Prosti brojevi i polinomi

Da li postoji funkcija čije vrednosti su isključivo prosti brojevi?

"funkcija koja 'proizvodi' proste brojeve"

• Ona ne može biti polinom:

(T1) [Goldbach] Ako je $F(t) \in \mathbb{Z}[t]$ nekonstantan polinom sa pozitivnim vodećim koeficijentom, onda je $F(n)$ složen za beskonačno mnogo prirodnih brojeva n.

$$= \sum_{j=0}^{d} a_j t^j, \quad a_d > 0$$

▽ Pretp. da je F nekonstantan polinom takav da je $F(n)$ prost broj za sve $n \geq N_0$ $(N_0 \in \mathbb{N})$

Označimo $p = F(N_0)$ - prost

Ali onda je

$$F(N_0 + kp) = \sum_{j=0}^{d} a_j (N_0 + kp)^j = \sum_{j=0}^{d} a_j \left(N_0^j + \sum \text{sabirci deljivi sa } p \right)$$

$$= \underbrace{\sum_{j=0}^{d} a_j N_0^j}_{= F(N_0) = p} + (\text{deljivo sa } p)$$

Dakle $p \mid F(N_0 + kp)$, za sve $k \in \mathbb{N}$.

Ali vodeći koef $a_d > 0$, pa za dovoljno veliko t, $a_d t^d$ dominira tj.: $F(N_0 + kp) > F(N_0) = p$ za sve dovoljno velike k, za koje je onda $F(N_0 + kp)$ deljiv sa p i strogo veći, pa

mora biti složen.

• Ali postoje polinomi koji uzimaju puno uzastopnih prostih vrednosti.

Primer Euler je pronašao polinom

$$\boxed{f(t) = t^2 + t + 41}$$

koji uzima proste vrednosti za sve $0 \leq n < 40$.

$f(0) = 41$
$f(1) = 43$
$f(2) = 47$
$f(3) = 53$
$f(4) = 61$
$f(5) = 71$
...
$f(37) = 1447$
$f(38) = 1523$
$f(39) = 1601$

$f(40) = 41^2 = 1681$

U čemu je "tajna" ovog polinoma? Kako ovo objasniti?

(T2) [G. Rabinowitsch, 1913.] Neka je $A \in \mathbb{N}$, $A \geq 2$ i $D := 1 - 4A < 0$. Sledeća tvrđenja su ekvivalentna:

(i) $n^2 + n + A$ je prost za sve $0 \leq n < A - 1$

(ii) $n^2 + n + A$ je prost za sve $0 \leq n \leq \frac{1}{2}\sqrt{\frac{|D|}{3}} - \frac{1}{2}$

(iii) prsten $\mathbb{Z}\left[\frac{-1+\sqrt{D}}{2}\right]$ je UFD (domen sa jednoznačnom faktorizacijom)
unique factorization domain

(T2) (i) $\to$ (ii) Trivijalno, jer je

$$\frac{1}{2}\sqrt{\frac{4A-1}{3}} - \frac{1}{2} < A-1 \iff 3A^2-4A+1>0 \quad \text{za } A \geq 2$$

- $A \in \mathbb{Z}_{\geq 2}$ $\qquad (x-\eta)(x-\bar{\eta}) = x^2+x+A$

η = fiksiran kompleksni koren jednačine $x^2+x+A=0$

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

$$\boxed{\eta^2 = -\eta - A} \quad (*)$$

Prsten

$$\mathbb{Z}[\eta] = \{ p(\eta) \mid p \in \mathbb{Z}[t] \}$$ [ali zbog (*) svi veći stepeni ($2., 3., \ldots$) mogu da se izraze preko $1, \eta$

$$= \mathbb{Z} + \mathbb{Z}\eta = \{ x + y\eta : x, y \in \mathbb{Z} \}$$

- Za $\alpha \in \mathbb{Z}[\eta]$, sa $\bar{\alpha}$ označavamo njegov kompleksni konjugat
- $\boxed{\bar{\eta} = -1-\eta} \in \mathbb{Z}[\eta]$

pa dobijamo $\alpha \in \mathbb{Z}[\eta]$, $\alpha = x + y\eta$ ($x, y \in \mathbb{Z}$), onda je:

$$\bar{\alpha} = \overline{x+y\eta} = x + y\bar{\eta} = x + y(-1-\eta) = \underbrace{x-y}_{\in\mathbb{Z}} - y\eta \in \mathbb{Z}[\eta]$$

tj. prsten $\mathbb{Z}[\eta]$ je zatvoren za kompleksno konjugovanje.

Def **Norma** elementa $\alpha = x+y\eta \in \mathbb{Z}[\eta]$ je definisana sa

$$N(\alpha) := |\alpha|^2 = \alpha \cdot \bar{\alpha} = (x+y\eta)(x+y\bar{\eta}) =$$

$$= x^2 + y^2 \underbrace{|\eta|^2}_{=A} + xy \underbrace{(\eta+\bar{\eta})}_{=-1} = x^2 - xy + Ay^2$$

Primedba Za $\alpha \in \mathbb{Z}[\gamma]$ je $N(\alpha) \in \mathbb{Z}$; dodatno, $N(\alpha) > 0$ za sve $\alpha \neq 0$.

- Važi i multiplikativnost:

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta), \quad \forall \alpha, \beta \in \mathbb{Z}[\gamma].$$

Def

- Za $\alpha, \beta \in \mathbb{Z}[\gamma]$ kažemo da α deli β, $\alpha \mid \beta$ ako $\exists\, \gamma \in \mathbb{Z}[\gamma]$: $\beta = \alpha\gamma$.
- $\alpha \in \mathbb{Z}[\gamma]$, $\alpha \neq 0$ je <u>jedinica</u> (invertibilan el.) ako $\alpha \mid 1$
- El. $\alpha \in \mathbb{Z}[\gamma]$ koji nije jedinica je <u>ireducibilan</u> ako iz $\alpha = \beta\gamma$, $\beta, \gamma \in \mathbb{Z}[\gamma]$ sledi $\beta \mid 1$ ili $\gamma \mid 1$.
- El. $\pi \in \mathbb{Z}[\gamma]$ je <u>prost</u> ako iz $\pi \mid \beta\gamma$, $\beta, \gamma \in \mathbb{Z}[\gamma]$ sledi $\pi \mid \beta$ ili $\pi \mid \gamma$.

L. 3 Element $\alpha \in \mathbb{Z}[\gamma]$ je jedinica $\iff N(\alpha) = 1$.
Jedine jedinice u prstenu $\mathbb{Z}[\gamma]$ su ± 1.

▼ ($\rightarrow$) α jedinica: $\exists\, \gamma$: $\alpha\gamma = 1 \rightarrow N(\alpha)N(\gamma) = N(\alpha\gamma) = N(1) = 1$
Al: $N(\alpha), N(\gamma) \in \mathbb{Z}_{>0} \rightarrow N(\alpha) = N(\gamma) = 1$.

($\leftarrow$) Ako je $\alpha \in \mathbb{Z}[\gamma]$ takav da je $N(\alpha) = 1$, onda iz $\alpha \cdot \overline{\alpha} = 1$ ($\overline{\alpha} \in \mathbb{Z}[\gamma]$) upravo sledi da je α invertibilan.

Na kraju, ako je $y \neq 0$:

$$N(x+y\gamma) = x^2 - xy + 4y^2 = \underbrace{\left(x - \frac{y}{2}\right)^2}_{\geq 0} + \frac{4 \cdot 4 - 1}{4} \underbrace{y^2}_{\geq 1} \geq \frac{7}{4} > 1$$

pa $x+y\gamma$ ne može biti jedinica. Dakle, mora biti $y=0$, ali onda iz $N(x) = x^2 = 1 \rightarrow x = \pm 1$ ▨

L.4 Ako je $\alpha \neq 0$ i nije jedinica u $\mathbb{Z}[\gamma]$, onda se α može predstaviti kao produkt ireducibilnih elemenata iz $\mathbb{Z}[\gamma]$.

▨ Ako ovo nije tačno, $\exists$ kontraprimeri.

Neka je $\alpha \neq 0$, neinvertibilan koji je kontraprimer i najmanje norme (princip dobrog uređenja skupa $\mathbb{Z}_{>0}$)

Kako je α kontraprimer, α sâm nije ireducibilan, pa $\exists\, \beta, \gamma$ nenula, neinvertibilni t.d. $\boxed{\alpha = \beta\gamma}$

$$\rightarrow N(\alpha) = \underbrace{N(\beta)}_{>1} \cdot \underbrace{N(\gamma)}_{>1} \rightarrow \begin{cases} N(\beta) < N(\alpha) \\ N(\gamma) < N(\alpha) \end{cases}$$

(jer β, γ nisu jedinice)

Ali zbog izbora α, ovi β i γ moraju imati faktorizaciju na ireducibilne faktore, ali onda to ima i $\beta\cdot\gamma = \alpha$. ↯ ▨

T.2 (iii) $\longrightarrow$ (i):

Neka je $0 \le n < A-1$. Imamo faktorizaciju:

$$n^2+n+A = (n-\gamma)(n-\bar{\gamma}) = (n-\gamma)(n+1+\gamma) \qquad (\star)$$

Neka je p neki prost delioc n^2+n+A

Mi pretp. (iii) tj. prsten $\mathbb{Z}[\gamma]$ je UFD.

- Ako bi p bio ireducibilan u $\mathbb{Z}[\gamma]$, on bi bio i prost element, pa zbog $(\star)$:

$$p \mid n-\gamma \quad \text{ili} \quad p \mid (n+1+\gamma)$$

Ali ovo je nemoguće, jer $\frac{n}{p} - \frac{1}{p}\gamma$, $\frac{n+1}{p} + \frac{1}{p}\gamma \notin \mathbb{Z}[\gamma] = \mathbb{Z}+\mathbb{Z}\gamma$

- Dakle, p nije ireducibilan u $\mathbb{Z}[\gamma]$ tj. $\exists\, \alpha, \beta \in \mathbb{Z}[\gamma]$:

$$p = \alpha \cdot \beta, \qquad \alpha, \beta \text{ nisu jedinice}$$

Uzmemo norme:

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)\,N(\beta)$$

$N(\alpha), N(\beta)$: celi brojevi > 1 (jer α, β nisu jedinice)

$\longrightarrow N(\alpha) = N(\beta) = p$.

Neka je

$\alpha = x + y\gamma, \quad x, y \in \mathbb{Z}$

Onda $y \neq 0$ (inače $x^2 = p$, x, p celi, p prost $\not\in$):

$$p = N(\alpha) = x^2 - xy + Ay^2 = \underbrace{\left(x - \frac{y}{2}\right)^2}_{\ge 0} + \left(A - \frac{1}{4}\right)\underbrace{y^2}_{\ge 1} \ge A - \frac{1}{4}$$

tj. $\boxed{p \geq A}$ jer su p, A celi brojevi

Sa druge strane, iz $0 \leq n < A-1$

$$n^2+n+A < (A-1)^2 + (A-1) + A = (A-1)A + A = A^2 \quad \text{tj.}$$

$$\boxed{\sqrt{n^2+n+A} < A}$$

Dakle, svaki prost delioc n^2+n+A je $>$ od $\sqrt{n^2+n+A}$, što je moguće samo ako je $n^2+n+A = p$ prost broj! ◢

L.5 Ako je $\pi \in \mathbb{Z}[y]$ čija norma je $\mathcal{N}(\pi) = p$ – racionalan prost broj, onda je π prost element prstena $\mathbb{Z}[y]$.

▼ $\langle \pi \rangle = \pi \cdot \mathbb{Z}[y]$ glavni ideal generisan elementom π

Dodajemo da je

$$\boxed{\mathbb{Z}[y]/\langle \pi \rangle \cong \mathbb{Z}/p\mathbb{Z}} \qquad (\text{Iz } 0.)$$

Prsten na d.s. je polje, što znači da je ideal $\langle \pi \rangle$ maksimalan u $\mathbb{Z}[y]$. Ali to znači da je element π prost

[Ako $\pi \mid \beta \cdot \gamma$, za neke $\beta, \gamma \in \mathbb{Z}[y]$, onda $\beta \cdot \gamma \in \langle \pi \rangle$
Ali $\langle \pi \rangle$ je maksimalan, pa time i prost ideal u $\mathbb{Z}[y]$
pa je $\beta \in \langle \pi \rangle$ ili $\gamma \in \langle \pi \rangle$ ($\Leftrightarrow \pi \mid \beta$ ili $\pi \mid \gamma$)]

Dokaz (Iz 0):

Podimo od homomorfizma prstena

$$\psi : \mathbb{Z} \longrightarrow \mathbb{Z}[y]/\langle \pi \rangle$$

$$n \longmapsto n + \langle \pi \rangle$$

Iz uslova

$$p = N(\pi) = \pi \cdot \overline{\pi} \in \langle \pi \rangle \qquad \text{tj.} \quad p \equiv 0 \pmod{\pi}$$

sledi da je

$$\psi(p) = 0 + \langle \pi \rangle \quad = \text{nula element količničkog prstena } \mathbb{Z}[y]/\langle \pi \rangle$$

Sledi $p \in \ker \psi$, pa $\ker \psi$ sadrži i ceo glavni ideal $p\mathbb{Z}$:

$$p\mathbb{Z} \subseteq \ker \psi \subseteq \mathbb{Z}$$

$p\mathbb{Z}$ maksimalan ideal (jer je p racionalan prost)

pa imamo 2 mogućnosti:

1) $\ker \psi = \mathbb{Z}$, što znači da je ψ identičko nula preslikavanje — ali to nije moguće jer je $\psi(1) = 1 + \langle \pi \rangle \neq 0 + \langle \pi \rangle$, jer $1 \notin \langle \pi \rangle$, jer π nije jedinica u $\mathbb{Z}[y]$

2) ako je (pa je) $\boxed{\ker \psi = p\mathbb{Z}}$ Teorema o homomorfizmu za prstene onda daje

$$\mathbb{Z}/\ker\psi = \mathbb{Z}/p\mathbb{Z} \cong \operatorname{im}\psi$$

• Ostaje još da pokažemo da je ψ surjektivan homomorfizam, jer je onda $\operatorname{im}\psi = \mathbb{Z}[\gamma]/\langle\pi\rangle$.

Napišimo

$\pi = r + s\gamma$, $\quad r, s \in \mathbb{Z}$

Neka je

$x + y\gamma \in \mathbb{Z}[\gamma]$ proizvoljni element, $\quad x, y \in \mathbb{Z}$

tj. neka je

$x + y\gamma + \langle\pi\rangle$ proizvoljni koset količ. prstena $\mathbb{Z}[\gamma]/\langle\pi\rangle$.

Ovaj element želimo da pogodimo sa ψ. Ali elementi iz $\operatorname{im}\psi$ su oblika $\psi(m) = m + \langle\pi\rangle$ za $m \in \mathbb{Z}$.

Dakle, želimo da nađemo $a + b\gamma \in \mathbb{Z}[\gamma]$ tj. $a, b \in \mathbb{Z}$ takve da je

$$m := x + y\gamma - \pi\cdot(a+b\gamma) \in \mathbb{Z} \qquad (\text{❀})$$

$$= (x + y\gamma) - (r+s\gamma)(a+b\gamma)$$

$$= x + y\gamma - ar - bs\gamma^2 - rb\gamma - as\gamma$$

$$\gamma^2 = -\gamma - A$$

Koeficijent uz γ mora da bude 0:

$$b\cdot(r-s) + a\cdot s = y \qquad \text{— linearna Diofantova j-na koja ima rešenja jer je}$$

$$\text{NZD}(r-s, s) = \text{NZD}(r, s) = 1$$

(ako bi ovo bilo > 1, $N(\pi)$ ne bi mogla biti prost broj)

• za $(a, b) \in \mathbb{Z}^2$ koji rešavaju ovu j-nu dobijamo iz (❀) $m \in \mathbb{Z}$

za koje je $\psi(m) = x+y\eta + \langle \pi \rangle$ tj. ψ je "na"

(T.2) (ii) $\longrightarrow$ (iii):

Pretpostavimo da je n^2+n+A prost broj za sve

$$0 \leq n \leq \frac{1}{2}\sqrt{\frac{|D|}{3}} - \frac{1}{2}$$

Treba da pokažemo da onda $\mathbb{Z}[y] = \mathbb{Z}\left[\frac{-1+\sqrt{D}}{2}\right]$ ima jedinstvenu faktorizaciju.

Pretpostavimo suprotno, tj. da nema. To znači da postoje elementi u prstenu $\mathbb{Z}[y]$ koji imaju 2 suštinski različite faktorizacije.

Neka je $\alpha \neq 0$, neinvertibilan, element minimalne norme koji ima 2 suštinski različite faktorizacije: na ireducibilne elemente:

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_k = \rho_1 \cdot \ldots \cdot \rho_j$$

Ovde suštinski različite znači da je ili $k \neq j$, ili je $k=j$, ali ne postoji permutacija $\sigma \in S_k$ takva da je

$$\rho_{\sigma(1)} = \pm\pi_1, \quad \rho_{\sigma(2)} = \pm\pi_2, \ldots, \quad \rho_{\sigma(k)} = \pm\pi_k$$

U opštim prstenima, ovde bi stajalo $\rho_{\sigma(t)} = u \cdot \pi_t$, gde je u jedinica prstena; ali ovde su jedine jedinice ± 1

(Z.1)

• Zbog minimalnosti $N(\alpha) > 0$, vidimo da nijedan ireducibilni element π_t nije jednak $\pm \rho_s$, ni za jedno ρ_s iz druge faktorizacije.

| jer ako bi $\pi_t = \pm \rho_s$, element $\frac{\alpha}{\pi_t}$ bi imao dve suštinski različite faktorizacije, a imao bi normu $N\left(\frac{\alpha}{\pi_t}\right) = \frac{N(\alpha)}{N(\pi_t)} < N(\alpha)$, što je u kontradikciji sa izborom α |

(Z.2)

• Odavde sledi: da nijedan od ireducibilnih elemenata

$\pi_1, \pi_2, \dots, \pi_k, \rho_1, \dots, \rho_j$

ne može biti prost element u prstenu $\mathbb{Z}[y]$.

| Npr. ako bi π_1 bio prost, kako $\pi_1 \mid \alpha = \rho_1 \cdot \dots \cdot \rho_j$, sledilo bi da π_1 deli neki od ρ-ova Npr. neka $\pi_1 \mid \rho_1$. To znači da $\exists r \in \mathbb{Z}[y]$ tako da je $\rho_1 = \pi_1 \cdot r$ Ali, ρ_1 je ireducibilan, pa kako π_1 nije jedinica, r mora biti jedinica (tj. ± 1). Ali ovo je upravo u kontradikciji sa prethodnim zaključkom. |

• Dalje, možemo pretpostaviti da je $N(\pi_1) \leq N(\rho_1)$ (ako nije, zamenimo strane dvema faktorizacijama)

• Strategija: za dva elementa $\xi, \gamma \in \mathbb{Z}[y]$ (koji su nam "na raspolaganju", tj. tek ćemo ih pogodno izabrati) definišemo element

$$\alpha' := (\rho_1 \xi - \pi_1 \gamma)\rho_2 \cdots \rho_j \qquad (1)$$

$$= \alpha \xi - \pi_1 \frac{\alpha}{\rho_1} \gamma$$

$$= \pi_1 (\pi_2 \cdots \pi_k \xi - \rho_2 \cdots \rho_j \gamma)$$

Dakle α' ima jednu faktorizaciju na ireducibilne faktore, u kojoj je jedan faktor π_1.

Ideja je da izaberemo ξ tako da $\pi_1 \nmid \rho_1 \xi$.

Onda $\pi_1 \nmid \rho_1 \xi - \pi_1 \gamma$, pa (1) daje faktorizaciju elementa α' na ireducibilne faktore, od kojih nijedan nije $\pm \pi_1$.

Takvo α' dakle ima 2 suštinski različite faktorizacije na ireducibilne faktore.

Ako pritom izaberemo γ tako da je

$$N(\rho_1 \xi - \pi_1 \gamma) < N(\rho_1),$$

onda će

$$N(\alpha') < N(\rho_1) \cdot N(\rho_2) \cdots N(\rho_j) = N(\rho_1 \rho_2 \cdots \rho_j) = N(\alpha)$$

a to je kontradikcija sa izborom elementa α!

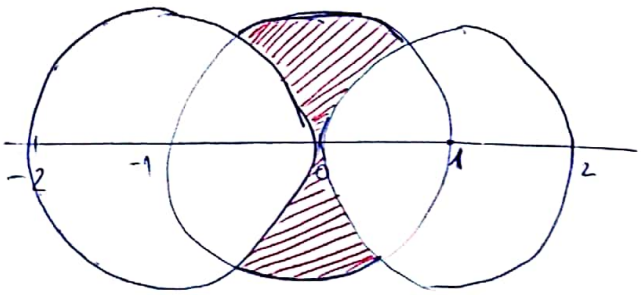
• Dakle, treba da nađemo elemente $\xi, \gamma \in \mathbb{Z}[\eta]$ koji zadovoljavaju sledeća dva uslova:

(U.1) $\pi_1 \nmid \rho_1 \xi$

(U.2) $N(\rho_1 \xi - \pi_1 \gamma) < N(\rho_1) \iff \left| \xi - \frac{\pi_1}{\rho_1} \gamma \right| < 1$

• Zbog pretpostavke da je $N(\pi_1) \leq N(\rho_1)$ imamo da je $N\left(\frac{\pi_1}{\rho_1}\right) = \frac{N(\pi_1)}{N(\rho_1)} \leq 1 \iff \left|\frac{\pi_1}{\rho_1}\right| \leq 1$ tj.

$\frac{\pi_1}{\rho_1}$ pripada zatvorenom jediničnom disku (sa centrom u 0)



Slučaj 1: $\frac{\pi_1}{\rho_1}$ ne leži u crvenom (šrafiranom) regionu

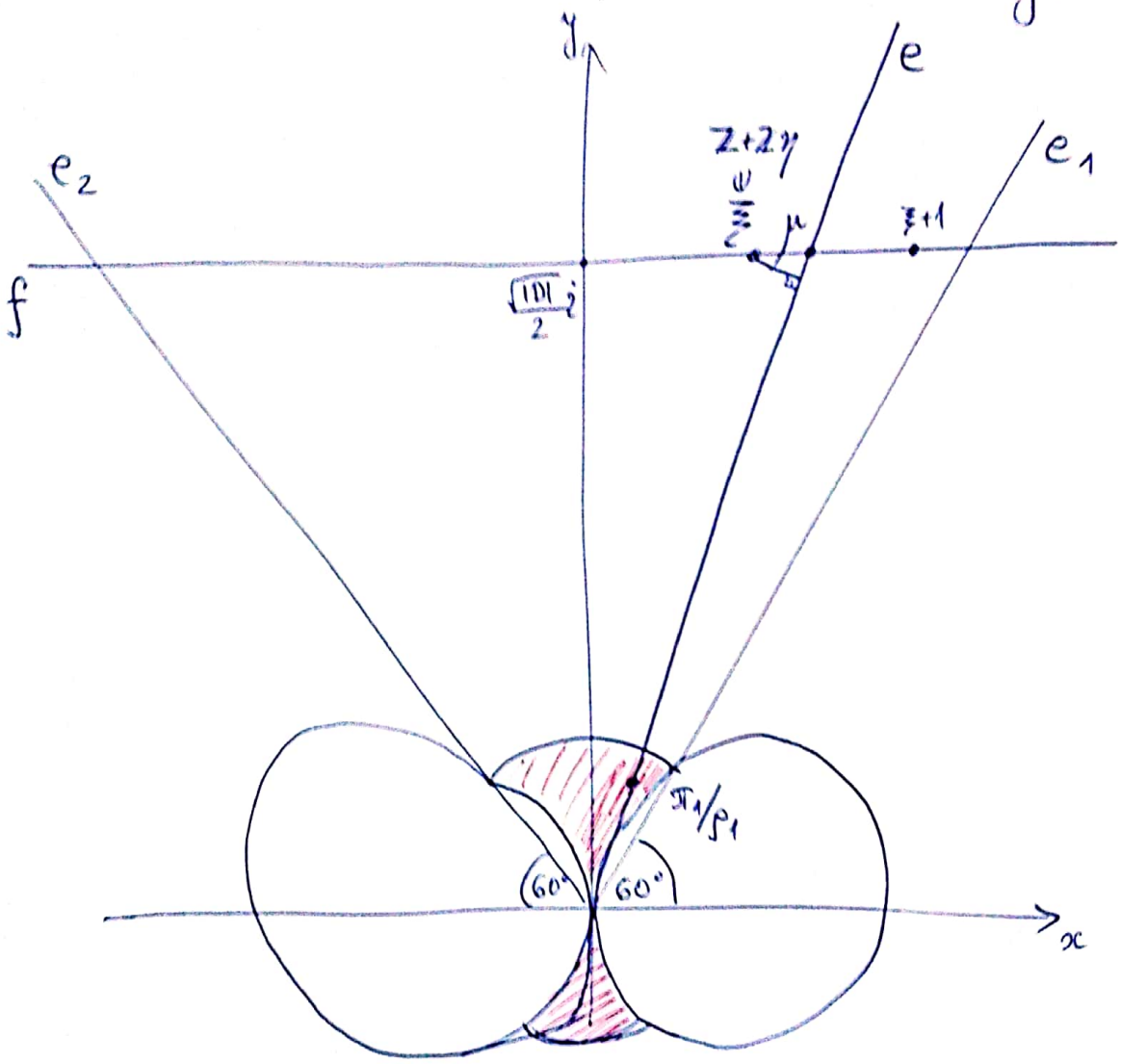
To znači da je ili za $\xi = 1$ ili za $\xi = -1$ ispunjeno

$$\left| \xi - \frac{\pi_1}{\rho_1} \right| < 1$$

pa su (U.1) : (U.2) ispunjeni za to ξ $\underbrace{\{1, -1\}}$; $\gamma = 1$

(U.1) je ispunjen jer je $\pi_1 \neq \pm\rho_1, \pm\rho_2, \ldots, \pm\rho_t$ prema dokazanom pa : $\pi_1 \nmid \pm\rho_1$

Slučaj 2: $\frac{\pi_1}{f_1}$ pripada crvenom regionu (ili je na gornjoj granici)



e_1 = polprava pod uglom od 60° u odnosu na pozitivan x-ose

e_2 = polprava pod uglom od 120° —||—

e - polprava od 0 kroz tačku $\frac{\pi_1}{f_1}$

- Onda se tačka $\frac{\pi_1}{f_1}$ nalazi u zatvorenom uglu $\sphericalangle e_1 O e_2$ (veličine 60°)

$f :=$ horizontalna prava $\left\{ \mathrm{Im}(z) = \frac{\sqrt{|D|}}{2} \right\}$

- prva horizontalna prava iznad x-ose koja sadrži tačke prstena $\mathbb{Z} + \mathbb{Z}y = \mathbb{Z}[y] \subseteq \mathbb{C}$ $\left(y = -\frac{1}{2} + \frac{\sqrt{D}}{2} = \frac{-1}{2} + \frac{\sqrt{|D|}}{2} i \right)$

$\mu := e \cap f \in \mathbb{C}$

• Dužina intervala na pravoj f između e_1 i e_2 je

$$\frac{2}{\sqrt{3}} \cdot \frac{\sqrt{|D|}}{2} = \sqrt{\frac{|D|}{3}} \geq \sqrt{\frac{7}{3}} > 1 \qquad \left(\text{jer je } A \geq 2 \text{ pa je } D \leq -7\right)$$

Dalje postoji tačka na pravoj f i u zatvorenom $\sphericalangle e_1 O e_2$ koja pripada i pruzi $\mathbb{Z}[y] = z + 2y$.

Od svih takvih tačaka izaberimo jednu, označimo je sa ξ, za koju je rastojanje $|\xi - \mu|$ minimalno.

• Sledeći korak: dokažimo da je za tako izabrano ξ, rastojanje od ξ do prave e, $\boxed{d(\xi, e) < \frac{\sqrt{3}}{2}}$ (2)

a) • ako: $\xi+1$ i $\xi-1$ (i ξ) pripadaju uglu $\sphericalangle e_1 O e_2$ onda je (situacija sa crteža — slično i sve ostale)

$$|\xi - \mu| \leq |(\xi+1) - \mu| \quad \rightarrow \quad |\xi - \mu| \leq \frac{1}{2}$$

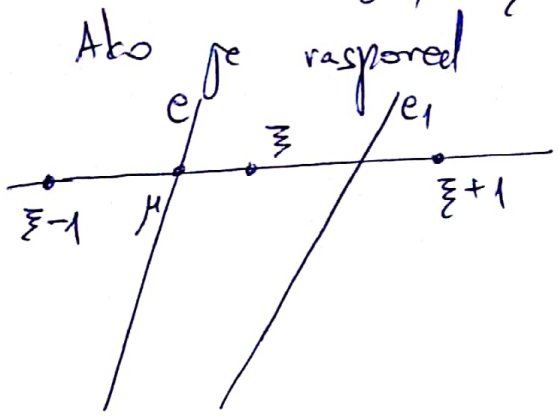
pa je:

$$d(\xi, e) = \text{kateta} \leq \text{hipotenuza} = |\xi - \mu| \leq \frac{1}{2} < \frac{\sqrt{3}}{2}$$

b) • zato pretp. da $\xi+1$ leži van $\sphericalangle e_1 O e_2$ (slučaj "sa druge strane", tj. da $\xi - 1$ leži van ugla radimo analogno)

U ovom slučaju, $\xi - 1$ mora pripadati uglu.

b.1) Ako je raspored



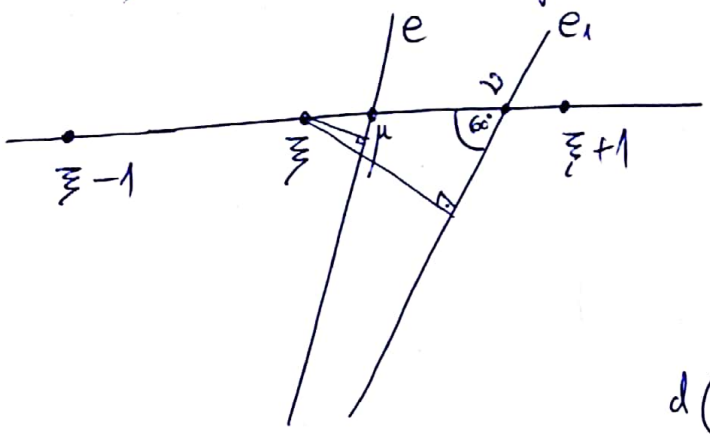
zbog pretpostavke o minimalnosti rastojanja od ξ do μ, opet je

$|\xi - \mu| \leq |(\xi - 1) - \mu|$

pa je $|\xi - \mu| \leq \frac{1}{2}$

Ocena kao u slučaju a)

b.2) Ako je raspored



označimo

$\nu := e_1 \cap f \in \mathbb{C}$

Onda je

$|\xi - \nu| < 1$

$\rightarrow$

$$d(\xi, e_1) < \frac{\sqrt{3}}{2} \cdot 1 = \frac{\sqrt{3}}{2}$$

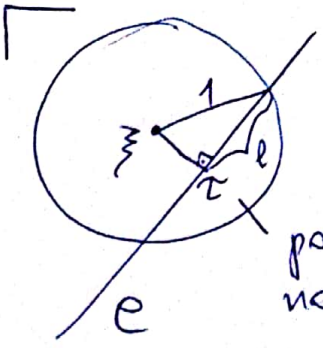
Ali pri ovom rasporedu, normala iz ξ do e_1 seče pravu e (između ξ i podnožja normale) pa sledi

$$d(\xi, e) \leq d(\xi, e_1) < \frac{\sqrt{3}}{2}$$

(kateta $\leq$ hipotenuza)

čime smo završili dokaz (2). ∎

- Ali (2) znači da jedinični disk (tj. poluprečnika = 1) sa centrom u ξ seče pravu e po segmentu dužine > 1



$$d(\xi, e) = |\xi, \hat{\tau}| < \frac{\sqrt{3}}{2}$$

podnožje normale

Pitagorina teorema: $\ell^2 = 1^2 - |\xi - \tau|^2 > 1 - \frac{3}{4} = \frac{1}{4}$

$\rightarrow \ell > \frac{1}{2}$ ∎

Vratimo se na glavni cilj:

$$\left|\frac{\pi_1}{\rho_1}\right| \leq 1$$

pa će celobrojni umnošci $\frac{\pi_1}{\rho_1}$, $2\frac{\pi_1}{\rho_1}$, $3\frac{\pi_1}{\rho_1}$, $4\frac{\pi_1}{\rho_1}$, ... svi ležati na polupravoj e – a kako su rastojanja između njih ≤ 1, a širina preseka e sa diskom oko ξ veća od 1, sledi da $\exists\, \gamma \in \mathbb{Z}$ t.d.

$$\gamma \cdot \frac{\pi_1}{\rho_1} \in e \cap \{\text{otvoren disk poluprečnika 1, sa centrom u } \xi\}$$

tj.

$$\left|\xi - \gamma \cdot \frac{\pi_1}{\rho_1}\right| < 1 \qquad (3)$$

- Dakle, ovim smo izabrali tačke $\xi, \gamma \in \mathbb{Z}+\mathbb{Z}y$ koje zadovoljavaju (3), a to je upravo uslov (U.2). Dokažimo da je zadovoljen i uslov (U.1). Za to će biti dovoljno da dokažemo da će izabrano ξ biti prost element u prstenu $\mathbb{Z}[y]$.

Jer, ako je ξ prost, a (U.1) ne važi, tj. ako:

$\pi_1 \mid \rho_1 \xi$,

$\exists\, \kappa \in \mathbb{Z}[y]$ takav da $\rho_1 \xi = \pi_1 \kappa$. $\longrightarrow$

(ξ prost)

$\xi \mid \pi_1$ ili $\xi \mid \kappa$.

- Ako bi $\xi \mid \pi_1$, kako je π_1 ireducibilan, imali bismo da je $\pi_1 = \xi \cdot u$ — mora biti jedinica (— ξ prost (pa nije jedinica)) tj. $\pi_1 = \pm\xi$

Ali to bi značilo da je π_1 prost element (jer je ξ prost). Ovo je kontradikcija sa 2. zaključkom na str. -6- (Z.2) da nijedan π_i nije prost.

- Dakle, mora $\xi \mid \kappa$: $\kappa = \xi \kappa_1$ ($\kappa_1 \in \mathbb{Z}[y]$) i onda

$$\rho_1 \xi = \pi_1 \cdot \xi \kappa_1 \quad / \text{podelimo sa } \xi$$

$$\rho_1 = \pi_1 \cdot \kappa_1$$ — mora biti jedinica ($= \pm 1$)

(ρ_1: ireducibilan; π_1: ireducibilan pa nije jedinica)

tj. sledilo bi da je $\rho_1 = \pm \pi_1$, što je kontradikcija sa 1. zaključkom na str. -6- (Z.1).

- U oba slučaja smo dobili kontradikciju koja dokazuje: ako je ξ prost el, mora važiti uslov (U.1).

Finalni korak: ξ je prost:

$\xi \in (\mathbb{Z} + \mathbb{Z}y) \cap f$ pa je oblika

$\xi = n + y$, za neko $n \in \mathbb{Z}$. $\xi = n - \frac{1}{2} + \frac{\sqrt{|D|}}{2} i$

Dodatno ξ pripada zatvorenom uglu $\sphericalangle e_1 O e_2$ pa je

$$|\mathrm{Re}\, \xi| \leq \frac{1}{2}\sqrt{\frac{|D|}{3}} \quad ;$$

$$N(\xi) = \left(n - \tfrac{1}{2}\right)^2 - \left(n - \tfrac{1}{2}\right)\frac{\sqrt{|D|}}{2} + A\frac{|D|}{4}$$

$$= n^2 - n + \frac{1}{4}$$

$$\left| n - \frac{1}{2} \right| \leq \frac{1}{2} \sqrt{\frac{|D|}{3}}$$

;

$$N(\xi) = N(n+y) = n^2 - n + A$$

$$= (n-1)^2 + (n-1) + A$$

ali ;

$$\left| (n-1) + \frac{1}{2} \right| = \left| n - \frac{1}{2} \right| \leq \frac{1}{2} \sqrt{\frac{|D|}{3}}$$

- ako je $n > 0$, nejednakost je

$$n - 1 \leq \frac{1}{2} \sqrt{\frac{|D|}{3}} - \frac{1}{2}$$

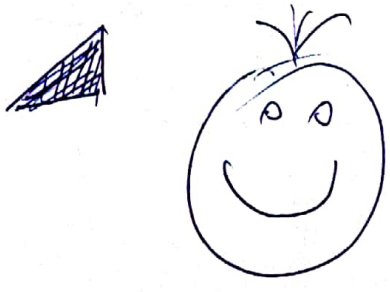
- ako je $n < 0$, nejednakost je

$$-n + \frac{1}{2} \leq \frac{1}{2} \sqrt{\frac{|D|}{3}} \quad \text{tj.} \quad -n \leq \frac{1}{2} \sqrt{\frac{|D|}{3}} - \frac{1}{2} .$$

U oba slučaja $n-1$, odnosno $-n$ su prirodni brojevi iz intervala iz pretpostavke (ii), pa sledi da je

$N(\xi)$ racionalan prost broj.

Ali onda (L.5) garantuje da je ξ i prost element u prstenu $\mathbb{Z}[y]$.



$A = 2$ $\quad D = -7$

n	n^2+n+2
0	2 – prost
1	

(T.2)(i) ispunjeno $\rightarrow$

$\mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$ ima jedinstvenu faktorizaciju

UFD

$A = 3$ $\quad D = -11$

n	n^2+n+3
0	3
1	5

$>$ prosti

$\mathbb{Z}\left[\frac{-1+\sqrt{-11}}{2}\right]$ je UFD

$A = 4$ $\quad D = -15$

(T.2) $\rightarrow \mathbb{Z}\left[\frac{-1+\sqrt{-15}}{2}\right]$ nije UFD!

n	n^2+n+4
0	4 – nije prost

$\gamma = \frac{-1+\sqrt{-15}}{2}$, $\quad \bar{\gamma} = \frac{-1-\sqrt{-15}}{2} = -1-\gamma$

$\gamma \cdot \bar{\gamma} = \frac{-1+\sqrt{-15}}{2} \cdot \frac{-1-\sqrt{-15}}{2} = 4 = 2 \cdot 2$

Dakle 4 se u prstenu $\mathbb{Z}\left[\frac{-1+\sqrt{-15}}{2}\right]$ faktorizira na 2 načina

$\gamma \cdot (-1-\gamma) = 2 \cdot 2 \qquad (4)$

- Npr. 2 je ireducibilan element u $\mathbb{Z}\left[\frac{-1+\sqrt{-15}}{2}\right]$:

$2 = \alpha \cdot \beta$, $\quad \alpha, \beta \in \mathbb{Z}[\gamma]$

$N(2) = N(\alpha) \cdot N(\beta)$

$\parallel$

4

Ako je $N(\alpha) = 1$ ili $N(\beta) = 1$

onda je α jedinica ili je β jedinica.

Ako je $N(\alpha)=N(\beta)=2$,

$\alpha = x+y\sqrt{y}$, $x,y\in\mathbb{Z}$

$N(\alpha) = x^2 - xy + 4y^2 = 2$

$\underbrace{\left(x-\frac{y}{2}\right)^2}_{\geq 0} + \underbrace{\frac{15}{4}y^2}_{>3 \text{ za } |y|\geq 1} = 2$

Ali, za $y=0$
$x^2=2$
nema rešenja u $\mathbb{Z}$.

Dakle 2 je ireducibilan!

I očigledno, $2 \neq \pm y, \pm(1+y)$, pa (4) daje dve suštinski različite faktorizacije elementa $4\in\mathbb{Z}[y]$.

Dokaz da je y ireducibilni element u $\mathbb{Z}[y]$:

$y = \alpha\cdot\beta$

Opet isto: $N(y)=4$, a $N(\alpha)=2$ nema rešenja u $\mathbb{Z}[y]$

$A=5$ $\quad D=-19$

n	n^2+n+5	
0	5	} svi prosti
1	7	
2	11	
3	17	

(T.2) $\rightarrow$ $\mathbb{Z}\left[\frac{-1+\sqrt{-19}}{2}\right]$ je UFD.

$A=6$ itd. za sve složene $A\geq 2$ znamo zbog $0^2+0+A=A$ da $\mathbb{Z}[y]$ nije UFD.

$A = 7$, $D = -27$

n	n^2+n+7
0	7
1	9 – nije prost

(T2) $\rightarrow$ $\mathbb{Z}\left[\frac{-1+\sqrt{-27}}{2}\right]$ nije UFD.

$A = 11$ $D = -43$

n	n^2+n+11	
0	11	} prosti
1	13	
2	17	
3	23	
4	31	
5	41	
6	53	
7	67	
8	83	
9	101	

(T2) $\rightarrow$ $\mathbb{Z}\left[\frac{-1+\sqrt{-43}}{2}\right]$ je UFD.

$A = 13$ $D = -51$

n	n^2+n+13
0	13
1	15 – nije prost

(T2) $\rightarrow$ $\mathbb{Z}\left[\frac{-1+\sqrt{-51}}{2}\right]$

nije UFD.

itd.

- Daljim računom, proverava se da su uslovi (i) ili (ii) (T.2) ispunjeni za $A = 2, 3, 5, 11, 17$ i 41.

Dakle imamo sledeću posledicu

Posledica 6. Prsten $\mathbb{Z}\left[\frac{-1+\sqrt{D}}{2}\right]$ je domen sa jedinstvenom faktorizacijom (UFD) za

$$D = -7, -11, -19, -43, -67, -163. \quad (5)$$

- Provera za veće vrednosti A, $A > 41$: dobar grad da računamo, nè daje još primera koji zadovoljavaju npr. uslov (ii).

Problem: da li je lista u Posledici 6 kompletna?

Ovaj problem je postavio još Gauss, u njegovoj knjizi *Disquisitiones Arithmeticae* (napisana 1798. objavljena 1801.)

i zove se

"Gausov problem klasnog broja 1"

- 1933. Lehmer je pokazao da ako postoji još neko A u listi (5), ono mora biti veliko, i to

$$|D| > 5 \cdot 10^9$$

- 1934. Heilbronn i Linfoot su pokazali da listi (5) može da nedostaje najviše jedna vrednost!

• Problem je konačno rešen 1952.

Teorema [Kurt Heegner, 1952.]

Ako je $A > 41$, $\mathbb{Z}[\gamma]$ nema jedinstvenu faktorizaciju.

Drugačije, ako je $A \geq 2$ takvo da je

$n^2 + n + A$ prost za sve $0 \leq n < A-1$,

onda je $A \leq 41$.

Dokaz je koristio teoriju modularnih funkcija. |

Drugi dokaz je dao Harold Stark 1969.