ALGEBARSKA TEORIJA BROJEVA

1. Uvod

Tradicionalno, (klasična) teorija brojeva se bavi istraživanjem aritmetičkih svojstava cijelih (kao i racionalnih) brojeva. Ponekad da bi odgovorili na neko klasično pitanje (npr. da bi riješili neku diofantsku jednadžbu u cijelim brojevima) potrebno je stvari promotriti malo šire kao što to pokazuju sljedeći primjer.

1.1. **Primjer.** Krenimo prvo sa jednim elementarnim zadatkom.

Zadatak 1. Riješite u cijelim brojevima jednadžbu

$$x^2 - 16 = y^3.$$

Rješenje. Vrijedi $y^3 = (x-4)(x+4)$. Ako je x neparan, tada je $(x-4, x+4) = 1$ (jer najveća zajednička mjera nužno dijeli $x+4-(x-4) = 8$), pa su $x+4$ i $x-4$ treće potencije cijelih brojeva. No, budući da razlika dva kuba nikad nije 8, u ovom slučaju jednadžba nema rješenja.

Ako je x paran, onda je i y paran pa slijedi da $4|x$. Neka je $x = 4x'$ i $y = 4y'$. Uvrštavanjem u polaznu jednadžbu dobivamo

$$x'^2 = 4y'^3 + 1,$$

iz čega slijedi da je x' neparan. Neka je $x' = 2m+1$, pa je $m(m+1) = m^2 + m = y'^3$. Kako su m i $m+1$ relativno prosti, oboje su treće potencije cijelih brojeva pa je $m = -1$ ili $m = 0$. U oba slučaja je $y' = 0$, odnosno $y = 0$ i $x = \pm 4$ je jedino cjelobrojno rješenje polazne jednadžbe.

□

Za rješavanje prethodne jednadžbe ključno je bilo to što smo mogli faktorizirati izraz $x^2 - 16$ te što prsten cijelih brojeva ima svojstvo jedinstvene faktorizacije.

Promotrimo još jedan zadatak.

Zadatak 2. Riješite u cijelim brojevima jednadžbu

$$x^2 + 2 = y^3.$$

Rješenje. Pretpostavimo da je (x, y) jedno rješenje. Primjetimo prvo da x ne može biti paran broj. Nadalje, faktorizirajmo lijevu stranu kao $(x+\sqrt{-2})(x-\sqrt{-2})$. Brojevi koji se pojavljuju u produktu su elementi prstena $\mathbb{Z}[\sqrt{-2}] = \left\{a + b\sqrt{-2} : a, b \in \mathbb{Z}\right\}$. Kako je $(x+\sqrt{-2}) - (x-\sqrt{-2}) = 2\sqrt{-2}$ i $(x+\sqrt{-2}) + (x-\sqrt{-2}) = 2x$ zaključujemo da su brojevi $(x+\sqrt{-2})$ i $(x-\sqrt{-2})$ relativno prosti. Budući da je $\mathbb{Z}[\sqrt{-2}]$ prsten jedinstvene faktorizacije postoji $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ takav da je

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

Specijalno, $3a^2b - 2b^3 = 1$, iz čega slijedi da je $b = \pm 1$.

a) Pretpostavimo da je $b = 1$. Tada je $3a^2 - 2 = 1$, odnosno $a = \pm 1$.

b) U slučaju da je $b = -1$, vrijedi da je $3a^2 - 2 = -1$, što nema rješenja u cijelim brojevima.

Dakle, rješenja polazne jednadžbe su $(\pm 5, 3)$. □

Da bi prethodni dokaz dobio neki smisao, trebamo definirati teoriju djeljivosti (što znači da jedan element dijeli drugi, što su to prosti elementi, što znači da su elementi relativno prosti, zašto je faktorizacija jedinstvena...) za prsten $\mathbb{Z}[\sqrt{-2}]$ (što ćemo napraviti općenito za integralne domene). Krenimo prvo se nekim definicijama.

2. Osnovne definicije

Definicija 2.1. *Prsten je algebarska struktura $(R, +, \cdot)$ koja se sastoji od skupa R i dvije binarne operacije na R, zbrajanje $+$ i množenje $\cdot$. Pri tom je $(R, +)$ abelova grupa, $(R, \cdot)$ monoid i vrijedi $a \cdot (b+c) = a \cdot b + a \cdot c$ odnosno $(b+c) \cdot a = b \cdot a + c \cdot a$. Prsten bez djeljitelja nule (tj. $a \cdot b = 0$ implicira $a = 0$ ili $b = 0$) se naziva integralna domena.*

Zadatak 3. Provjerite da je $\mathbb{Z}[\sqrt{-2}]$ uz standardne operacije zbrajanja i množenja integralna domena.

Svi primjeri integralnih domena (npr. $\mathbb{Z}[\sqrt{-2}]$) koji će se pojaviti u ovom predavanju su potprstenovi polja kompleksnih brojeva $\mathbb{C}$ tako da već "znamo" kako računati s tim brojevima.

Neka je sad R proizvoljna integralna domena. Cilj nam je za taj prsten definirati teoriju djeljivost (po uzoru na prsten $\mathbb{Z}$).

Za početak, neka su $x, y \in R$ proizvoljni elementi. Reći ćemo da x dijeli y, pišemo $x|y$, ako postoji $z \in R$ takav da je $y = xz$. Uočimo da je ova relacija tranzitivna.

Nadalje, analogon u R brojeva $\pm 1 \in \mathbb{Z}$ su invertibilni elementi (ili jedinice), $R^\times$, tj. elementi koji imaju multiplikativni inverz. Za elemente $x, y \in R$ za koje postoji $u \in R^\times$ takav da je $x = uy$ kažemo da su asocirani i pišemo $x \sim y$. Npr. u $\mathbb{Z}$ brojevi -7 i 7 su asocirani (mogli bi reći i da su aritmetički jednako zanimljivi). Za dva elementa $x, y \in R$ kažemo da su relativno prosti ako iz $z|x$ i $z|y$ nužno slijedi da je z jedinica (uočimo da invertibilni elementi dijele svaki element iz R).

Pojam prostog broja se generalizira na dva načina. Kažemo da je $x \in R$ ireducibilan, ako iz $yz = x$ slijedi da je y ili z jedinica, odnosno ako se x ne može prikazati na netrivijalan način kao produkt dva elementa (jasno, jedinice dijele sve elemente). S druge strane, kažemo da je x prost ako za sve $y, z \in R$ iz $x|yz$ slijedi da $x|y$ ili $x|z$. Kažemo da je prsten R prsten jedinstvene faktorizacije ako se svaki element iz R može na jedinstven način (do na jedinice i poredak) prikazati kao produkt ireducibilnih elemenata.

Zadatak 4. Prost element u domeni R je uvijek ireducibilan.

Zadatak 5. U domeni jedinstvene faktorizacije svaki je ireducibilan element prost.

3. Domene jedinstvene faktorizacije

3.1. Faktorizacija nije uvijek jedinstvena.

Zadatak 6. Prsten $\mathbb{Z}[\sqrt{-5}]$ nije domena jedinstvene faktorizacije.

Dokaz. Uočimo da je $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Dokažimo da su elementi $2, 3, (1 + \sqrt{-5})$ i $(1 - \sqrt{-5})$ ireducibilni.

Definirajmo funkciju normu $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ formulom

$$N(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2 = a^2 + 5b^2.$$

Važno je primjetiti da je norma multiplikativna: $N(xy) = N(x)N(y)$ za sve $x, y \in \mathbb{Z}[\sqrt{-5}]$.

Lema 3.1. *Element $x \in \mathbb{Z}[\sqrt{-5}]$ je invertibilan ako i samo ako je $N(x) = 1$.*

Dokaz. Neka je $x = a + b\sqrt{-5}$. Pretpostavimo da je x invertibilan. Tada je postoji $y \in \mathbb{Z}[\sqrt{-5}]$ takav da je $1 = xy$, odnosno $1 = N(1) = N(x)N(y)$ iz čega slijedi da je $N(x) = 1$. Obratno, ako je $N(x) = 1$, tada je $a = \pm 1$ i $b = 0$ pa je $x = \pm 1$ invertibilan. □

Lema 3.2. *U $\mathbb{Z}[\sqrt{-5}]$ nema elemenata norme 2 i 3.*

Dokaz. Neka je $x = a + b\sqrt{-5}$. Tvrdnja slijedi jer jednadžbe $a^2 + 5b^2 = 2$ i $a^2 + 5b^2 = 3$ nemaju rješenja u cijelim brojevima. □

Vrijedi $N(2) = 4$, $N(3) = 9$ i $N(1+\sqrt{-5}) = N(1-\sqrt{-5}) = 6$. Koristeći prethodne dvije leme, vidi se da su ti elementi ireducibilni. (Npr. $2 = xy$ gdje x i y nisu invertibilni implicira $4 = N(x)N(y)$ što nije moguće jer nema elemenata norme 2.) Budući da elementi nisu asocirani, zaključujemo da postoje dvije različite faktorizacije broja 6 na ireducibilne elemente, iz čega slijedi da prsten nema svojstvo jedinstvene faktorizacije. □

3.2. **Euklidska domena.** Sad ćemo za jednu klasu domena dokazati da su domene jedinstvene faktorizacije. To su domene u kojima se može definirati Euklidov algoritam.

Definicija 3.3. *Euklidska domena D je integralna domena za koju postoji funkcija $\phi : D\backslash\{0\} \to \mathbb{Z}$ takva da vrijedi*

(i) *$\phi(x) \geq 1$ za svaki $x \in D\backslash\{0\}$.*
(ii) *Za sve $a, b \in D$, $b \neq 0$, postoje $q, r \in D$ takvi da je $a = bq + r$ i ($r = 0$ ili $\phi(r) < \phi(b)$).*

Drugim riječima, možemo podijeliti dva elementa tako da je ostatak pri djeljenju manji od elementa s kojim dijelimo (veličinu elemena mjerimo funkcijom ϕ).

Evo jednog primjera na koji ćemo se kasnije vratiti. Neka je $\omega = \frac{1+\sqrt{-3}}{2}$ ($\omega^3 = 1$) i $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ norma na $\mathbb{Z}[\omega]$ definirana formulom $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$. Lako se vidi da je funkcija multiplikativna.

Zadatak 7. Dokažite da je $\mathbb{Z}[\omega]$ s normom $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ Euklidska domena.

Dokaz. Neka su $a, b \in \mathbb{Z}[\omega]$, $b \neq 0$. Tada postoji $z \in \mathbb{Z}[\omega]$ takav da je

$$\frac{a}{b} = \frac{a\bar{b}}{N(b)} = z + r_1 + r_2\omega,$$

gdje su $|r_1|, |r_2| \leq \frac{1}{2}$. Odnosno, $\left|\frac{a}{b} - z\right|^2 = r_1^2 - r_1r_2 + r_2^2 \leq \frac{3}{4}$. Množeći jednakost s $|b|^2$ dobivamo $|a - bz|^2 \leq \frac{3}{4}|b|^2 = \frac{3}{4}N(b)$, tj. $N(a - bz) < N(b)$. □

Napomena. Na sličan način se može pokazati da je $\mathbb{Z}[\sqrt{-2}]$ Euklidova domena.

Imamo sljedeći teorem.

Teorem 3.4. *Svaka Euklidska domena je domena jedinstvene faktorizacije.*

Napomena. U Euklidovoj domeni možemo definirati (i efikasno računati pomoću Euklidovog algoritma) pojam najvećeg zajedničkog djeljitelja dva elementa.

4. Jedan malo složeniji zadatak

U ovom odjeljku riješit ćemo sljedeći zadatak.

Zadatak 8 (IMO 2001). Neka su $a, b, c, d \in \mathbb{Z}$ takvi da je $a > b > c > d > 0$. Ako vrijedi

$$ac + bd = (b + d + a - c)(b + d - a + c), \tag{4.1}$$

pokažite da $ab + cd$ nije prost broj.

Primjetimo prvo da se uvjet (4.1) može zapisati kao $a^2 - ac + c^2 = b^2 + bd + d^2$. Koristit ćemo prsten $\mathbb{Z}[\omega]$ i njegovu normu N. Prisjetimo se da je to prsten jedinstvene faktorizacije (u kojem nema razlike između prostih i ireducibilnih elemenata) i da vrijedi $N(a + b\omega) = a^2 - ab + b^2$.

Zadatak 9. Pokažite da je $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm(1 + \omega)\}$.

Cilj nam je razumijeti kako se prosti brojevi iz $\mathbb{Z}$ faktoriziraju u $\mathbb{Z}[\omega]$.

Lema 4.1. *Ako je $\alpha \in \mathbb{Z}[\omega]$ prost, tada α dijeli neki prost broj $p \in \mathbb{Z}$ i vrijedi da je $N(\alpha) = p$ ili p^2.*

Dokaz. Vrijedi $\alpha|\alpha\bar{\alpha} = N(\alpha) \in \mathbb{Z}$. Možemo zapisati $N(\alpha) = \pm p_1 \cdots p_k$, gdje su p_i ne nužno različiti prosti brojevi. Iz definicije prostog elementa slijedi da α dijeli neki p_i, odnosno $N(\alpha)|N(p_i) = p_i^2$ pa tvrdnja slijedi. □

Lema 4.2. *Neka je $p \in \mathbb{Z}$ prost, $p \equiv 2 \pmod 3$. Tada je p prost i u $\mathbb{Z}[\omega]$.*

Dokaz. Rezultat slijedi iz prethodne leme i činjenice da je $a^2 - ab + b^2 \equiv 0, 1 \pmod 3$ (što onda implicira da je $N(\alpha) \neq p$ za sve $\alpha \in \mathbb{Z}[\omega]$ pa $\alpha|p$ implicira $N(\alpha) = p^2$). □

Lema 4.3. *Neka je $p \in \mathbb{Z}$ prost i $p \equiv 1 \pmod 3$. Tada postoji $x \in \mathbb{Z}$ takav da $p|x^2 - x + 1$.*

Dokaz. Tvrdnja slijedi iz činjenice da je -3 kvadratni ostatak modulo p za $p \equiv 1 \pmod p$ (formula za rješenje jednadžbe $x^2 - x + 1 = 0$: $x_{1/2} = \frac{1 \pm \sqrt{-3}}{2}$ vrijedi i nad konačnim poljem $\mathbb{F}_p$). □

Lema 4.4. *Neka je $p \in \mathbb{Z}$ prost i $p \equiv 1 \pmod 3$. Tada p nije prost u $\mathbb{Z}[\omega]$ i može prikazati kao produkt dva prosta elementa iz $\mathbb{Z}[\omega]$.*

Dokaz. Prema prethodnoj lemi postoji $x \in \mathbb{Z}$ takav da $p|x^2 - x + 1$ odnosno $p|(x + \omega)(x + \bar{\omega})$. Pretpostavimo da je p prost. Tada $p|(x + \omega)$ ili $p|(x + \bar{\omega}) = x - 1 - \omega$. Uočimo da ako cijeli broj c dijeli $a + b\omega$ (za neke $a, b \in \mathbb{Z}$), da onda $c|a$ i $c|b$. Specijalno, $p|1$ ili $p| - 1$ što je nije moguće.

Budući da p onda nije ni ireducibilan, postoje $\alpha, \beta \in \mathbb{Z}[\omega]$ koji nisu invertibilni takvi da je $p = \alpha\beta$. Vrijedi $p^2 = N(p) = N(\alpha)N(\beta)$ pa zaključujemo da su α i β prosti (jer je $N(\alpha) = N(\beta) = p$). □

Sljedeća propozicija opisuje proste elemente u $\mathbb{Z}[\omega]$.

Proposition 4.5. *Neka je $p \in \mathbb{Z}$ prost, $p \equiv 1 \pmod 3$. Tada postoji prost $\alpha \in \mathbb{Z}[\omega]$ takav da je $N(\alpha) = p$. Ako je i $N(\beta) = p$ i ako β nije asociran sa α, tada je β asociran sa $\bar{\alpha}$. Nadalje, ako je $p \in \mathbb{Z}$ prost i $p \equiv 2 \pmod p$ i ako je za $\alpha \in \mathbb{Z}[\omega]$, $N(\alpha) = p^2$ tada je α asociran s p.*

Napomena. Vrijedi $3 = -\omega^2(1 - \omega)^2$.

Zadatak 10. Ako je $N(\alpha) = 175$, odredite sve mogućnosti za α.

Rješenje. Imamo da je $175 = 5^2 \cdot 7$ i $7 = (3 + \omega)(2 - \omega)$. Dakle, $\alpha = \epsilon \cdot 5 \cdot (3 + \omega)$ ili $\alpha = \epsilon \cdot 5 \cdot (2 - \omega)$ za svaki $\epsilon \in \mathbb{Z}[\omega]^\times$. □

Sad možemo riješiti polazni zadatak.

Rješenje (Zadatak 8). Označimo sa $\alpha = a + c\omega$ i $\beta = b - d\omega$. Tada je $\alpha\beta = (ab + cd) + (bc + cd - ad)\omega$. Prema uvjetima zadatka vrijedi $N(\alpha) = N(\beta)$ pa direktno iz Propozicije 4.5 slijedi sljedeća lema.

Lema 4.6. *Elemente α i β možemo faktorizirati na proste faktore na sljedeći način:*

$$\alpha = \epsilon_1\pi_1 \cdots \pi_k\mu_1 \cdots \mu_l, \qquad \beta = \epsilon_2\pi_1 \cdots \pi_k\bar{\mu_1} \cdots \bar{\mu_l},$$

gdje su $\epsilon_1, \epsilon_2 \in \mathbb{Z}[\omega]^\times$, a $\pi_1, \ldots, \pi_k, \mu_1, \ldots, \mu_l$ prosti elementi iz $\mathbb{Z}[\omega]$.

Označimo s $\delta := \mu_1 \cdots \mu_l$, a s $\gamma := \pi_1 \cdots \pi_k$. Tada je

$$\alpha\beta = (ab + cd) + (bc + cd - ad)\omega = \epsilon_1\epsilon_2\gamma^2 N(\delta). \tag{4.2}$$

Kako $N(\delta)|ab + cd$, tvrdnja zadatka slijedi iz sljedeće leme.

Lema 4.7. *$N(\delta) \neq 1, ab + cd$.*

Dokaz. Pretpostavimo da je $N(\delta) = 1$. Tada je δ invertibilan pa je $\alpha = a + c\omega \sim \beta = b - d\omega$. Direktnom provjerom se vidi da to ne može biti (šest mogućnosti, koristi se $a > b > c > d > 0$).

Pretpostavimo da je $N(\delta) = ab + cd$. Tada dijeljenjem (4.2) s $N(\delta) = ab + cd$ dobivamo

$$1 + x\omega = \epsilon\gamma^2,$$

za neki $\epsilon \in \mathbb{Z}[\omega]^\times$ i $x \in \mathbb{Z}$. Slijedi $N(1+x\omega) = N(\gamma)^2$, tj. $x^2 - x + 1$ je kvadrat prirodnog broja. Budući da je (za $x > 1$) $(x-1)^2 < x^2 - x + 1 < x^2$ zaključujemo da su jedina rješenja ove jednadžbe $x = 0$ i $x = 1$ iz čega slijedi da je γ invertibilan. Slijedi $\alpha \sim \bar{\beta}$ što se opet lako provjeri da nije moguće. □

□

5. Zadaci

(1) Precizno definirajte što znači da domena ima svojstvo jedinstvene faktorizacije.
(2) Dokažite da je $\mathbb{Z}[\sqrt{-2}]$ Euklidova domena.
(3) Dokažite da $\mathbb{Z}[\sqrt{-26}]$ nije domena jedinstvene faktorizacije.
(4) Dokažite da je svaka Euklidova domena domena jedinstvene faktorizacije.
(5) Pokažite da je $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm(1+\omega)\}$.
(6) Riješite jednadžbu $y^2 = x^3 - 4$. Sve tvrdnje dokažite.