ALGEBARSKA TEORIJA BROJEVA

Petar Orlić

22. ožujka 2024.

Cilj ovog predavanja je dati kratki uvod u algebarsku teoriju brojeva i pokazati kako nam ona može pomoći u rješavanju diofantskih jednažbi. Kako je predavanje namijenjeno većinom studentima koji se još nisu susreli s algebrom, uvest čemo potrebne pojmove samo u posebnim slučajevima, i to na elementaran način koji ne zahtijeva veliko predznanje,
Radi ilustracije, krenimo s dvije diofantske jednadžbe.

Primjer 1. *U cijelim brojevima riješite jednadžbu*

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

Dokaz. Vrijedi $(x-4)(x+4) = y^3$. Ako je x neparan, tada su, zbog $(x-4, x+4) = 1$, $x-4$ i $x+4$ potpuni kubovi. Međutim, razlika dva kuba nikad nije 8 pa u ovom slučaju imamo kontradikciju.
Stoga su x i y parni pa lako dobivamo $4 \mid x, y$. Nakon supstitucije $x = 4x'$ i $y = 4y'$ jednadžba postaje

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

Sada vidimo da je x' neparan pa možemo pisati $x' = 2m + 1$. Jednadžba sada postaje

$$m(m+1) = y'^3.$$

Dakle, m i $m+1$ su potpuni kubovi pa je $m = -1$ ili $m = 0$. Zaključujemo da su $y = 0$, $x = \pm 4$ jedina cjelobrojna rješenja jednadžbe. □

Primjer 2. *U cijelim brojevima riješite jednadžbu*

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

Dokaz. Izraz $x^2 + 2$ se ne može faktorizirati u cijelim brojevima (za razliku od prošlog primjera). Međutim, može se faktorizirati u prstenu

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}.$$

Kako je to prsten jedinstvene faktorizacije, ideje iz prethodnog primjera možemo primijeniti i ovdje.
Primijetimo prvo da je x neparan. Vrijedi

$$(x - \sqrt{-2})(x + \sqrt{-2}) = y^3.$$

Kako je $(x - \sqrt{-2}, x + \sqrt{-2}) = (x - \sqrt{-2}, 2\sqrt{-2}) = 1$ i kako su jedini invertibilni elementi u prstenu $\mathbb{Z}[\sqrt{-2}]$ točno ± 1, zaključujemo da su $x \pm \sqrt{-2}$ potpuni kubovi. Stoga je

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

za neke $a, b \in \mathbb{Z}$. Specijalno, $3a^2b - 2b^3 = 1$ pa je $b = \pm 1$.
U slučaju $b = 1$ dobivamo $3a^2 - 2 = 1$, tj. $a = \pm 1$, a u slučaju $b = -1$ dobivamo $3a^2 - 2 = -1$, što nema rješenja u cijelim brojevima.
Sad nije teško zaključiti da su $x = \pm 5$, $y = 3$ jedina cjelobrojna rješenja jednadžbe. □

Vidimo da smo u ovom zadatku imali tri koraka:

- Naći pogodan prsten algebarskih brojeva koji je ujedno prsten jedinstvene faktorizacije.
- U tom prstenu odrediti invertibilne i proste/ireducibilne elemente.
- Nakon toga rješavati jednadžbu kao što smo već navikli sa cijelim brojevima.

Kratki uvod u algebarske strukture
Grupa je uređeni par $(G, \cdot)$, gdje je $\cdot$ operacija na skupu G sa sljedećim svojstvima:

- zatvorenost, tj $g_1 g_2 \in G, \forall g_1, g_2 \in G$
- asocijativnost, tj. $g_1(g_2 g_3) = (g_1 g_2) g_3, \forall g_1, g_2, g_3 \in G$
- postoji neutralni element $e \in G$, za njega vrijedi $ge = eg = g, \forall g \in G$
- svaki $g \in G$ ima inverz g^{-1}, za njega vrijedi $gg^{-1} = g^{-1}g = e$

Ako je operacija $\cdot$ komutativna, tada grupu G zovemo Abelova i tada operaciju množenja često označavamo s $+$ umjesto $\cdot$, a neutralni element s 0.
Podgrupa H je podskup grupe G koji je grupa s obzirom na istu operaciju $\cdot$, to označavamo s $H \leq G$.
Prsten je uređena trojka $(R, +, \cdot)$, gdje su $+$ i $\cdot$ operacije na skupu R sa sljedećim svojstvima:

- $(R, +)$ je Abelova grupa
- operacija $\cdot$ je zatvorena, asocijativna i postoji neutralni element 1
- operacija $\cdot$ je distributivna prema $+$

Integralna domena je komutativni prsten u kojem vrijedi

$$ab = 0 \implies a = 0 \text{ ili } b = 0.$$

Polje je komutativni prsten u kojem svaki element osim 0 ima multiplikativni inverz.
Analogon pogrupa u prstenima je ideal. (Lijevi) ideal I je (pravi) podskup prstena R za koji vrijedi:

- $(I, +) \leq (R, +)$,
- $rx \in I, \forall r \in R, x \in I$.

To označavamo s $I \trianglelefteq R$.
Sad ćemo iskazati formalnu definiciju domene jedinstvene faktorizacije.

Definicija 3. *Neka je R integralna domena. Kažemo da je $u \in R$ invertibilan (ili jedinica) ako postoji $v \in R$ za koji vrijedi $uv = vu = 1$. Skup jedinica označavamo s $R^\times$. Kažemo da su $a, b \in R$ asocirani ako postoji $u \in R^\times$ za koji je $a = bu$.*
Također, kažemo da je $a \in R$ ireducibilan ako se ne može prikazati kao produkt dva neinvertibilna elementa, tj.

$$a = bc \text{ za } b, c \in R \implies b \in R^\times \text{ ili } c \in R^\times.$$

Definicija 4. *Neka je R integralna domena. Kažemo da je R domena jedinstvene faktorizacije ako se, do na poredak i asociranost, svaki $a \in R$ može jedinstveno prikazati u obliku*

$$a = up_1^{\alpha_1} \dots p_k^{\alpha_k},$$

gdje je u invertibilan, a p_i ireducibilni elementi.

Primjer 5. *$\mathbb{Z}[\sqrt{-6}]$ nije domena jedinstvene faktorizacije jer je*

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Kasnije ćemo pokazati da su sva ova 4 broja ireducibilna te da nisu asocirani.

Kvadratna polja

U rješavanju diofantskih jednadžbi ovom metodom najčešće se koriste kvadratna polja, tj. polja oblika $\mathbb{Q}(\sqrt{d})$ za $d \in \mathbb{Z}$. Nije teško pokazati da su svi elementi polja $\mathbb{Q}(\sqrt{d})$ korijeni nekog normiranog polinoma s cjelobrojnim koeficijentima stupnja ≤ 2. Takav polinom zovemo minimalni polinom tog elementa.

Definicija 6. *$\alpha \in \mathbb{Q}(\sqrt{d})$ je algebarski cijeli broj ako njegov minimalni polinom ima cjelobrojne koeficijente.*

Algebarski cijeli brojevi polja $\mathbb{Q}(\sqrt{d})$ čine prsten. Nije teško provjeriti da su među racionalnim brojevima jedini algebarski cijeli brojevi upravo cijeli brojevi.

Propozicija 7. *Za kvadratno slobodan $d \in \mathbb{Z}$, prsten cijelih brojeva polja $\mathbb{Q}(\sqrt{d})$ je*

$$\begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], \text{ ako je } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}], \text{ inače.} \end{cases}$$

Na $\mathbb{Q}(\sqrt{d})$ možemo definirati normu

$$N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, N(a + b\sqrt{d}) = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}).$$

Ponekad koristimo i oznaku $|\cdot|$. Tako definirana funkcija je multiplikativna i ima brojna korisna svojstva.

Propozicija 8. *Ako je $\alpha \in \mathbb{Q}(\sqrt{d})$ algebarski cijeli broj, tada je $N(\alpha) \in \mathbb{Z}$.*

Korolar 9. *U prstenu cijelih brojeva polja $\mathbb{Q}(\sqrt{d})$, invertibilni elementi su točno oni čija je norma ± 1, a svi elementi čija je norma prosta su ireducibilni.*

Nije teško vidjeti da prsten cijelih brojeva polja $\mathbb{Q}(\sqrt{d})$ ima konačno jedinica za $d < 0$. Za $d > 0$ situacija je malo drugačija jer je jednadžba $a^2 - db^2 = 1$ zapravo Pellova jednadžba koja ima beskonačno rješenja, a ona su sva potencija minimalnog rješenja. Stoga za $d > 0$ jedinice čine beskonačnu cikličku grupu.

Sad možemo dokazati tvrdnje iz Primjera 5. $\mathbb{Z}[\sqrt{-6}]$ je prsten cijelih brojeva polja $\mathbb{Q}(\sqrt{-6})$. Svi invertibilni elementi su ± 1 jer jednadžba $a^2 + 6b^2 = 1$ ima samo ta 2 rješenja. Također, vrijedi $N(2) = 4, N(5) = 10, N(2 \pm \sqrt{6}) = 10$, a nije teško provjeriti da jednadžba $a^2 + 6b^2 = \pm 2, \pm 5$ nema rješenja. Stoga su svi ti elementi ireducibilni i našli smo dva različita rastava broja 10 na ireducibilne faktore.

Propozicija 7. kaže da $\mathbb{Z}[\sqrt{d}]$ nije uvijek prsten cijelih brojeva. U takvim slučajevima je smislenije koristiti prsten $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Npr. prsten $\mathbb{Z}[(]\sqrt{-7}]$ nije domena jedinstvene faktorizacije. Naime,

$$8 = 2^3 = (1+\sqrt{-7})(1-\sqrt{-7}).$$

Međutim, $\mathbb{Z}[(]\frac{1+\sqrt{-7}}{2}]$ jest. Vrijedi

$$\frac{1+\sqrt{-7}}{2}\frac{1-\sqrt{-7}}{2} = 2$$

pa su te dvije faktorizacije zapravo jednake

$$\left(\frac{1+\sqrt{-7}}{2}\right)^3\left(\frac{1-\sqrt{-7}}{2}\right)^3.$$

Domene glavnih ideala

Najlakši način za dokazivanje da je neki prsten domena jedinstvene faktorizacije je da dokažemo da je to domena glavnih ideala. Definirajmo prvo što je domena glavnih ideala.

Definicija 10. *Neka je R komutativni prsten. Kažemo da je ideal $I \trianglelefteq R$ glavni ako je oblika*

$$I = (a) = \{ax, x \in R\}.$$

Integralna domena R je domena glavnih ideala ako je svaki ideal $I \trianglelefteq R$ glavni.

Primjer 11. *Svi ideali u prstenu $\mathbb{Z}$ su oblika $(n), n \in \mathbb{Z}$. Stoga je $\mathbb{Z}$ domena glavnih ideala.*

Teorem 12. *Svaka domena glavnih ideala je ujedno i domena jedinstvene faktorizacije.*

Ovdje se nećemo baviti metodama dokazivanja da je neki prsten domena glavnih ideala jer bismo izašli iz okvira predavanja.

Propozicija 13. *Neka je R prsten cijelih brojeva polja $\mathbb{Q}(\sqrt{d})$. Ako je $0 < d < 100$, tada je R domena glavnih ideala ako i samo ako je*

$$\begin{aligned} d \in \{&2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41,43,\\ &46,47,53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,97\}. \end{aligned}$$

Ako je $d < 0$, tada je R domena glavnih ideala ako i samo ako je

$$d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}.$$

Domaća zadaća

Treba točno riješiti barem 5 zadataka. Zadaće predajte do petka 5. travnja 2024.

1. Dokažite Propoziciju 7, Propoziciju 8. i Korolar 9.
2. U cijelim brojevima riješite jednadžbu $x^5 - 1 = y^2$.
3. U cijelim brojevima riješite jednadžbu $y^2 = x^3 + 7$.
4. U cijelim brojevima riješite jednadžbu $x^3 - 2y^3 = 1$.
5. U cijelim brojevima riješite jednadžbu $x^3 = 3y^2 + 1$.
6. U cijelim brojevima riješite jednadžbu $x^3 + 48 = y^4$.
7. Niz prirodnih brojeva (a_n) je rekurzivno definiran s $a_0 = 0$, $a_1 = 1$ i $a_n = 2a_{n-1} + a_{n-2}$ za $n > 1$. Dokažite da za svaki prirodni broj k vrijedi $2^k \mid a_n$ ako i samo ako $2^k \mid n$.
8. Neka je p prost broj. Odredite ostatak koji broj $\prod_{k=1}^{p-1}(k^2 + 1)$ daje pri dijeljenju s p.
9. Dokažite da za svaki prirodni broj $n \geq 3$ postoje jedinstveni neparni prirodni brojevi x, y za koje je $x^2 + 7y^2 = 2^n$.
10. Neka su x, y, z prirodni brojevi takvi da je $xy = z^2 + 1$. Dokažite da postoje cijeli brojevi a, b, c, d takvi da je $x = a^2 + b^2$, $y = c^2 + d^2$, $z = ac + bd$.