GAUSS-EGÉSZEK

Waldhauser Tamás

SZTE Bolyai Intézet

2023. március 13.

Definíció

Gauss-egészen olyan komplex számot értünk, melynek valós és képzetes része is egész szám. A Gauss-egészek halmazát $\mathbb{Z}[i]$ jelöli. Tehát

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Állítás

A Gauss-egészek kommutatív, egységelemes, zérusosztómentes gyűrűt (azaz integritástartományt) alkotnak.

Az oszthatóság minden integritástartományban definiálható, és hasonló tulajdonságokkal rendelkezik, mint az egész számok körében. Így speciálisan a Gauss-egészek oszthatósága is értelmezhető.

Definíció

Azt mondjuk, hogy az α Gauss-egész osztója a β Gauss-egésznek, ha van olyan γ Gauss-egész, amelyre $\beta = \alpha \cdot \gamma$. Formálisan:

$$\alpha \mid \beta \iff \exists \gamma \in \mathbb{Z}[i] \colon \beta = \alpha \cdot \gamma.$$

Példa: $(1 + i) \mid 2$, mert $2 = (1 + i)(1 - i)$.

Definíció

Az $\alpha = a + bi \in \mathbb{Z}[i]$ Gauss-egész normája:

$$\|\alpha\| = |\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2 \in \mathbb{N}_0.$$

Tétel

Tetszőleges $\alpha, \beta \in \mathbb{Z}[i]$ Gauss-egészek esetén teljesülnek az alábbiak:

(1) $\|\alpha \cdot \beta\| = \|\alpha\| \cdot \|\beta\|$

Biz: $\|\alpha \cdot \beta\| = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = \|\alpha\| \cdot \|\beta\|$

(2) $\alpha \mid \beta \implies \|\alpha\| \Big| \|\beta\|$

Biz: $\alpha \mid \beta \implies \exists \gamma \in \mathbb{Z}[i] \colon \beta = \alpha \cdot \gamma$

$\implies \|\beta\| = \|\alpha\| \cdot \|\gamma\| \implies \|\alpha\| \Big| \|\beta\|$

(3) $\alpha \mid 1 \iff \|\alpha\| = 1$

Biz: $\implies$: következik (2)-ből.

$\impliedby$: következik abból, hogy $\alpha \Big| \|\alpha\| = \alpha\overline{\alpha}$.

Definíció

Azt mondjuk, hogy az ε Gauss-egész egység, ha osztója az egységelemnek, azaz $\varepsilon \mid 1$. Az egységek halmazát $\mathbb{Z}[i]^*$ jelöli.

Következmény

A Gauss-egészek gyűrűjének egységei: $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

Bizonyítás.

$$\begin{aligned} \varepsilon = a + bi \in \mathbb{Z}[i]^* &\iff \|\varepsilon\| = 1 \\ &\iff a^2 + b^2 = 1 \\ &\iff a = \pm 1,\ b = 0 \ \text{ vagy } \ a = 0,\ b = \pm 1 \end{aligned}$$ ■

Megjegyzés

Az egységek minden kommutatív egységelemes gyűrűben csoportot alkotnak a szorzás műveletével. A fentiek szerint a Gauss-egészek gyűrűjének egységcsoportja éppen a negyedik egységgyökökből álló csoport.
Egy másik nevezetes példa: $\mathbb{Z}_m$ egységcsoportja a redukált maradékosztályokból álló $\mathbb{Z}_m^*$ csoport.

Definíció

Azt mondjuk, hogy az α és β Gauss-egészek asszociáltak, ha kölcsönösen osztják egymást:

$$\alpha \sim \beta \iff \alpha \mid \beta \text{ és } \beta \mid \alpha.$$

Állítás

Az asszociáltság ekvivalenciareláció a Gauss-egészek halmazán.
Két Gauss-egész akkor és csak akkor asszociált, ha csak egység tényezőben különböznek egymástól:

$$\alpha \sim \beta \iff \exists \varepsilon \in \mathbb{Z}[i]^* : \alpha = \varepsilon\beta.$$

Megjegyzés

Az asszociáltság és az egységek között minden integritástartományban fennáll a fenti kapcsolat. Asszociált elemeket oszthatóság szempontjából nem érdemes (sőt, nem is lehet!) megkülönböztetni.

Példa: Az $\alpha = 2 + 3i$ Gauss-egész asszociáltjai:

$$\alpha = 2 + 3i, \quad -\alpha = -2 - 3i, \quad i\alpha = -3 + 2i, \quad -i\alpha = 3 - 2i.$$

Tétel

Gauss-egészeken lehet maradékos osztást végezni: tetszőleges $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ esetén léteznek olyan ϑ, ρ Gauss-egészek, amelyekre $\alpha = \beta \cdot \vartheta + \rho$ és $\|\rho\| < \|\beta\|$. (Itt ϑ a hányados és ρ a maradék.)

Bizonyítás.

Tetszőleges ϑ esetén a $\rho := \alpha - \beta \cdot \vartheta$ választással teljesülni fog az $\alpha = \beta \cdot \vartheta + \rho$ egyenlőség. A „kunszt” az, hogy olyan ϑ Gauss egészet találjunk, amelyre $\|\rho\| = \|\alpha - \beta \cdot \vartheta\| < \|\beta\|$. Ez ekvivalens azzal, hogy

$$\left|\frac{\alpha}{\beta} - \vartheta\right| < 1.$$

Ha ϑ az $\frac{\alpha}{\beta}$ komplex számhoz legközelebb eső Gauss-egész a komplex számsíkon, akkor ez teljesülni fog.

(Rajzoljuk le: A Gauss-egészek egy egységnyi oldalú négyzetekből álló rács csúcsai. Az $\frac{\alpha}{\beta}$ komplex szám valamelyik négyzetbe esik (esetleg a határára). A négyzet valamelyik csúcsa biztosan 1-nél közelebb lesz $\frac{\alpha}{\beta}$-hoz.) ■

Példa

Osszuk el maradékosan az $\alpha = -7 + 5i$ Gauss-egészt a $\beta = 1 + 2i$ Gauss-egésszel.

Számítsuk ki a hányadost a komplex számok testében:

$$\frac{\alpha}{\beta} = \frac{-7 + 5i}{1 + 2i} = \frac{3}{5} + \frac{19}{5}i = 0,6 + 3,8i \approx 1 + 4i.$$

Kerekítsük a hányados valós és képzetes részét is a legközelebbi egész számra: $\vartheta := 1 + 4i$. Ekkor $\rho = \alpha - \beta \cdot \vartheta = -i$, és ez valóban jó lesz maradéknak, mert $\|\rho\| = 1 < 5 = \|\beta\|$.

Megjegyzés: Jó lenne a $\vartheta := 4i$ választás is, mert ekkor $\rho = 1 + i$ jön ki maradéknak, és $\|\rho\| = 2 < 5 = \|\beta\|$. Tehát a maradék és a hányados nem egyértelmű.

(Hasonlóan ellenőrizhető, hogy még $\vartheta = 1 + 3i$ is megfelelő, de $\vartheta = 3i$ már nem.)

A maradékos osztásra építve lehet euklideszi algoritmust végezni a Gauss-egészek körében, és így bebizonyítható, hogy bármely két Gauss-egésznek létezik legnagyobb közös osztója.

Definíció

A $\delta \in \mathbb{Z}[i]$ Gauss-egészt az α és β Gauss-egészek legnagyobb közös osztójának nevezzük, ha kielégíti a következő két feltételt:

(KO) $\delta \mid \alpha$ és $\delta \mid \beta$;

(LN) $\forall \varkappa \in \mathbb{Z}[i] : (\varkappa \mid \alpha \text{ és } \varkappa \mid \beta) \implies \varkappa \mid \delta$.

Tétel

Bármely két Gauss-egésznek létezik legnagyobb közös osztója, és az kifejezhető a két elem „lineáris kombinációjaként”:

$$\forall \alpha, \beta \in \mathbb{Z}[i]\ \exists \xi, \eta \in \mathbb{Z}[i] \colon \mathsf{Inko}(\alpha, \beta) = \alpha\xi + \beta\eta.$$

Erre a tételre alapozva az egész számokhoz hasonlóan megmutatható, hogy a Gauss-egészek gyűrűjében is ekvivalens a felbonthatatlanság és a prímtulajdonság, és érvényes a számelmélet alaptétele is.

Definíció

Azt mondjuk, hogy a $\pi \in \mathbb{Z}[i]$ elem irreducibilis (vagy felbonthatatlan), ha nem nulla és nem egység, és csak úgy bontható két elem szorzatára, hogy az egyik tényező asszociált π-hez. (Ekkor a másik tényező szükségképpen egység; ilyenkor triviális faktorizációról beszélünk.) Formálisan:

$$\forall \alpha, \beta \in \mathbb{Z}[i] \colon \pi = \alpha\beta \implies \pi \sim \alpha \text{ vagy } \pi \sim \beta.$$

Definíció

Azt mondjuk, hogy a $\pi \in \mathbb{Z}[i]$ elem prím, ha nem nulla és nem egység, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall \alpha, \beta \in \mathbb{Z}[i] \colon \pi \mid \alpha\beta \implies \pi \mid \alpha \text{ vagy } \pi \mid \beta.$$

Tétel

A Gauss-egészek gyűrűjében az irreducilibis elemek pontosan ugyanazok, mint a prím elemek.

A Gauss-egészek gyűrűjének prím (avagy felbonthatatlan) elemeit Gauss-prímeknek nevezzük. Szükségünk lesz időnként az egész számok gyűrűjének prím (avagy felbonthatatlan) elemeire is; ezekre egyszerűen csak prímszámokként hivatkozunk.

Tétel

A Gauss-egészek gyűrűjében érvényes a számelmélet alaptétele: minden $\alpha \in \mathbb{Z}[i]\backslash\{0\}$ Gauss-egész felbomlik Gauss-prímek szorzatára, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű.

Példa

A $17 + 19i$ Gauss-egész felbontása Gauss-prímek szorzatára:

$$17 + 19i = (1 + i) \cdot (2 - i)^2 \cdot (2 + 3i).$$

Hogy itt $1 + i$, $2 - i$ és $2 + 3i$ valóban Gauss-prímek, az a náluk kisebb normájú Gauss-egészek vizsgálatával ellenőrizhető.

A továbbiakban az a célunk, hogy leírjuk a Gauss-prímeket, és egyszerű módszert adjunk a fentihez hasonló felbontások megtalálására.

Lemma

Minden $\pi \in \mathbb{Z}[i]$ Gauss-prímhez van olyan $p \in \mathbb{N}$ prímszám, amelyre $\pi \mid p$.

Bizonyítás.

Tekintsük a $\|\pi\|$ természetes szám felbontását prímszámok szorzatára:

$$\|\pi\| = p_1 \cdot \ldots \cdot p_n.$$

Mivel $\|\pi\| = \pi \cdot \overline{\pi}$, világos, hogy $\mathbb{Z}[i]$-ben teljesül a $\pi \mid \|\pi\|$ oszthatóság.

Ezt összevetve a fentivel, és használva π prímtulajdonságát, kapjuk, hogy

$$\pi \mid \pi \cdot \overline{\pi} = \|\pi\| = p_1 \cdot \ldots \cdot p_n \implies \exists k : \pi \mid p_k.$$

Tehát π osztja a p_k prímszámok valamelyikét. ■

Ezek szerint az összes Gauss-prímet megkapjuk, ha elkészítjük a prímszámok $\mathbb{Z}[i]$-beli prímfaktorizációját. Ezekről a faktorizációkról szól a következő lemma.

Lemma

Ha a $p \in \mathbb{N}$ prímszám nem Gauss-prím, akkor $\mathbb{Z}[i]$-beli prímfelbontása így fest: $p = \pi \cdot \overline{\pi}$.

Bizonyítás.

Ha p nem Gauss-prím, akkor felbomlik Gauss-prímek szorzatára:

$$p = \pi_1 \cdot \ldots \cdot \pi_n \qquad (n \geqslant 2).$$

Vegyük mindkét oldal normáját:

$$p^2 = \|p\| = \|\pi_1\| \cdot \ldots \cdot \|\pi_n\|.$$

Ez csak úgy lehetséges, hogy $n = 2$ és $\|\pi_1\| = \|\pi_2\| = p$.

Ekkor tehát $p = \|\pi_1\| = \pi_1 \cdot \overline{\pi_1}$, és ezzel meg is kaptuk p prímfelbontását $\mathbb{Z}[i]$-ben. ■

Példa

Íme az első három prímszám felbontása Gauss-prímek szorzatára:

- $2 = (1+i)\cdot(1-i) \sim (1+i)^2$;
- 3 Gauss-prím;
- $5 = (2+i)\cdot(2-i)$.

Tétel

(1) A 2 prímszám felbomlik $\mathbb{Z}[i]$-ben: $2 = (1+i)\cdot(1-i) \sim (1+i)^2$.

(2) Ha a p prímszám $4k+3$ alakú, akkor p a $\mathbb{Z}[i]$ gyűrűben is felbonthatatlan.

(3) Ha a p prímszám $4k+1$ alakú, akkor a $\mathbb{Z}[i]$ gyűrűben két Gauss-prím szorzatára bomlik: $p = (a+bi)\cdot(a-bi) = a^2+b^2$.
(Itt a két tényező (1)-gyel ellentétben nem asszociáltja egymásnak.)

A Gauss-egészek gyűrűjének irreducibilis elemei éppen a fenti felbontásokban szereplő elemek (asszociáltság erejéig).

Bizonyítás.

(1) Trivi.

(2) Ha p nem lenne Gauss-prím, akkor a lemma szerint

$$p = (a + bi) \cdot (a - bi) = a^2 + b^2.$$

A modulo 4 maradékok vizsgálatával belátható, hogy ez $p \equiv 3 \pmod 4$ esetén nem lehetséges.

(3) Ha $p \equiv 1 \pmod 4$, akkor -1 négyzetes maradék modulop p, azaz $k^2 \equiv -1 \pmod p$ alkalmas k egész számmal. Ekkor

$$p \mid k^2 + 1 = (k + i)(k - i).$$

Ha p Gauss-prím lenne, akkor ebből az következne, hogy

$$p \mid k + i \text{ vagy } p \mid k - i,$$

de egyik sem lehetséges. ∎

Következmény (Fermat-féle kétnégyzetszám-tétel)

Egy pozitív egész akkor és csak akkor bontható két négyzetszám összegére, ha prímhatványtényezős felbontásában a $4k+3$ alakú prímek páros kitevővel szerepelnek.

Bizonyítás.

A két négyzetszám összegeként előálló pozitív egészek pontosan a nemnulla Gauss-egészek normái. Tekintsük egy tetszőleges $0 \neq \zeta$ Gauss-egész prímfelbontását $\mathbb{Z}[i]$-ben:

$$\zeta \sim (1+i)^{\ell} \cdot p_1^{n_1} \cdot \ldots \cdot p_s^{n_s} \cdot \pi_1^{m_1} \cdot \ldots \cdot \pi_r^{m_r}, \text{ ahol}$$

(1) $\ell \in \mathbb{N}_0$ (ha $1+i$ nem szerepel ζ felbontásában, akkor legyen $\ell = 0$),

(2) mindegyik p_i egy $4k+3$ alakú prímszám, $s \in \mathbb{N}_0$, $n_i \in \mathbb{N}$,

(3) mindegyik π_j olyan Gauss-prím, amelynek normája $q_j := \|\pi_j\|$ egy $4k+1$ alakú prímszám, $r \in \mathbb{N}_0$, $m_j \in \mathbb{N}$.

Ekkor ζ normája:

$$\|\zeta\| = 2^{\ell} \cdot p_1^{2n_1} \cdot \ldots \cdot p_s^{2n_s} \cdot q_1^{m_1} \cdot \ldots \cdot q_r^{m_r}.$$

■

Példa

Bontsuk Gauss-prímek szorzatára a $\zeta = 17 + 19i$ Gauss-egészt.

Először bontsuk a $\|\zeta\|$ természetes számot prímszámok szorzatára:

$$\|\zeta\| = 17^2 + 19^2 = 650 = 2 \cdot 5^2 \cdot 13.$$

Bontsuk mindegyik fellépő prímszámot Gauss-prímek szorzatára:

$$2 = (1+i)\cdot(1-i), \quad 5 = (2+i)\cdot(2-i), \quad 13 = (2+3i)\cdot(2-3i).$$

Ezeket behelyettesítve a fenti egyenlőségbe, megkapjuk a $\zeta \cdot \overline{\zeta}$ szorzat prímfelbontását $\mathbb{Z}[i]$-ben:

$$\|\zeta\| = \zeta \cdot \overline{\zeta} = (1+i)\cdot(1-i)\cdot(2+i)^2\cdot(2-i)^2\cdot(2+3i)\cdot(2-3i).$$

Itt a tényezők fele adja ζ felbontását, a másik fele meg $\overline{\zeta}$ felbontását. Hogy kiderüljön, melyik tényező hova tartozik, maradékos osztással vizsgáljuk meg, hogy melyik osztója ζ-nak, és melyik nem:

Példa (folyt.)

$$\|\zeta\| = \zeta \cdot \overline{\zeta} = (1+i)\cdot(1-i)\cdot(2+i)^2\cdot(2-i)^2\cdot(2+3i)\cdot(2-3i).$$

Itt a tényezők fele adja ζ felbontását, a másik fele meg $\overline{\zeta}$ felbontását. Hogy kiderüljön, melyik tényező hova tartozik, maradékos osztással vizsgáljuk meg, hogy melyik osztója ζ-nak, és melyik nem:

$$1+i \mid \zeta,\ \ 1-i \mid \zeta,\ \ 2+i \nmid \zeta,\ \ 2-i \mid \zeta,\ \ 2+3i \mid \zeta,\ \ 2-3i \nmid \zeta.$$

(Vegyük észre, hogy itt az első két oszthatóság ugyanaz, mert $1+i \sim 1-i$, és helytelen lenne ebből levonni azt a következtetést, hogy ζ osztható $(1+i)(1-i) = 2$-vel!)

Tehát ζ felbontása Gauss-prímek szorzatára így fest:

$$17+19i = (1+i)\cdot(2-i)^2\cdot(2+3i).$$

Megjegyzés

Azt kaptuk, hogy

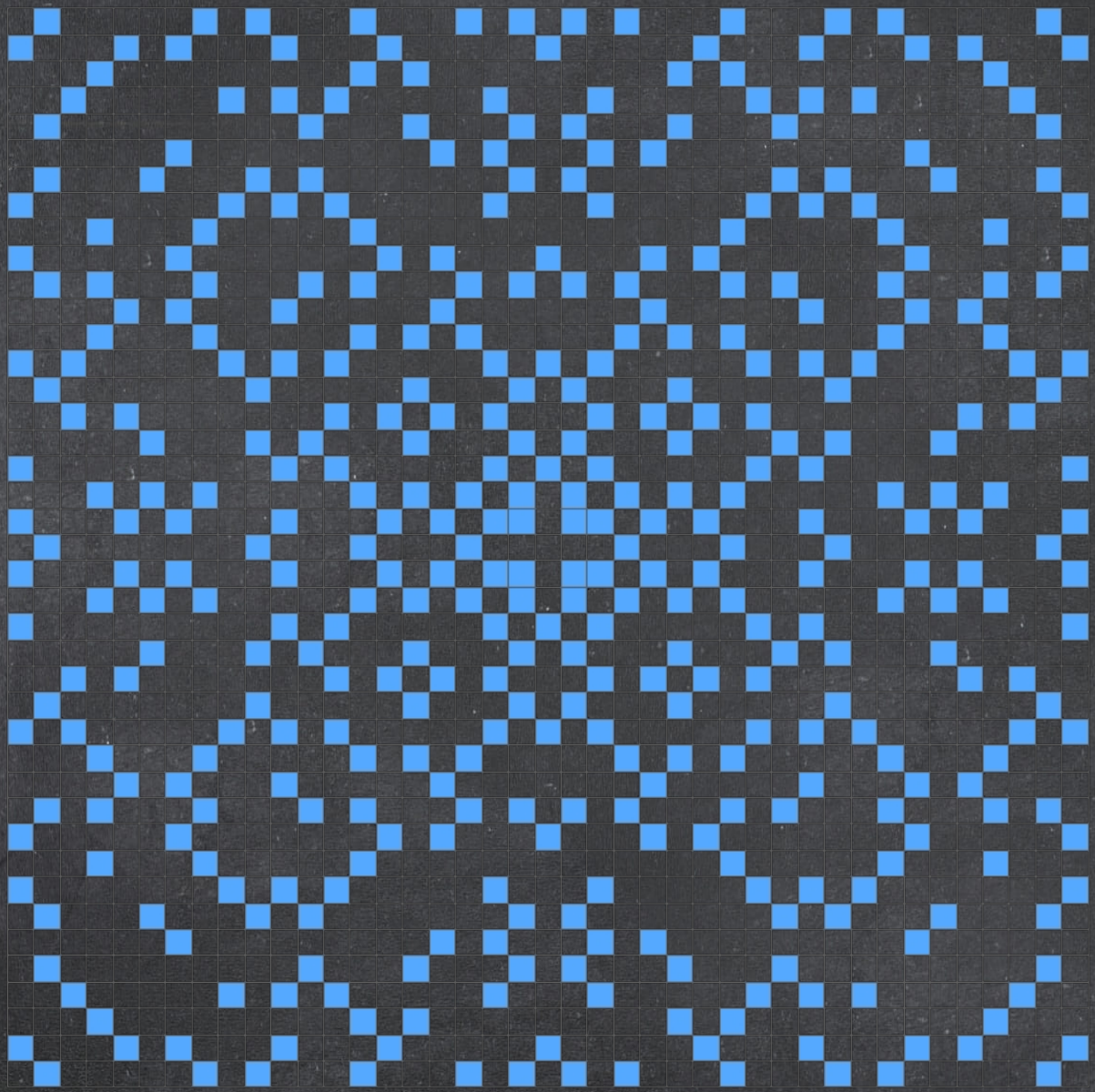
$$17 + 19i = (1 + i) \cdot (2 - i)^2 \cdot (2 + 3i).$$

Az egységekkel „játszva” másképp is felírhatjuk ugyanezt:

$$17 + 19i = (-i)(1 + i) \cdot (2 - i)^2 \cdot i(2 + 3i) = (1 - i) \cdot (2 - i)^2 \cdot (-3 + 2i).$$

Még sok más formában felírhatnánk ugyanezt a prímfelbontást. Az egész számokhoz képest furcsa lehet, hogy itt az asszociáltság nemcsak az előjel variálását jelentheti, pl. $2 + 3i$ és $-3 + 2i$ is asszociáltak (de $2 - 3i$ már nem asszociált hozzájuk!).

Gauss-prímek



Gauss-prímek