4. Algebrai Módszerek Klasszikus Eredmények Igazolásában, Út az Algebrai Számelmélet felé

4.1. Maradékosztálygyűrűk egységcsoportjai szerkezete.

Jelölés. Tetszőleges $n > 1$ egészre jelölje $\mathcal{U}_n$ a $\mathbb{Z}_n$ maradékosztálygyűrű egységei (invertálható elemei) csoportját. Elemeiket a maradékosztályok legkisebb nemnegatív reprezentánsaival fogjuk jelölni.

Megjegyzés. Tudjuk, hogy $|\mathcal{U}_n| = \varphi(n)$, de például $\mathcal{U}_5$ és $\mathcal{U}_8$ egyaránt 4 elemű, ám nem izomorfak, hiszen az előbbi ciklikus, míg az utóbbi $C_2 \times C_2$-vel izomorf (az ún. Klein-féle négyes csoporttal).

4.1.1. Tétel. *Ha valamely $n > 1$ egészre $\mathcal{U}_n$ ciklikus, akkor generátor elemei primitív gyökök modulo n.*

Célunk az lesz, hogy meghatározzuk azon $n > 1$ egészeket, amelyekre az $\mathcal{U}_n$ csoport ciklikus, ami egyenértékű azzal, hogy meghatározzuk, hogy mely $n > 1$-re van primitív gyök modulo n.

4.1.2. Lemma. *Valamely $a \in \mathcal{U}_n$ pontosan akkor primitív gyök modulo n, ha $\varphi(n)$ minden q prímosztójára $a^{\frac{\varphi(n)}{q}} \neq 1$.*

Bizonyítás. Ha $a \in \mathcal{U}_n$ primitív gyök modulo n, akkor $\mathrm{o}_n(a) = \varphi(n)$, és így $a^k \neq 1$ minden $1 \leq k < \varphi(n)$-re, speciálisan akkor is, ha $k = \varphi(n)/q$ valamely q prímosztóra.

Ha pedig a nem primitív gyök, akkor az ő k rendje valódi osztója $\varphi(n)$-nek, így $\varphi(n)/k > 1$. Ha most q egy prímfaktora $\varphi(n)/k$-nak, akkor $k|\varphi(n)/q$, amiből $a^{\frac{\varphi(n)}{q}} = 1$ adódik $\mathcal{U}_n$-ben. Ez ellentmond a lemma föltételének.

Példák.

(1) Vizsgáljuk meg, hogy $a = 2$ primitív gyök-e modulo 11. $\varphi(11) = 10$, amelynek két prímosztója 2 és 5. Így $\varphi(n)/q$ lehetséges értékei rendre 5 és 2. Egyszerű számolással $2^5, 2^2 \not\equiv 1 \pmod{11}$, így a lemmából adódik, hogy a 2 primitív gyök modulo 11. Hasonló számolással adódik, hogy az $a = 3$ nem primitív gyök modulo 11, ugyanis $3^5 = 243 \equiv 1 \pmod{11}$.

(2) Hasonló számolással kaphatjuk, hogy 2 nem primitív gyök modulo 17, míg a 3 az.

(3) Legyen most $n = 9$. A $\varphi(9) = 6$ prímosztói 2 és 3, tehát a $\varphi(n)/q$ lehetséges értékei most rendre 3 és 2. A lemma szerint valamely $a \in \mathcal{U}_9$ pontosan akkor primitív gyök modulo 9, ha $a^2, a^3 \neq 1$ $\mathcal{U}_9$-ben. Mivel $2^2, 2^3 \not\equiv 1 \pmod{9}$ kapjuk, hogy a 2 primitív gyök modulo 9.

4.1.3. Tétel. *Tetszőleges p prímszámra az $\mathcal{U}_p$ csoportban $\varphi(d)$ számú d rendű elem van minden $d|p-1$-re.*

Következmény. *Tetszőleges p prímre az $\mathcal{U}_p$ csoport ciklikus.*

Bizonyítás. (Következmény.) Legyen $d = p - 1$. A tétel szerint $\mathcal{U}_p$-nek $\varphi(p-1)$ számú $p-1$ rendű eleme van. Mivel $\varphi(p-1) \geq 1$ az $\mathcal{U}_p$ csoportban van legalább egy $p-1$ rendű elem. Bármely ilyen elem generálja a csoportot, lévén $|\mathcal{U}_p| = p - 1$.

Példa. Az $\mathcal{U}_7$ csoportnak az 5 generátoreleme, ugyanis e csoportban

$$5^1 = 5,\ 5^2 = 4,\ 5^3 = 6,\ 5^4 = 2,\ 5^5 = 3,\ 5^6 = 1.$$

A tétel bizonyítása. Legyen p páratlan prím és $d|p-1$. Jelölje A_d az $\mathcal{U}_p$ csoport d rendű elemei halmazát, azaz

$$A_d = \{a \in \mathcal{U}_p \colon \mathrm{o}_p(a) = d\},$$

továbbá $\omega(d) = |A_d|$. Megmutatjuk, hogy minden $d|p-1$-re $\omega(d) = \varphi(d)$. Lagrange tételéből következik, hogy $\mathcal{U}_p$ minden elemének rendje osztója $p-1$-nek, ezért az A_d halmazok $\mathcal{U}_p$ egy osztályozását alkotják (e ponton engedjük meg, hogy valamely A_d üres is lehessen). Ez azt is jelenti, hogy

$$\sum_{d|p-1} \omega(d) = p - 1,$$

másrészt tudjuk, hogy az Euler-függvény összegzési függvénye az identikus függvény, tehát

$$\sum_{d|p-1} \varphi(d) = p - 1.$$

E két egyenlőségből azt kapjuk, hogy

$$\sum_{d|p-1} (\varphi(d) - \omega(d)) = 0.$$

A bizonyítás befejezéséhez ezután már elegendő azt megmutatni, hogy $\varphi(d) \geq \omega(d)$ teljesül $p-1$ minden d osztójára.

Valóban, ha valamely $d|p-1$-re $A_d = \emptyset$, akkor az egyenlőtlenség nyilván teljesül, ezért föltehető, hogy $A_d \neq \emptyset$. Legyen $a \in A_d$ és tekintsük az $a, a^2, \ldots, a^d = 1$ elemeket. Mivel ezen elemek d-edik hatványai 1-gyel egyenlők, az $f(x) = x^d - 1$ polinomnak van d számú különböző gyöke $\mathbb{Z}_p$-ben.

Igazolható, hogy egy $g \in \mathbb{Z}_p[x]$ polinomnak legföljebb $\deg(g)$ számú különböző gyöke van $\mathbb{Z}_p$-ben, ezért az előbbi $a, a^2, \ldots, a^d$ elemek az f polinom összes $\mathbb{Z}_p$-beli gyökét megadják. Az A_d halmaz pedig azon a^i gyökökből áll, amelyekre $\mathrm{ln.\,k.\,o.}(i, d) = 1$.

Ha $b \in A_d$, akkor egyrészt $f(b) = 0$, másrészt $b = a^k$ valamely $1 \leq k \leq d$-re. Ha $j = \mathrm{ln.\,k.\,o.}(k, d)$, akkor

$$b^{d/j} = \left(a^k\right)^{d/j} = \left(a^d\right)^{k/j} = 1^{k/j} = 1$$

$\mathcal{U}_p$-ben. De a b egy d-edrendű elem, így d-nél alacsonyabb kitevős hatványa nem lehet 1, ami azt jelenti, hogy $j = 1$.

Ezzel kaptuk, hogy a csoportunkban minden d rendű elem a^k alakú, ahol $\mathrm{ln.\,k.\,o.}(k, d) = 1$. Az ilyen kitevők száma $\varphi(d)$, tehát a d rendű elemek száma nem lehet ennél több. Ezzel igazoltuk az $\varphi(d) \geq \omega(d)$ egyenlőtlenséget, amivel a bizonyítás teljes.

Az előbbi tétel és következménye bizonyítását kissé módosítva egy sokkal általánosabb eredményt is igazolhatunk.

4.1.4. Tétel. *Tetszőleges F test esetén a nemzérő elemei F^* csoportjának minden véges részcsoportja ciklikus.*

Megjegyzés. A 4.1.3. Tétel után említett következmény megfordítása nem igaz, ugyanis $\mathcal{U}_4$ is ciklikus csoport.

4.1.5. Tétel. *Tetszőleges páratlan p prímre és $k \in \mathbb{N}$-re az $\mathcal{U}_{p^k}$ csoport ciklikus.*

Bizonyítás. A bizonyítás vázlata a következő.
(a) A 4.1.3. Tétel utáni Következmény alapján föltehető, hogy $k > 1$.
(b) Előbb egy g modulo p primitív gyököt választunk, majd
(c) megmutatjuk, hogy g, vagy $g + p$ primitív gyök modulo p^2.
(d) Végül megmutatjuk, hogy ha h primitív gyök modulo p^2, akkor h primitív gyök modulo p^k minden $k \geq 2$-re is.

Legyen g primitív gyök modulo p, így $g^{p-1} \equiv 1 \pmod{p}$ és $g^i \not\equiv 1 \pmod{p}$ valahányszor $1 \leq i < p-1$. Mivel $\ln.\,\mathrm{k.\,o.}(g,p) = 1$, $\ln.\,\mathrm{k.\,o.}(g,p^2) = 1$ is teljesül, ami azt jelenti, hogy g-t tekinthetjük $\mathcal{U}_{p^2}$ elemének is.

Jelölje d a g rendjét modulo p^2. Euler tételéből következik, hogy $d|\varphi(p^2) = p(p-1)$. Tudjuk, hogy $g^d \equiv 1 \pmod{p^2}$, így $g^d \equiv 1 \pmod{p^2}$ is teljesül. De $\mathrm{o}_p(g) = p-1$, ezért $p-1|d$. A p prím e két tény maga után vonja, hogy csak a $d = p(p-1)$ és a $d = p-1$ esetek lehetségesek. Az előbbi esetben g primitív gyök modulo p^2, így a továbbiakban csak a $d = p-1$ esettel foglalkozunk.

Legyen $h = g + p$. Mivel $h \equiv g \pmod{p}$, a h is primitív gyök modulo p. Megismételve az előbbi gondolatmenetet kapjuk, hogy $\mathrm{o}_{p^2}(h) = p(p-1)$, vagy $\mathrm{o}_{p^2}(h) = p-1$. Tudjuk, hogy $g^2 \equiv 1 \pmod{p^2}$ ezért — alkalmazva a binomiális tételt — kapjuk, hogy

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \ldots \equiv 1 + pg^{p-2} \pmod{p^2},$$

ahol a ki nem írt tagok oszthatók p^2-tel. Mivel $\ln.\,\mathrm{k.\,o.}(g,p) = 1$, $pg^{p-2} \not\equiv 0 \pmod{p^2}$, ezért $h^{p-1} \not\equiv 1 \pmod{p^2}$. Ez pedig azt jelenti, hogy a h rendje nem lehet $(p-1)$ az $\mathcal{U}_{p^2}$ csoportban, tehát az szükségképp $p(p-1)$, ami azt jelenti, hogy a h primitív gyök modulp p^2.

Végül foglalkozzunk a (d) esettel. Legyen h primitív gyrök modulo p^2. k-szerinti indukcióval fogjuk igazolni, hogy h primitív gyök modulo p^k tetszőleges $k \geq 2$-re. Mivel a $k = 2$ nyilvánvaló, föltesszük, hogy h primitív gyök modulo p^k valamely $k \geq 2$-re. Legyen p^k rendje modulo p^{k+1} d. A további gondolatmenetünk hasonlít arra, amit a (c) esetben követtünk.

Világos, hogy $d|\varphi(p^{k+1}) = p^k(p-1)$ és $\varphi(p^k)|d$, azaz $p^{k-1}(p-1)|d$. Ez a kettő együtt csak akkor teljesül, ha $d = p^k(p-1)$, vagy $d = p^{k-1}(p-1)$. Az első esetben h primitív gyök modulo p^{k+1}, így csak a másodikkal kell foglalkozni. Meg fogjuk mutatni, hogy $h^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$.

Lévén h primitív gyök modulo p^k, a rendje $\mathcal{U}_{p^k}$-ban $\varphi(p^k) = p^{k-1}(p-1)$, így $h^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Euler tételéből azonban következik, hogy $h^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$ ugyanis $p^{k-2}(p-1) = \varphi(p^{k-1})$. E két kongruenciából az adódik, hogy

$$h^{p^{k-2}(p-1)} = 1 + kp^{k-1}, \quad \text{ahol } \ln.\,\text{k.}\,\text{o.}(k,p) = 1.$$

A binomiális tételt alkalmazva

$$\begin{aligned} h^{p^{k-1}(p-1)} &= (1 + kp^{k-1})^k \\ &= 1 + \binom{p}{1} kp^{k-1} + \binom{p}{2} (kp^{k-1})2 + \dots \\ &= 1 + kp^k + \frac{1}{2}k^2 p^{2k-1}(p-1) + \dots \end{aligned}$$

ahol a ... olyan tagok helyett áll, amelyek mindegyike osztható $(p^{k-1})^3$-nel, és így p^{k+1}-gyel is, ugyanis $3(k-1) \geq k+1$, valahányszor $k \geq 2$.

Ebből következik, hogy

$$h^{p^{k-1}(p-1)} \equiv 1 + kp^k + \frac{1}{2}k^2 p^{2k-1}(p-1) \pmod{p^{k+1}}.$$

A föltétel szerint p páratlan prím, az előbbi kongruencia jobb oldalán levő harmadik tag osztható p^{k+1}-gyel, mivel $2k-1 \geq k+1$ valahányszor $k \geq 2$.. Ez pedig azt jelenti, hogy

$$h^{p^{k-1}(p-1)} \equiv 1 + kp^k \pmod{p^{k+1}}.$$

Mivel $p \nmid k$, kapjuk, hogy

$$h^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}},$$

amely a bizonyítást teljessé teszi azzal, hogy a $d = p^{k-1}(p-1)$ eset nem lehetséges.

Megjegyzés. A $p \neq 2$ föltétel szükséges, mert $k = 2$-re az indukciónk nem működik. A „harmadik tagra" vonatkozó megjegyzésünk nem igaz ekkor, ugyanis $p = 2$ esetén $k^2 p^{2k-1}(p-1)/2 = k^2 2^{2k-2}$, amely nem osztható 2^{k+1}-gyel.

4.1.6. Tétel. *Az $\mathcal{U}_{2^k}$ csoport pontosan akkor ciklikus, ha $k = 1, 2$.*

Bizonyítás. Nyilvánvaló, hogy az $\mathcal{U}_2$, $\mathcal{U}_4$ csoportok ciklikusok, így csak azt kell igazolni, hogy $k \geq 3$-ra az $\mathcal{U}_{2^k}$ csoportok nem ciklikusok. Ehhez pedig elég azt megmutatni, hogy $\mathcal{U}_{2^k}$-nak nincs $\varphi(2^k) = 2^{k-1}$ rendű eleme. Ez abból következik, hogy

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \qquad (*)$$

minden páratlan $a \in \mathbb{N}$-re. Ez utóbbit k-szerinti indukcióval fogjuk igazolni.

A legkisebb vizsgálandó kitevő a $k = 3$. Azt kell igazolni, hogy $a^2 \equiv 1 \pmod 8$ minden páratlan a-ra. Ez igaz, hiszen $a = 2b + 1$-ből

$a^2 = 4b(b+1) \equiv 1 \pmod 8$ adódik. Ha $k \geq 3$ és a páratlan, akkor, föltételezve, hogy $(*)$ teljesül, belőle azt kapjuk, hogy

$$a^{2^{k-2}} = 1 + 2^k c,$$

ahol $c \in \mathbb{Z}$. Négyzetre emelve ezen egyenlőséget

$$a^{2^{(k+1)-2}} = (1+2^k c)^2 = 1+2^{k+1}c+2^{2k}c^2 = 1+2^{k+1}(c+2^{k-1}c^2 \equiv 1 \pmod{2^{k+1}},$$

ami épp $(*)$ teljesülését jelenti $k+1$-re. Ezzel a bizonyítás teljes, hiszen igazoltuk $(*)$ teljesülését minden $k \geq 3$-ra.

4.1.7. Tétel. *Az $\mathcal{U}_n$ csoport pontosan akkor ciklikus, ha*

$$n = 1, 2, 4, p^k, 2p^k,$$

ahol p páratlan prím, $k \in \mathbb{N}$.

Megjegyzés. A tételt ebben az általános formában nem igazoljuk. Emlékeztetünk, hogy korábban igazoltuk, hogy tetszőleges p páratlan prímre az $\mathcal{U}_{p^k}$ csoportok ciklikusok tetszőleges $k \in \mathbb{N}$-re. Az pedig, hogy az $\mathcal{U}_n$ csoportok $n = 1, 2, 4$-re ciklikusok triviális.

Következmény. *Pontosan akkor létezik primitív gyök modulo n, ha $n = 2, 4, p^k, 2p^k$, ahol p páratlan prím és $k \in \mathbb{N}$.*

Kérdés, hogy mit mondhatunk azon n-ekre az $\mathcal{U}_n$ csoportokról, amelyekre azok nem ciklikusok. A Kinai-maradéktétel segítségével egyszerűen igazolható a $\mathbb{Z}_n$ gyűrű alábbi direkt fölbontása:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}},$$

ahol $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, és $p_1, p_2, \ldots, p_m$ különböző prímek. Az itt szereplő gyűrű izomorfizmust az előforduló gyűrűk egységcsoportjaira megszorítva adódik a következő:

$$\mathcal{U}_n \cong \mathcal{U}_{p_1^{k_1}} \times \mathcal{U}_{p_2^{k_2}} \times \ldots \times \mathcal{U}_{p_m^{k_m}},$$

ahol $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, és $p_1, p_2, \ldots, p_m$ Vegyük észre, hogy ezen legutóbbi direkt fölbontás éppen az $\mathcal{U}_n$ véges Abel-csoport alaptétel szerinti fölbontása.

4.2. Gauss-egészek.

Mielőtt ténylegeen algebrai számelméleti eredményeket, problémákat ismertetnénk, egy bevezető példát tekintünk.

Definíció. Azon $a + bi$ alakú komplex számokat, amelyekre $a, b \in \mathbb{Z}$ *Gauss-egészeknek* nevezzük. Az összes Gauss-egészek halmazát az elkövetkezőkben $\mathbb{Z}[i]$ fogja jelölni.

Jelölés. Az egyértelmű megkülönböztetés érdekében az ún. *racionális egészeket*, azaz $\mathbb{Z}$ elemeit latin betűkkel, míg a Gauss-egészeket görög betűkkel fogjuk jelölni.

Megjegyzés. Világos, hogy minden racionális egész Gauss-egész, de ez nem fog jelölésbeli zzavart okozni.

Definíció. Az $\alpha = a + bi$ Gauss-egész *normájának* nevezzük és $N(\alpha)$-val jelöljük α abszolút értékének négyzetét:

$$N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2.$$

A Gauss-egészek definíniójából és a komplex számok abszolút értékére vonatkozó ismereteink alapján nyilvánvalók a következő tétel állításai.

4.2.1. Tétel. *Tetszőleges α, β Gauss-egészekre*

$(\imath)$ $N(\alpha)$ *nemnegatív egész,*
$(\imath\imath)$ $N(\alpha) = 0 \quad \Leftrightarrow \quad \alpha = 0,$
$(\imath\imath\imath)$ $N(\alpha\beta) = N(\alpha)N(\beta).$

Megmutatjuk, hogy a Gauss-egészekre lényegében ugyanolyan számelmélet építhető, mint a racionális (közönséges) egész számokra. Az első említésre méltó különbség a maradékos osztásoknál fog jelentkezni.
Definíció. Azt mondjuk, hogy az α Gauss egész *osztója* a β Gauss-egésznek, ha van olyan γ Gauss-egész, hogy $\beta = \alpha\gamma$. Ez esetben alkalmazni fogjuk az ismert $\alpha \mid \beta$ jelölést.

4.2.2. Tétel. *Ha az $\alpha, \beta \in \mathbb{Z}[i]$-re $\alpha \mid \beta$, akkor $N(\alpha) \mid N(\beta)$ is teljesül a racionális egészek körében.*
Definíció. Azt mondjuk, hogy az ε Gauss-egész *egység*, ha minden Gauss-egésznek osztója.
Megjegyzés. Ez nem az integritástartománybeli egység szokásos definíciója, de a Gauss-egészek körében tradicionálisan így definiálják. A következő tételben megmutatjuk, hogy a két definíció ekvivalens.

4.2.3. Tétel. *Egy ε Gauss-egészre a következő állítások ekvivalensek.*

$(\imath)$ ε egység.
$(\imath\imath)$ $\varepsilon \mid 1.$
$(\imath\imath\imath)$ $N(\varepsilon) = 1.$
$(\imath\nu)$ $\varepsilon = \pm 1,$ vagy $\varepsilon = \pm i.$

Bizonyítás.
$(\imath) \Rightarrow (\imath\imath)$ Azonnal adódik az egység iménti definíciójából.
$(\imath\imath) \Rightarrow (\imath\imath\imath)$ Következik az 4.2.2. Tételből.
$(\imath\imath\imath) \Rightarrow (\imath\nu)$ Az $N(a+bi) = a^2 + b^2 = 1$ egyenlőség a racionális egészek körében csak akkor teljesül, ha $a = \pm 1$ és $b = 0$, vagy $a = 0$ és $b = \pm 1$.
$(\imath\nu) \Rightarrow (\imath)$ Bármely α Gauss-egészre

$$\alpha = 1\alpha = (-1)(-\alpha) = i(-i\alpha) = (-i)(i\alpha).$$

A következő tétel a Gauss-egészek maradékos (euklideszi) osztásáról szól

4.2.4. Tétel. *Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ, ϱ Gauss-egészek, hogy*

$$\alpha = \beta\gamma + \varrho \qquad \text{és} \qquad N(\varrho) < N(\beta). \tag{1}$$

Bizonyítás. Vegyük észre, hogy az (1) föltétel ekvivalens a következővel:

$$\frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad \left|\frac{\varrho}{\beta}\right| < 1.$$

Ez azt jelenti, hogy olyan γ Gauss-egészt kell keresni, amelyre

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1. \tag{2}$$

A Gauss-egészek a sík egész koordinátájú rácspontjaival reprezentálhatók, így van a síkon olyan 1 oldalhosszúságú négyzet, amely belsejében, vagy a határán tartalmazza az $\frac{\alpha}{\beta}$ komplex számot reprezentáló pontot. Az elemi geometriából tudjuk, hogy van legalább egy olyan csúcspontja ezen négyzetnek, amelyik 1-nél kisebb távolságra van e ponttól (akár az összes csúcspont ilyen lehet). Ezek közül választhatjuk γ-t.

Legyen $\frac{\alpha}{\beta} = r+si$, és tekintsük a hozzá legközelebb eső csúcspontot (Gauss-egészt), jelölje ezt $\gamma = u+vi$. Világos, hogy u, v az r, s racionális számokhoz legközelebb eső egész.

Ekkor — ugyancsak elemi geometriai ismereteink alapján — kapjuk, hogy

$$\left|\frac{\alpha}{\beta} - \gamma\right| = (r-u)^2 + (s-v)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

Megjegyzés. Eredményünk azt is jelenti, hogy a Gauss-egészek gyűrűje az imént bevezetett normával euklideszi gyűrű.

A Gauss-egészek — föltéve, hogy legalább az egyikük nemzéró — *legnagyobb közös osztóját* ugyanúgy definiáljuk, mint általában integritástartományokban, azaz *olyan közös oszó, amelynek mindegyik közös osztó osztója.* Világos, hogy a legnagyobb közös osztó csak egységszerestől eltekintve egyértelmű.

Bármely két Gauss-egésznek (ha legalább az egyik nem nulla) van legnagyobb közös osztója és egy legnagyobb közös meghatározható euklideszi algoritmussal, annak utolsó nemzéró maradéka. Ugyanúgy, mint korábban, $\ln.\,\mathrm{k.\,o.}(\alpha, \beta)$ az α, β Gauss-egészek bármely legnagyobb közös osztóját jelölheti.

Definiáljuk a Gauss-egészek körében is a fölbonthatatlan-(irreducibilis), ill. a prím elemeket.

Definíció. A π egységtől különböző, nemzéró Gauss-egészt *Gauss-prímnek* nevezzük ha csak úgy lehet osztója két Gauss-egész szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

$$\pi \,|\, \alpha\beta \qquad \Rightarrow \qquad \pi \,|\, \alpha \quad \text{vagy} \quad \pi \,|\, \beta.$$

Definíció. A π egységtől különböző, nemzéró Gauss-egészt *Gauss-fölbonthatatlannak* nevezzük ha csak úgy bontható föl két Gauss-egész

szorzatára, hogy valamelyik tényező egység. Azaz

$$\pi = \alpha\beta \qquad \Rightarrow \quad \alpha \text{ vagy } \beta \text{ egység.}$$

4.2.5. Tétel. *Egy Gauss-egész pontosan akkor prím, ha fölbonthatatlan.*

Bizonyítás. Tegyük föl, hogy ϱ Gauss prím, és $\varrho = \alpha\beta$ valamely α, β Gauss egészekre. Világos, hogy $\varrho|\alpha\beta$, és mivel prím, valamely tényezőnek is osztója, mondjuk $\varrho|\alpha$. Ekkor $\alpha\beta|\alpha$ is áll, amiből $\alpha \neq 0$ révén $\beta|1$ következik, azaz β egység.

Most legyen ϱ fölbonthatatlan elem, és $\varrho|\alpha\beta$. Ha $\varrho|\alpha$, akkor készen vagyunk, ϱ prím. Ha pedig $\varrho \nmid \alpha$, akkor $\ln.\,k.\,o.(\varrho, \alpha) = 1$. Ekkor van olyan γ, δ Gauss-egész, hogy $\varrho\gamma + \alpha\delta = 1$, amely hasonlóan igazolható, mint a racionális egészek körében. Ebből már egyszerűen adódik, hogy $\varrho|\beta$.

Megjegyzés. Mivel a Gauss-egészek körében a fölbonthatatlan elemek pontosan a prímelemek, ezért az elkövetkezőkben általában a prímelem, vagy egyszerűen a prím elnevezést részesítjük előnyben.

4.2.6. Tétel. (A számelmélet alaptétele) *Minden 0-tól és az egységektől különböző Gauss-egész fölbontható Gauss-fölbonthatatlanok szorzatára. A fölbontás a tényezők sorrendjétől és egységszeresektől eltekintva egyértelmű.*

Bizonyítás. Az egyértelműség bizonyítása a 4.2.5. Tétel segítségével ugyanúgy végezhető el, mint a racionális egészek esetén.

A felbonthatóság igazolásának menete is ugyanaz, csak az abszolút érték helyett a normát kell figyelembe venni.

Megjegyzés. Láttuk, hogy a számelmélet alaptételének igazolásakor a fölbontás létezését a racionális- és a Gauss-egészeknél lényegében ugyanúgy mutattuk meg, ugyanazt a gondolatmenetet követtük. Az egyértelműség bizonyításához vezető út lépései pedig a következő voltak:

Maradékos osztás $\Rightarrow$ létezik legnagyobb közös osztó (olyan osztó, amely minden közös osztónak osztója) $\Rightarrow$ minden fölbonthatatlan egyben prím is $\Rightarrow$ a fölbontás egyértelmű.

Megmutatható, hogy a (megfelelő értelemben vett) maradékos osztás létezéséből mindig következik, hogy az adott integritástartományban érvényes a számelmélet alaptétele, de a fordított irányú implikáció már nem. Másképpen mondva, nem minden Gauss-gyűrű Euklideszi-gyűrű.

A következő tétel teljesen leírja a Gauss-prímeket.

4.2.7. Tétel.

(*i*) *Minden π Gauss-prímhez pontosan egy olyan p pozitív (racionális) prím létezik, amelyre $\pi|p$.*

(*ii*) *Minden p pozitív (racionális) prímszám vagy maga is Gauss-prím, vagy két olyan Gauss-prím szorzata, amelyek normája p és egymás konjugáltjai.*

Bizonyítás.
(*i*) π prím, így $N(\pi) > 1$, és így $N(\pi)$ fölbontható pozitív (racionális) prímek szorzatára: $N(\pi) = p_1 p_2 \dots p_r$. Ekkor

$$\pi \mid \pi\overline{\pi} = N(\pi) = p_1 p_2 \dots p_r.$$

Mivel π (Gauss-)prím, osztója a szorzat valamely tényezőjének, azaz valamelyik p_i-nek is.

A egyértelműség igazolásához legyenek p, q olyan különböző pozitív (racionális) prímek, amelyeknek π osztója. Mivel p, q relatív prímek, léteznek olyan u, v egész számok, hogy $1 = pu + qv$, amiből $\pi|p$ és $\pi|q$ miatt $\pi|1$ adódik, ami lehetetlen.
(*ii*) Ha a $p > 0$ prímszám nem Gauss-prím, akkor fölírható legalább két Gauss-prím szorzataként (5.1.6. Tétel):

$$p = \pi_1 \dots \pi_r \qquad r \geq 2.$$

Ez azt jelenti, hogy

$$p^2 = N(p) = N(\pi_1) \dots N(\pi_r),$$

ahol $N(\pi_i) > 1$. Mivel p^2 csak egyféleképp bomlik egynél nagyobb (racionális) egészek szorzatára, ezért $r = 2$, és $N(\pi_1) = N(\pi_2) = p$.

Mivel $p = \pi_1\pi_2$ és $p = N(\pi_1) = \pi_1\overline{\pi_1}$, a bizonyítandó $\pi_2 = \overline{\pi}_1$ egyenlőséget kapjuk.

A következő tételben megadjuk a Gauss-prímek „listáját".

4.2.8. Tétel. *Legyen $\varepsilon \in \mathbb{Z}[i]$ tetszőleges egység. Az alábbi Gauss-egészek adják az összes Gauss-prímet.*
(*i*) $\varepsilon(1 + i)$.
(*ii*) εq, *ahol q olyan pozitív (racionális) prím, amelyre* $q \equiv -1 \pmod 4$.
(*iii*) *Olyan π, amelyre $N(\pi) = p$ pozitív (racionális) prím, és* $p \equiv 1 \pmod 4$*; minden ilyen prímszámhoz egységszerestől eltekintve két Gauss-prím tartozik, amelyek egymás konjugáltjai, de nem egységszeresei.*

Példák.
(1) A $-1 + i = i(1 + i)$, $-7i$ Gauss-prímek.
(2) A $2 - 5i$ szintén Gauss-prím, mert $N(2 - 5i) = 29$, amely racionális prím 1-gyel kongruens modulo 4.
(3) A -37, és a $9 + 2i$ nem Gauss-prímek.

Bizonyítás. A 4.2.7. Tétel alapján az összes Gauss-prímet a pozitív (racionális) prímek fölbontásából kapjuk attól függően, hogy e racionális prím a 2 (ez az (*i*) eset), $4k - 1$ alakú (a (*ii*) eset), illetve $4k + 1$ alakú (a (*iii*) eset).

(*i*) A $2 = (1 + i)(1 - i) = i^2(1 + i)^2$ egyenlőségekből adódik.

(*ii*) Legyen q olyan pozitív prím, hogy $q \equiv -1 \pmod 4$. Ha nem Gauss-prím, akkor az 4.2.7. Tétel (*ii*) állítása szerint van olyan $\pi = a + bi$ Gauss-prím, hogy

$$q = N(\pi) = a^2 + b^2,$$

ami lehetetlen, mert a modulo 4 -1-gyel kongruens pozitív prímek nem bonthatók két négyzetszám összegére.

(*iii*) Legyen $p \equiv 1 \pmod 4$ pozitív prímszám. Korábbi számelméleti tanulmányainkból tudjuk, hogy az $x^2 + 1 \equiv 0 \pmod p$ kongruencia megoldható, azaz van olyan $c \in \mathbb{Z}$, hogy $p|c^2 + 1 = (c + i)(c - i)$. Ekkor, amennyiben p Gauss-prím, osztója valamelyik tényezőnek. Ez azonban nem teljesül, hiszen

$$\frac{c \pm i}{p} = \frac{c}{p} \pm \frac{1}{p} i$$

nem Gauss-egészek, lévén, hogy a képzetes részük nem egész.

Alkalmazzuk ismét az előző tételt. Ez alapján $p = \pi\overline{\pi}$, ahol a jobb oldalon álló két tényező Gauss-prím. Azt kell csak igazolnunk, hogy $\pi \neq \varepsilon\overline{\pi}$, ahol ε egység. Ez azonban egyszerű számolással adódik, ugyanis ε lehetséges értékei $\pm 1, \pm i$.