ha egy

szám $m$-hez relatív prím, akkor annak oszlopában mindegyik szám $m$-hez relatív prím (▼ Igazoljuk!). Most ezek közül válasszuk ki az $n$-hez relatív prímeket. Mindegyik oszlop egy-egy teljes maradékrendszer (mod $n$), ahol $(m,n)=1$, lásd Tétel, így mindegyik oszlopban $\phi(n)$ szám relatív prím $n$-hez. Kapjuk, hogy a keresett szám $\phi(m)\phi(n)$.

b) Az a) alapján

$$\phi(n)=\phi(p_1^{a_1}p_2^{a_2}...p_r^{a_r})=\phi(p_1^{a_1})\phi(p_2^{a_2}...p_r^{a_r})=...=\phi(p_1^{a_1})\phi(p_2^{a_2})...\phi(p_r^{a_r}).$$

Így elegendő $\phi(p^a)$ meghatározása, ahol $p^a$ egy prímhatvány. Az $1,2,3,...,p^a$ számok közül a $p^a$-hoz nem relatív prímek a $p,2p,3p,...,p^{a-1}p=p^a$, ezek száma $p^{a-1}$, így a $p^a$-nal relatív prímek száma $p^a-p^{a-1}=p^a(1-1/p)$.

Kapjuk, hogy

$$\phi(n)=p_1^{a_1}(1-1/p_1)p_2^{a_2}(1-1/p_2)...p_r^{a_r}(1-1/p_r)=$$

$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_r}\right).\square$$

**Megjegyzés.** Használatos a következő jelölés:

$$\phi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

ahol a szorzat az $n$ összes $p$ prímosztójára vonatkozik.

**Tétel.** Minden $n\in\mathbb{N}$ esetén

$$\sum_{d|n}\phi(d)=n,$$

ahol az összegzés $n$ pozitív $d$ osztóira vonatkozik.

**Bizonyítás.** Tekintsük az $\frac{1}{n},\frac{2}{n},\frac{3}{n},...,\frac{n}{n}$ törteket, ezek száma $n$. Ugyanakkor, egyszerűsítve mindegyik tört $\frac{k}{d}$ alakú lesz, ahol $d|n$ és $(k,d)=1, k\le d$. Az $n$ minden $d$ pozitív osztója esetén lesz $d$ nevezőjű tört és az ugyanolyan $d$ nevezőjű törtek száma $\phi(d)$. Így a törtek száma összesen $\sum_{d|n}\phi(d)$, s ezzel bizonyítottuk a képletet. $\square$

**Feladatok**

▼ 1. Határozzuk meg a $\tau(n),\sigma(n)$ és $\phi(n)$ értékeket, ahol $n=12$, $n=24$, $n=120$, illetve $n=p^2q^3$, $p\ne q$ prímek.

▼ 2. Legyenek $f$ és $g$ multiplikatív függvények. Vizsgáljuk, hogy multiplikatív-e az $fg$ szorzatfüggvény és az $f+g$ összegfüggvény.

▼ 3. Lehet-e prímszám vagy prímhatvány tökéletes szám?

▼ 4. Igazoljuk, hogy $n$ akkor és csak akkor tökéletes szám, ha $n$ osztói reciprokainak az összege 2.

▼ 5. Igazoljuk, hogy ha $n$ páros tökéletes szám, akkor $n$ utolsó számjegye (10-es számrendszerben) 6 vagy 8.

▼ 6. Igazoljuk, hogy minden $m,n\ge 1$ esetén $\tau(mn)\le\tau(m)\tau(n)$.

Mikor áll fenn az egyenlőség?

▼ 7. Igazoljuk, hogy minden $n\ge 1$-re $\phi(n^2)=n\phi(n)$.

**Definíció.** Legyen $f\in\mathcal{F}$ egy számelméleti függvény. Azt mondjuk, hogy

i) $f$ **additív**, ha minden $m,n\in\mathbb{N}^*,(m,n)=1$ esetén $f(mn)=f(m)+f(n)$,

ii) $f$ **teljesen additív**, ha minden $m,n\in\mathbb{N}^*$ számpárra $f(mn)=f(m)+f(n)$.

Ha $f$ teljesen additív, akkor $f$ additív, és fordítva nem.

Definiáljuk az $\omega$ és $\Omega$ függvényeket a következőképpen. Legyen $\omega(1) = \Omega(1) = 0$ és ha $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} > 1$, akkor legyen $\omega(n) = r$ az $n$ különböző prímosztóinak száma és $\Omega(n) = a_1 + a_2 + ... + a_r$ az $n$ különböző prímhatvány osztóinak száma.

**Tétel.** Az $\omega$ függvény additív, $\Omega$ pedig teljesen additív.

**Bizonyítás.** Ha $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, $m = q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s}$ és $(n,m) = 1$, akkor $nm$ kanonikus alakja $nm = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s}$ és $\omega(nm) = r+s = \omega(n)+\omega(m)$. Továbbá minden $n, m$ esetén $\Omega(nm) = a_1 + a_2 + ... + a_r + b_1 + b_2 + ... + b_s = \Omega(n) + \Omega(m)$. □

Az $\omega$ nem teljesen additív, mert például $\omega(12) = \omega(2^2\cdot 3) = 2 \neq 3 = 2+1 = \omega(2\cdot 3)+\omega(2)$.

További fontos példa a logaritmusfüggvény, amely teljesen additív. Nézzük az additív függvények tulajdonságait.

**Tétel.** Ha $f \in \mathcal{F}$ additív függvény, akkor $f(1) = 0$.

**Bizonyítás.** Valóban, $f(1) = f(1\cdot 1) = f(1) + f(1)$ alapján $f(1) = 0$. □

Legyen a továbbiakban $n > 1$ kanonikus alakja $n = p_1^{a_1}p_2^{a_2}...p_r^{a_r}$.

**Tétel.** Ha $f$ additív függvény, akkor $f$ értékeit elegendő a prímhatványokra ismerni:

$$f(n) = f(p_1^{a_1}) + f(p_2^{a_2}) + ... + f(p_r^{a_r}).$$

**Bizonyítás.** Valóban, az additivitás alapján $f(n) = f(p_1^{a_1}) + f(p_2^{a_2}...p_r^{a_r}) =$

$$= f(p_1^{a_1}) + f(p_2^{a_2}) + f(p_3^{a_3}...p_r^{a_r}) = ... = f(p_1^{a_1}) + f(p_2^{a_2}) + ... + f(p_r^{a_r}).\square$$

**Tétel.** Ha $f$ teljesen additív függvény, akkor $f$ értékeit elegendő a prímszámokra ismerni:

$$f(n) = a_1 f(p_1) + a_2 f(p_2) + ... + a_r f(p_r).$$

**Bizonyítás.** Ha $p^a$ prímhatvány, akkor $f(p^a) = f(p) + f(p^{a-1}) = ... = af(p)$ és alkalmazzuk az előző Tételt. □

A multiplikativitás és additivitás kapcsolatára mutat rá a következő tétel.

**Tétel.** Ha $f$ additív, $g$ teljesen additív és $k \neq 0$ valós szám, akkor $F(n) = k^{f(n)}$ multiplikatív, $G(n) = k^{g(n)}$ pedig teljesen multiplikatív függvény.

Fordítva, ha $F$ multiplikatív, $G$ teljesen multiplikatív és pozitív értékű függvények, akkor $f(n) = \ln F(n)$ additív, $g(n) = \ln G(n)$ teljesen additív. □

**Feladatok.** ▼ Igazoljuk ezt tételt.

▼ Legyenek $f$ és $g$ additív függvények. Vizsgáljuk, hogy additív-e az $f + g$ összeg, az $f - g$ különbség és az $fg$ szorzatfüggvény.

▼ Igazoljuk, hogy $2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)}$ minden $n \geq 1$-re.

**Definíció. Möbius-függvény**nek nevezzük a

$$\mu(n) = \begin{cases} 1, \text{ ha } n = 1, \\ 0, \text{ ha létezik } p \text{ prím, amelyre } p^2|n, \\ (-1)^r, \text{ ha } n = p_1p_2...p_r, p_i \neq p_j \end{cases}$$

képlettel definiált függvényt. Például, $\mu(30) = \mu(2\cdot 3\cdot 5) = (-1)^3 = -1, \mu(12) = \mu(2^2\cdot 3) = 0, \mu(14) = \mu(2\cdot 7) = (-1)^2 = 1$. Megjegyezzük, hogy $|\mu(n)| = (\mu(n))^2 = 1$ akkor és csak akkor, ha $n$ négyzetmentes, azaz $n$ különböző prímek szorzata.

**Tétel.** $\mu$ multiplikatív függvény.

**Bizonyítás.** Igazoljuk, hogy $\mu(mn) = \mu(m)\mu(n)$ minden $m, n \in \mathbb{N}^*, (m, n) = 1$ esetén. Ha $m = n = 1$, akkor $\mu(mn) = \mu(1) = 1 = \mu(m)\mu(n)$. Ha $m = 1$ és $n \neq 1$, akkor $\mu(mn) = \mu(n) = 1 \cdot \mu(n) = \mu(m)\mu(n)$ (hasonlóan, ha $n = 1$ és $m \neq 1$). Ha $m \neq 1, n \neq 1$ és ha $m$ vagy $n$ nem négyzetmentes, azaz ha létezik $p$ prím úgy, hogy $p^2|m$ vagy $p^2|n$, akkor $p^2|mn$ és $\mu(mn) = 0 = \mu(m)\mu(n)$. Végül, ha $m$ is és $n$ is négyzetmentes, akkor legyen $m = p_1p_2...p_r$ és $n = q_1q_2...q_s, p_i \neq q_j$, akkor $\mu(mn) = \mu(p_1p_2...p_rq_1q_2...q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. □

**Tétel.** A Möbius-függvény összegzési függvénye

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ha } n = 1, \\ 0, & \text{ha } n > 1. \end{cases}$$

**Bizonyítás.** Legyen $F(n) = \sum_{d|n} \mu(d)$. Mivel $\mu$ multiplikatív, következik, hogy $F$ is multiplikatív függvény korábbi Tétel alapján. Ha $n = 1$, akkor $F(1) = \mu(1) = 1$. Legyen $n = p^a$ egy prímhatvány, akkor $F(p^a) = \sum_{d|p^a} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^a) = 1 - 1 + 0 + ... + 0 = 0$. Így, mivel $\mu$ multiplikatív, következik, hogy $F(n) = 0$. □

**Tétel.** (Möbius-féle megfordítási képlet) Ha $f, g \in \mathcal{F}$, akkor egyenértékűek a következő állítások:

1) $g(n) = \sum_{d|n} f(d)$ minden $n \in \mathbb{N}^*$ esetén,

2) $f(n) = \sum_{d|n} \mu(d)g(n/d)$ minden $n \in \mathbb{N}^*$ esetén.

**Bizonyítás.** Ha $g(n) = \sum_{d|n} f(d), n \in \mathbb{N}^*$, azaz ha $g$ az $f$ összegzési függvénye, akkor

$$\sum_{d|n} \mu(d)g(n/d) = \sum_{d|n} \left( \sum_{e|n/d} f(e) \right) = \sum_{e|n} f(e) \sum_{d|n/e} \mu(d) = f(n),$$

átcsoportosítva a kettős összeg tagjait és használva az előző Tételt, amely szerint

$$\sum_{d|n/e} \mu(d) = \begin{cases} 1, & \text{ha } e = n, \\ 0, & \text{ha } e < n. \end{cases}$$

Hasonlóképpen igazolható a másik implikáció is. □

Az Euler-függvény kifejezhető a Möbius-függvény segítségével:

**Tétel.** Minden $n \in \mathbb{N}^*$ esetén

$$\phi(n) = \sum_{d|n} d\mu(n/d) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

**Első bizonyítás.** Alkalmazzuk a Möbius-féle megfordítási képletet az $f(n) = \phi(n)$, $g(n) = n$ esetben.

★ **Második bizonyítás.** A Möbius-függvény tulajdonsága szerint

$$\phi(n) = \sum_{1 \leq k \leq n,\, (k,n)=1} 1 = \sum_{1 \leq k \leq n} \sum_{d|(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{d|k,\, d|n} \mu(d) = \sum_{d|n} \mu(d) \sum_{\ell=1}^{n/d} 1 = \sum_{d|n} \mu(d)(n/d),$$

ahol $k = d\ell$. ★ □

### 3.8. Számelméleti függvények konvolúciószorzása

**Definíció.** Az $f$ és $g$ függvények **konvolúciószorzat**a (Dirichlet-szorzata) az $f * g$ függvény, ahol

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{de=n} f(d)g(e), \quad n \in \mathbb{N}^*,$$

az összegzés itt $n$ pozitív $d$ osztóira vonatkozik, illetve mindazokra a $\langle d, e\rangle$ számpárokra, amelyekre $de = n$.

Legyen $E_s(n) = n^s, E_1(n) = E(n) = n, E_0(n) = U(n) = 1$,

$$\delta(n) = \begin{cases} 1, & \text{ha } n = 1, \\ 0, & \text{ha } n > 1. \end{cases}$$

Így a korábbiakban vizsgált függvényekre:

$$\sigma_s = U * E_s, \quad \sigma = U * E, \quad \tau = U * U, \quad \mu * U = \delta, \quad \phi = \mu * E.$$

Láttuk, hogy multiplikatív függvények konvolúciószorzata multiplikatív (előző szakasz, Tétel).

**Tétel.** (A konvolúció tulajdonságai) Ha $f, g, h$ tetszőleges számelméleti függvények, akkor

1) $f * g = g * f$ (kommutativitás),
2) $(f * g) * h = f * (g * h)$ (asszociativitás),
3) $f * \delta = f$ ($\delta$ egységelem),
4) $f * (g + h) = f * g + f * h$ (a konvolúció disztributív az összeadásra nézve),
5) $f * g \equiv 0 \Leftrightarrow f \equiv 0$ vagy $g \equiv 0$,
6) adott $f \in \mathcal{F}$ esetén akkor és csak akkor létezik $g \in \mathcal{F}$ úgy, hogy $f * g = \delta$, ha $f(1) \neq 0$, és ha létezik ilyen $g$, akkor az egyértelmű,

azaz $(\mathcal{F}, +, *)$ kommutatív, egységelemes, zérusosztómentes gyűrű (integritástartomány) és egy adott $f \in \mathcal{F}$ elemnek akkor és csak akkor létezik inverze, ha $f(1) \neq 0$.

**Bizonyítás.** 1), 3), 4) azonnali a definíció alapján. Továbbá,

$$((f * g) * h)(n) = \sum_{dd_3=n} (f * g)(d)h(d_3) = \sum_{dd_3=n} \left( \sum_{d_1d_2=d} f(d_1)g(d_2) \right) h(d_3)$$

$$= \sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3),$$

ahol az összegzés mindazokra a $\langle d_1, d_2, d_3\rangle$ számhármasokra vonatkozik, amelyekre $d_1d_2d_3 = n$ és $(f * (g * h))(n)$-et ugyanez az összeg adja, innen következik 2).

5) igazolása érdekében megmutatjuk, hogy ha $f \not\equiv 0$ és $g \not\equiv 0$, akkor $f * g \not\equiv 0$. Legyen $m_0$ a legkisebb olyan szám, melyre $f(m_0) \neq 0$ és legyen $n_0$ a legkisebb olyan szám, melyre $g(n_0) \neq 0$. Akkor

$$(f * g)(m_0n_0) = \sum_{de=m_0n_0} f(d)g(e) = f(m_0)g(n_0) \neq 0,$$

itt ha $d < m_0$, akkor $f(d) = 0$, ha $d > m_0$, $e < n_0$ és $g(d) = 0$, tehát az összeg minden tagja nulla, kivéve az $f(m_0)g(n_0)$ tagot.

6) Tegyük fel, hogy $f \in \mathcal{F}$ esetén létezik $g \in \mathcal{F}$ úgy, hogy $f * g = \delta$. Akkor $n = 1$-re $f(1)g(1) = 1$, s innen $f(1) \neq 0$.

Ha $f(1) \neq 0$, akkor olyan $g$ függvényt keresünk, melyre $f * g = \delta$, azaz $f(1)g(1) = 1$ és ha $n > 1$, akkor

$$(f * g)(n) = \sum_{de=n} f(d)g(e) = f(1)g(n) + \sum_{d|n,\, d>1} f(d)g(n/d) = 0.$$

Legyen $g(1) = 1/f(1)$ és rekurzív módon minden $n > 1$-re

$$(**) \quad g(n) = -\frac{1}{f(1)} \sum_{d|n,\, d>1} f(d)g(n/d) = 0,$$

itt $n/d < n$, így ha ismert $g(k)$ értéke minden $k < n$-re, akkor (**) alapján $g(n)$ meghatározott. □

**Megjegyzés.** $(\mathcal{F}, +, \cdot)$ kommutatív, egységelemes gyűrű, de itt vannak zérusosztók. A konvolúció valódi függvény-művelet, $(f * g)(n)$ kiszámításához nem elegendő $f(n)$ és $g(n)$ ismerete. □

Legyen $\mathcal{F}_1 = \{f \in \mathcal{F} : f(1) \neq 0\}$ és legyen $\mathcal{MF}$ a nem azonosan nulla multiplikatív függvények halmaza. Akkor

**Tétel.** Az $(\mathcal{F}_1, *)$ struktúra kommutatív csoport és $(\mathcal{MF}, *)$ ennek részcsoportja.

Bizonyítás. Az első tulajdonság azonnali az előző Tétel alapján (ha $f, g \in \mathcal{F}_1$, akkor $f * g \in \mathcal{F}_1$, mert $(f * g)(1) = f(1)g(1) \neq 0$). Ha $f, g \in \mathcal{MF}$, akkor $f * g \in \mathcal{MF}$, lásd előző szakasz, Tétel.

★ Még azt kell igazolnunk, hogy ha $f$ multiplikatív és $f * g = \delta$, akkor $g = f^{-1}$ (azaz $f$ konvolúcióinverze) is multiplikatív.

Definiáljuk a $h$ multiplikatív függvényt a következőképpen: $h(p^a) = f^{-1}(p^a)$ minden $p^a$ prímhatványra és mivel azt akarjuk, hogy $h$ multiplikatív legyen, ha $n = \prod p^a$, akkor legyen $h(n) = \prod f^{-1}(p^a)$. Az $f$ és $h$ függvények multiplikativak, ezért $f * h$ is multiplikatív. Továbbá minden $p^a$ prímhatványra

$$(f * h)(p^a) = \sum_{de=p^a} f(d)h(e) = \sum_{de=p^a} f(d)f^{-1}(e) = (f * f^{-1})(p^a) = \delta(p^a).$$

Így $f * h = \delta$, s mivel az inverz egyértelmű, következik, hogy $f^{-1} = h$ és $f^{-1}$ multiplikatív. ★ □

**Megjegyzés.** A $\mu * U = \delta$ összefüggés alapján következik, hogy a kissé „furcsa” $\mu$ függvény a „szép” $U$ függvény konvolúcióinverze, s ennek alapján új, átláthatóbb bizonyítás adható a Möbius-féle megfordítási képletre:

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow g = f * U \Leftrightarrow g * \mu = (f * U) * \mu$$

$$\Leftrightarrow g * \mu = f * (U * \mu) \Leftrightarrow g * \mu = f * \delta \Leftrightarrow g * \mu = f \Leftrightarrow f(n) = \sum_{d|n} \mu(d)g(n/d). \square$$

**Feladat.** ▼ Igazoljuk, hogy minden $n \geq 1$-re

$$a) \quad \sum_{d|n} \mu(d)\sigma(n/d) = n, \qquad b) \quad \sum_{d|n} \sigma(d) = n \sum_{d|n} \frac{\tau(d)}{d},$$

$$c) \quad \sum_{d|n} \mu(d)\tau(n/d) = 1, \qquad d) \quad \sum_{d|n} \tau^2(d)\mu(n/d) = \sum_{d|n} \mu^2(d)\tau(n/d).$$

**Tartalomjegyzék**



2006. ápr. 4.