$\square + \square$

$\boxed{n = x^2 + y^2}$, $x, y, n \in \mathbb{Z}_{\geq 0}$

Koji prirodni brojevi n se mogu predstaviti kao zbir dva kvadrata?

T.1 Prirodan broj n je oblika $\square+\square$ $\Longleftrightarrow$ svaki prost $p \mid n$ koji je $\equiv 3 \pmod 4$ se pojavljuje u faktorizaciji broja n sa parnim eksponentom.

Primer

$13 = 3^2 + 2^2$ $\quad$ $13 \equiv 1 \pmod 4$

14 nije $\square+\square$ $\quad$ $14 = 2 \cdot 7^1$ ← neparno $\quad$ $7 \equiv 3 \pmod 4$

$18 = 3^2 + 3^2$ $\quad$ $18 = 2 \cdot 3^2$ ← parno

22 nije $\square+\square$ $\quad$ $22 = 2 \cdot 11^1$ $\quad$ $11 \equiv 3 \pmod 4$

$29 = 5^2 + 2^2$ $\quad$ $29 \equiv 1 \pmod 4$

27 nije $\square+\square$ $\quad$ $27 = 3^3$ ← neparno

- $i^2 = -1$

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ $\quad$ prsten Gausovih celih

Norma N na $\mathbb{Z}[i]$:

$\alpha = a + bi$, $\quad N(\alpha) = \alpha \cdot \bar{\alpha} = |\alpha|^2$, $\quad N(\alpha) = N(a+bi) = a^2 + b^2$

$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$, $\quad \forall \alpha, \beta \in \mathbb{Z}[i]$

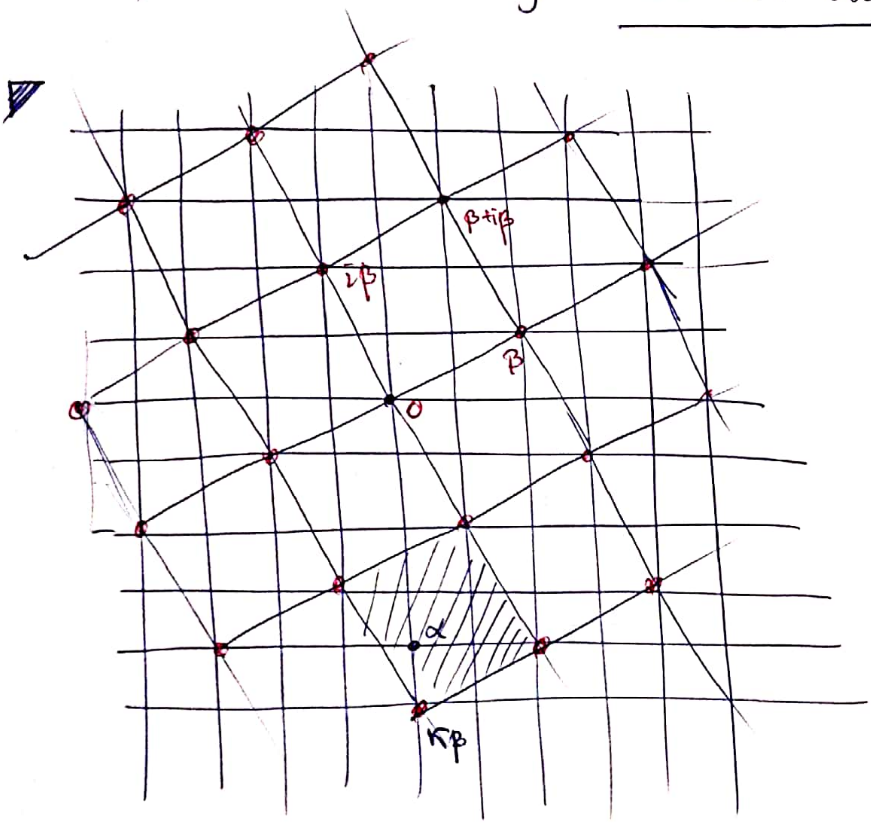
- Element $u \in \mathbb{Z}[i]$ je jedinica ako $\exists v \in \mathbb{Z}[i]$ tako da $uv = 1$. El. u je jedinica $\Longleftrightarrow N(u) = 1 \Longleftrightarrow u \in \{\pm 1, \pm i\}$

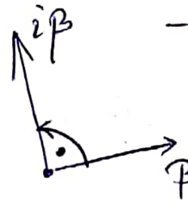
Tv.2 Ako su $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, onda postoje $\kappa, \rho \in \mathbb{Z}[i]$ takvi da je

$$\boxed{\alpha = \beta \cdot \kappa + \rho \quad \text{i} \quad \mathcal{N}(\rho) < \mathcal{N}(\beta).}$$

Dakle, prsten $\mathbb{Z}[i]$ je <u>euklidski domen</u>.

▼





$i\beta$ – zarotiran za $90°$

Posmatrajmo skup (za fiksirano β)

$$\Lambda := \{\kappa \cdot \beta \mid \kappa \in \mathbb{Z}[i]\} \subseteq \mathbb{Z}[i]$$

$\kappa = k_1 + k_2 i$, $\quad k_1, k_2 \in \mathbb{Z}$

$$\kappa \cdot \beta = (k_1 + k_2 i)\beta = k_1 \cdot \beta + k_2 \cdot \beta i$$

$0, \beta, i\beta, \beta + i\beta$ – temena kvadrata, pa je Λ "kvadratna rešetka", kao na slici

Proizvoljni $\alpha \in \mathbb{Z}[i]$ mora upasti u jedan od kvadrata rešetke Λ pa je rastojanje α do najbližeg temena $\kappa\beta$ tog kvadrata

$$|\alpha - \kappa\beta| \leq \frac{|\beta| \cdot \sqrt{2}}{2} < |\beta| \quad \to \quad \mathcal{N}(\underbrace{\alpha - \kappa\beta}_{=\rho}) < \mathcal{N}(\beta)$$

(polovina dijagonale)

Najbliže teme ne mora biti jedinstveno, pa odabir κ, ρ nije jedinstven. ◢

$\mathbb{Z}[i]$ je euklidski, pa je glavnoidealski, pa je UFD.
Dakle, svaki ireducibilni el. prstena $\mathbb{Z}[i]$ je i prost.

(L.3) Ako su m, n zbirovi 2 kvadrata, onda je to i mn.

▼ $m = a^2+b^2 = \mathcal{N}(a+bi)$, $n = c^2+d^2 = \mathcal{N}(c+di) \longrightarrow$

$$mn = \mathcal{N}(a+bi)\,\mathcal{N}(c+di) \underset{\substack{\text{multiplikativnost} \\ \text{norme}}}{=} \mathcal{N}((a+bi)(c+di)) = (ac-bd)^2+(ad+bc)^2$$ ▲

(L.4) Ako je $p = 4k+3$ prost, $k \in \mathbb{Z}_{\geq 0}$ i $a, b \in \mathbb{Z}$ taki da $p \mid a^2+b^2$, onda $p \mid a$ i $p \mid b$.

▼ Ako $p \nmid a$, $a^2+b^2 \equiv 0 \pmod{p} \rightarrow (ba^{-1})^2 \equiv -1 \pmod{p}$
tj. kongruencija $x^2 \equiv -1 \pmod{p}$ ima rešenje $u \pmod{p}$.
Grupa $(\mathbb{Z}/p\mathbb{Z})^\times$ je ciklična i neka je g jedan njen generator ("primitivni koren" modulo p). Onda je

$u = g^j \pmod{p}$ za neko $0 < j < p-1$

• $\left(g^{\frac{p-1}{2}}\right)^2 \equiv g^{p-1} \equiv 1 \pmod{p} \rightarrow g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

Ali nije $+1$, jer je red el. g $p-1$, a ne $\frac{p-1}{2}$.

Dakle $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, pa

$$g^{2j} \equiv u^2 \equiv -1 \equiv g^{\frac{p-1}{2}} \pmod{p} \rightarrow \boxed{\underbrace{2j}_{\text{parno}} \equiv \underbrace{\frac{p-1}{2}}_{\substack{\text{neparno} \\ (\text{za } p=4k+3)}} \mod \underbrace{(p-1)}_{\text{parno}}}$$

Kontradikcija.
Sled: $p \mid a$, i onda $p \mid b$. ▲

T.5 [Fermat] Neparan prost broj je zbir 2 kvadrata akko $p = 4k+1$, $k \in \mathbb{N}$.

$(\rightarrow)$ $p = x^2 + y^2$ Ali $x^2 \equiv 0,1 \pmod 4$, pa $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$

p - neparan, prost $\rightarrow$ $1 \pmod 4$ jedina mogućnost

$(\leftarrow)$ $p = 4k+1$

- U ovom slučaju kongruencija $x^2 \equiv -1 \pmod p$ je rešiva.

  Npr. Wilson-ova teorema $(p-1)! \equiv -1 \pmod p$

  $j(p-j) \equiv -j^2 \pmod p$, pa uparivanjem j i $p-j$:

  $$-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)! \right)^2 \equiv a^2 \pmod p$$

  za $a = \left(\frac{p-1}{2}\right)!$

- Sada, za $\forall x \in \mathbb{Z}$

  $x^2(a^2+1) \equiv 0 \pmod p \rightarrow x^2 + (ax)^2 \equiv 0 \pmod p$

  Ako je y ceo broj takav da $y \equiv \pm ax \pmod p$, onda

  $p \mid x^2 + y^2$

- Tvrdim: $\exists x, y \in \{1, 2, \dots, \lfloor \sqrt{p} \rfloor\}$ takvi da $y \equiv \pm ax \pmod p$

  $A := \{ax - y \mid 0 \leq x, y \leq \lfloor \sqrt{p} \rfloor\}$

  Broj mogućnosti za (x,y) je $(1 + \lfloor \sqrt{p} \rfloor)^2 > p$,

  pa postoje različiti $(x,y) \neq (x', y')$

  $ax - y \equiv ax' - y' \pmod p$

$$y-y' \equiv a(x-x') \pmod p$$

$$-\lfloor\sqrt p\rfloor \leq y-y',\ x-x' \leq \lfloor\sqrt p\rfloor$$

Možemo pretp. $y-y' \geq 0$, $x-x' \geq 0$, ali je onda

$$y-y' \equiv \pm a(x-x') \pmod p$$

Bar jedan od $x-x'$, $y-y' > 0$ (jer su parovi različiti), ali je onda i drugi, jer je $a \not\equiv 0 \pmod p$.

- Za ovako nađene $x, y \in \{1, 2, .., \lfloor\sqrt p\rfloor\}$

$$p \mid x^2+y^2 \leq \lfloor\sqrt p\rfloor^2 + \lfloor\sqrt p\rfloor^2 < 2p \implies x^2+y^2 = p.$$

Dokaz T1.

Ako je $n = n_1 \cdot n_2^2$, n_1-beskvadratan i $n_1 \in \square+\square$, onda je i $n \in \square+\square$.

Na osnovu T5 svaki $p = 4k+1 \in \square+\square$, $2 = 1^2+1^2 \in \square+\square$, pa je na osnovu L.3 svaki proizvod ovih takođe $\square+\square$.

($\leftarrow$) Ako je faktorizacija navedenog oblika, svi prosti brojevi p koji dele n_1 (= beskvadratni deo od n) su oblika $4k+1$ pa tvrđenje sledi iz gornjeg razmatranja.

($\rightarrow$) $n \in \square+\square$, $n = a^2+b^2$

Treba da pokažemo: ako je $p = 4k+3$ i $p^\alpha \| n$, onda je α parno.

$n = p^\alpha m, \qquad (m,p) = 1$

$\xrightarrow{L.4}$ $p \mid a$ i $p \mid b$, $\quad a = pa_1, \quad b = pb_1$

Onda je

$$p^\alpha m = n = (pa_1)^2 + (pb_1)^2 = p^2(a_1^2 + b_1^2) \longrightarrow$$

$$p^{\alpha-2} m = a_1^2 + b_1^2$$

- Ako je α neparno, ponavljanjem ovog procesa dolazimo do

$$pm = a_2^2 + b_2^2, \quad \text{za neke } a_2, b_2 \in \mathbb{Z}.$$

$\xrightarrow{L.4}$ $p \mid a_2$ i $p \mid b_2$ $\longrightarrow$ $p^2 \mid pm$ $\lightning$.

Dakle, α mora biti parno.

Prosti elementi u prstenu $\mathbb{Z}[i]$

- Kao i ranije, imamo da ako je $N(\pi) \in \mathbb{Z}$ racionalan prost, onda je π prost el. u $\mathbb{Z}[i]$

Npr. $N(1+i) = 2$, pa je $1+i$ prost el. u $\mathbb{Z}[i]$
Isto i za $1-i$ $\qquad 1-i$

Ako je $p \in \mathbb{Z}$, $p \equiv 1 \pmod 4$, iz T.5 slijedi da je

$$p = a^2 + b^2, \quad \text{za neke } a, b \in \mathbb{Z}$$
$$= N(a+bi), \text{ pa je } a+bi \text{ prost u } \mathbb{Z}[i].$$

- Neka je sada $p = 4k+3 \in \mathbb{Z}$ racionalan prost
Ako je

$$p = z \cdot w, \qquad z, w \in \mathbb{Z}[i]$$

— proizvoljna faktorizacija

Uzmemo norme:

$p^2 = \mathcal{N}(p) = \mathcal{N}(z)\mathcal{N}(w) \rightarrow p \mid \mathcal{N}(z)$ ili $p \mid \mathcal{N}(w)$.

Neka $p \mid \underset{a+bi}{\mathcal{N}(z)} = a^2+b^2$. Iz (L.4) $\rightarrow$ $p \mid a$ i $p \mid b$

pa i $p^2 \mid a^2+b^2 = \mathcal{N}(z) \rightarrow \mathcal{N}(z) = p^2$, $\mathcal{N}(w) = 1$

tj. w mora biti jedinica u prstenu $\mathbb{Z}[i]$.

Sledi da je $p = 4k+3$ ireducibilan (pa i prost) u $\mathbb{Z}[i]$.

T6 [Teorema o prostim elementima u $\mathbb{Z}[i]$]

Elementi

- $1 \pm i$
- $a+bi$, za $a, b \in \mathbb{Z}$, $a^2+b^2 = p = 4k+1$ — racionalan prost
- $p = 4k+3$

i njima asocirani elementi ($\rho_1 \sim \rho_2$ su asocirani ako je $\rho_1 = u \cdot \rho_2$, za jedinicu $u \in \{\pm 1, \pm i\}$)

čine potpunu listu svih prostih elemenata prstena $\mathbb{Z}[i]$.

◸ Neka je ϖ prost el. u $\mathbb{Z}[i]$.

$\varpi \mid \varpi \cdot \overline{\varpi} = \mathcal{N}(\varpi) \in \mathbb{Z}$

$\mathcal{N}(\varpi) = p_1 p_2 \cdots p_k$ — faktorizacija na proste u $\mathbb{Z}$ (mogu se ponavljati)

Dakle $\varpi \mid p_1 p_2 \cdots p_k$ u $\mathbb{Z}[i]$, i ϖ je prost $\rightarrow$

$\varpi \mid p_j$ za neko $1 \le j \le k$.

Dakle svaki prost ω u $\mathbb{Z}[i]$ mora deliti bar jedan racionalan prost p.

→ ako je $p = 4k+1$ ili $p=2$, onda je

$$\omega \mid p = a^2+b^2 = (a+bi)(a-bi) \rightarrow \omega \mid a+bi \text{ ili } \omega \mid a-bi$$

ireducibilni

ω prost

$\omega \sim a+bi$ ili $\omega \sim a-bi$

(moraju biti asocirani, jer su oba ireducibilna)

→ ako je $p = 4k+3$, napišimo $\boxed{\omega = m+ni}$

Iz $\omega \mid p \longrightarrow m^2+n^2 = N(\omega) \mid N(p) = p^2$

$\longrightarrow m^2+n^2 \in \{1, p, p^2\}$

- $m^2+n^2=1 \longrightarrow N(\omega)=1$ tj. ω bi bila jedinica – što je nemoguće, jer je ω ireducibilan.
- $m^2+n^2=p$, onda opet $\xrightarrow{L.4}$ $p \mid m$ i $p \mid n$, ali onda i $p^2 \mid m^2+n^2=p$ $\lightning$
- $m^2+n^2=p^2$ – jedina mogućnost

Opet $\xrightarrow{L.4}$ $p \mid m$ i $p \mid n$ tj. $m = pm_1$, $n = pn_1$, $m_1, n_1 \in \mathbb{Z}$

$$p^2 = (pm_1)^2 + (pn_1)^2 = p^2(m_1^2+n_1^2) \rightarrow$$

$m_1^2+n_1^2 = 1 \rightarrow m_1 + in_1$ je jedinica u $\mathbb{Z}[i]$ tj.

$$\omega = m+ni = p(m_1+in_1) \sim p$$

◢

$p = 4k+1$ racionalan prost

$p = a^2 + b^2$

Ako bismo imali 2 ovakve reprezentacije

$$a^2 + b^2 = a_1^2 + b_1^2$$

$$(a+bi)(a-bi) = (a_1 + b_1 i)(a_1 - b_1 i)$$

kako su svi $a \pm bi$, $a_1 \pm b_1 i$ ireducibilni, sledi da je $a+bi \sim a_1 + b_1 i$ ili $a+bi \sim a_1 - b_1 i$ tj.

$$a+bi = u(a_1 \pm b_1 i), \quad u \in \{\pm 1, \pm i\} \longrightarrow \{|a|, |b|\} = \{|a_1|, |b_1|\}.$$

Zato je reprezentacija $p = a^2 + b^2$ uz uslov $\boxed{a > b > 0}$ jedinstvena.

- Uvedimo oznaku: $\omega_p := a + bi$. (za navedene jedinstvene a, b)

Proste elemente

$1+i$, ω_p, $\overline{\omega}_p$ (za proste $p = 4k+1$) i proste $q = 4k+3$

zovemo "standardni" prosti elementi prstena $\mathbb{Z}[i]$.

(T.7) Svaki element prstena Gausovih celih $\mathbb{Z}[i]$ se može napisati u obliku

$$u \cdot m \cdot (1+i)^a \prod_{p \equiv 1 \pmod 4} \omega_p^{e_p} \cdot \overline{\omega}_p^{f_p}$$

na jedinstven način — do na permutaciju faktora. Ovde je:

$u \in \{1, -1, i, -i\} = \mathbb{Z}[i]^\times$ jedinica prstena

$m \in \mathbb{Z}$, - proizvod racionalnih prostih oblika $4k+3$

$\prod_{p \equiv 1 (4)}$ — konačan proizvod po nekim racionalnim prostim oblika $4k+1$

Primer

$$2 = -i(1+i)^2$$

$$12 = -3(1+i)^4$$

$$60 = -3(1+i)^4(2+i)(2-i)$$

Funkcija $r(n)$

$r(n)$ = broj predstavljanja $n\in\mathbb{N}$ kao zbira 2 kvadrata

$= \#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2=n\}$

$=$ # tačaka sa celobrojnim koordinatama na krugu $\{|z|=\sqrt{n}\}$

$$n = m\cdot 2^{\alpha}\cdot \prod_{\substack{p\mid n\\ p\equiv 1\,(4)}} p^{\beta_p}$$

– faktorizacija u $\mathbb{Z}$, gde je m = proizvod (sa ponavljanjem) svih prostih delioca od n oblika $4k+3$

Iz T.1 sledi $r(n)=0$ ako m nije kvadrat ($m\neq\square$)

T.8 Za svako $n\in\mathbb{N}$ je

$$\boxed{r(n)=\begin{cases}0, & \text{ako } m\neq\square\\ 4\prod\limits_{\substack{p\equiv 1(4)\\ p\mid n}}(1+\beta_p), & \text{ako je } m=\square\end{cases}}$$

▼

$n = x^2+y^2 = N(x+iy)$ pa je i $r(n) = \#\{z\in\mathbb{Z}[i] \mid N(z)=n\}$

Svaki takav $z=x+iy$ ima svoju faktorizaciju u obliku iz T.7

tj.

$$z = u \cdot k \cdot (1+i)^a \prod_{p\equiv 1(4)} \omega_p^{e_p} \overline{\omega}_p^{f_p}$$

$\in\{\pm 1, \pm i\}$

konačan proizvod

proizvod prostih oblika $4k+3$

Norma je multiplikativna:

$$n = N(z) = N(k)\, N(1+i)^a \prod_{p\equiv 1(4)} N(\omega_p)^{e_p} N(\overline{\omega}_p)^{f_p}$$

$$= k^2 \cdot 2^a \prod_{p\equiv 1(4)} p^{e_p+f_p} = n = m \cdot 2^\alpha \prod_{p\equiv 1(4)} p^{\beta_p}$$

Odavde je:

$m = k^2$, $a = \alpha$ i za sve racionalne proste p oblika $4k+1$ je

$$\boxed{e_p + f_p = \beta_p}$$

rešenja ovoga je $1+\beta_p$

dakle, a i k su fiksirani

Na kraju, imamo 4 mogućnosti za jedinicu u, što daje formulu. ◢

<u>Primer</u> $180 = 3^2 \cdot 2^2 \cdot (2+i)(2-i)$

Mogućnosti za $z \in \mathbb{Z}[i]$, norme $N(z) = 180$ su dakle

$u \cdot 3 \cdot (1+i)^2 \cdot (2+i) = u(-6+12i)$

$u \cdot 3 \cdot (1+i)^2 \cdot (2-i) = u(6+12i)$

$u \in \{\pm 1, \pm i\}$

Dakle $r(180) = 8$. Rešenja $a^2+b^2 = 180$ su $(\pm 6, \pm 12), (\pm 12, \pm 6)$ ◢

$r(n)$ – aritmetička fja, koja se dakle ponaše iregularno.
Npr. vrednosti $r(n)$ i $r(n+1)$ nisu ni u kakvoj vezi

(D) Kažemo da aritmetička f-ja $f : \mathbb{N} \to \mathbb{C}$ ima <u>srednju vrednost</u> $c \in \mathbb{C}$ ako limes

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(n)$$

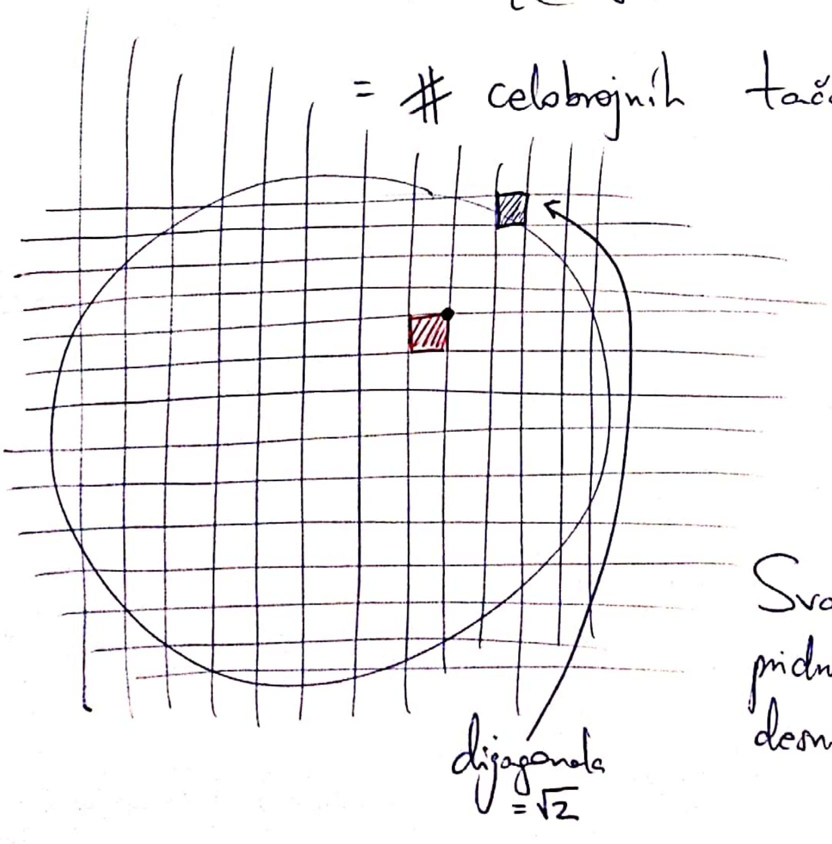
postoji i $= c$.

• Srednja vrednost f-je $r(n)$:

$$\sum_{n=0}^{N} r(n) = \sum_{n=0}^{N} \#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2=n\}$$

$$= \#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2 \leq N\}$$

$= \#$ celobrojnih tačaka u krugu poluprečnika $\sqrt{N}$



Intuitivno ovo treba da bude $\sim$ (površina kruga) $= \pi N$

Svakoj integralnoj tački iz $\mathbb{Z}^2$ pridružimo kvadratić rešetke čije desno gornje teme je ta tačka.

"Popločajmo" naš krug ovakvim kvadratićima. Neki od njih leže celi unutar kruga, ali svi imaju bar neprazan presek i svi leže unutar kruga poluprečnika $\sqrt{N}+\sqrt{2}$.

\# celobrojnih tačaka unutar kruga poluprečnika $\sqrt{N}$ je svakako $\leq$ ~~broj~~ \# kvadratića u ovom popločavanju

pa sledi

$$\sum_{n=0}^{N} r(n) \leq \pi\left(\sqrt{N}+\sqrt{2}\right)^2 = \pi N + 2\pi\sqrt{2}\sqrt{N} + 2\pi$$

Slično, ceo krug poluprečnika $\sqrt{N}-\sqrt{2}$ je popločan kvadratićima čije gornje desno teme pripada originalnom krugu tj. i

$$\sum_{n=0}^{N} r(n) \geq \pi\left(\sqrt{N}-\sqrt{2}\right)^2 = \pi N - 2\pi\sqrt{2}\sqrt{N} + 2\pi$$

T.9 [Gaus] Kad $N \to \infty$

$$\sum_{n=0}^{N} r(n) = \pi N + \mathcal{O}\left(\sqrt{N}\right) \qquad (1)$$

tj. srednja vrednost f-je $r(n)$ je π.

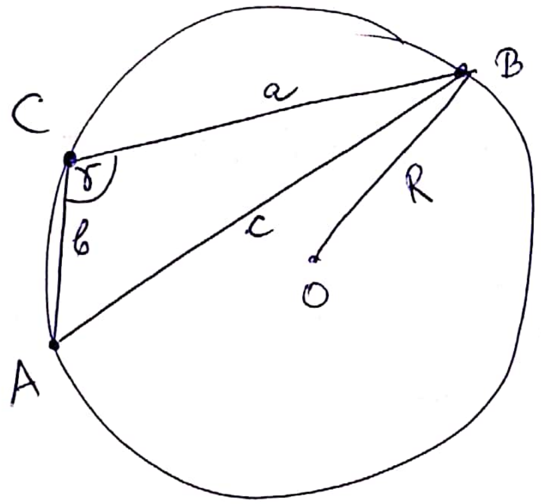
"Gausov problem kruga" – dobijanje što preciznije ocene za grešku ($\mathcal{O}$-član) u asimptotskoj f-li (1).

- Sierpinski (1906.) je dobio iznenađujuće poboljšanje: desna str. (1) $= \pi N + \mathcal{O}\left(N^{1/3}\right)$. | M. Huxley (2000.) $+\mathcal{O}\left(N^{0.3149\ldots}\right)$

Distribucija celobrojnih tačaka na krugovima i lukovima

$r(n)$ - ukupan broj celobrojnih tačaka na krugu $\{|z|^2=n\}$

Još delikatnija/dublja pitanja: kakva je njihova distribucija?



$A, B, C \in \mathbb{Z}^2$ tri celobrojne tačke na krugu poluprečnika R

L = dužina luka koji sadrži sve tri tačke ($\widehat{ACB}$ na slici)

P = površina ΔABC

a, b, c dužine stranica trougla

$$P = \frac{1}{2} ab \sin\gamma = \frac{1}{2} ab \frac{c/2}{R} \quad \longrightarrow \quad abc = 4P\cdot R$$

Ali površina trougla sa celobrojnim temenima je bar $\frac{1}{2}$ pa je

$$2R \leq 4\cdot P\cdot R = abc \leq \max\{a,b,c\}^3 \leq L^3$$

Sledi:

T.10 [Jarnik] Luk na krugu poluprečnika R čija dužina je $< (2R)^{\frac{1}{3}}$ može sadržati najviše 2 celobrojne tačke.

• $\boxed{?}$ Međutim, šta je sa lukovima koji sadrže veći broj celobrojnih tačaka?

Stvari postaju mnogo komplikovanije.
Naredna teorema je dokazana skoro i ocena u njoj je oštra za $m=3$ tačke, ali je otvoreno pitanje da li je se može popraviti za $m \geq 4$ tačke!

T.11 [Cilleruelo, Córdoba, 1992.]
Na krugu poluprečnika R sa centrom u $(0,0)$, svaki luk dužine

$$\sqrt{2}\, R^{\frac{1}{2} - \frac{1}{4[m/2]+2}}$$

sadrži najviše m celobrojnih tačaka.

Možemo pretpostaviti da je $R = \sqrt{n}$ i da je

$$n = k^2 \cdot 2^\alpha \cdot \prod_{p \equiv 1 (4)} p^{\beta_p}$$

tj. $m = k^2$ (iz T.8)
– inače je $r(n) = 0$ tj. na celom krugu $\{|z|^2 = n\}$ nema nijedna celobrojna tačka.

k = proizvod prostih oblika $4k+3$
Ukupan broj celobrojnih tačaka na tom krugu je
$r(n) = 4 \prod_p (1+\beta_p)$, i svaka od njih $(a,b) \in \mathbb{Z}^2$ zadovoljava

$$\mathcal{N}(a+bi) = n, \qquad a+bi = \underset{\{\pm 1, \pm i\}}{\underset{\Uparrow}{u}} \cdot k \cdot (1+i)^\alpha \prod_{p \equiv 1(4)} \omega_p^{e_p} \bar{\omega}_p^{f_p}$$

$$e_p + f_p = \beta_p$$

• Za svaki $p \equiv 1\ (4)$ ćemo uvesti oznaku

$$\boxed{\omega_p = \sqrt{p} \cdot e^{2\pi i \phi_p}}$$

$$N(\omega_p) = \omega_p \cdot \overline{\omega_p} = p$$

Onda je $\overline{\omega_p} = \sqrt{p} \cdot e^{-2\pi i \phi_p}$ i

$$\omega_p^{e_p}\, \overline{\omega_p}^{f_p} = p^{\frac{\beta_p}{2}}\, e^{2\pi i (e_p - f_p)\phi_p} = p^{\frac{\beta_p}{2}}\, e^{2\pi i (\beta_p - 2f_p)\phi_p}$$

• Svaka jedinica je oblika

$$e^{2\pi i \frac{t}{4}}, \qquad t \in \{0, 1, 2, 3\}$$

• Dakle, sve zajedno, svaki el. $a+bi$ norme n se može napisati u obliku

$$\boxed{\sqrt{n} \cdot e^{2\pi i \left(\phi_2 + \sum_p \gamma_p \phi_p + \frac{t}{4}\right)}}$$

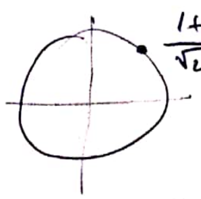
gde

• $t \in \{0, 1, 2, 3\}$

• $\gamma_p = e_p - f_p$, $|\gamma_p| \le \beta_p$, $\gamma_p \equiv \beta_p \pmod 2$

$\sum_p$ je suma po prostim $p \equiv 1 \pmod 4$

• $2^{\frac{\alpha}{2}} \cdot \frac{(1+i)^\alpha}{2^{\alpha/2}} = 2^{\frac{\alpha}{2}} \left(\frac{1+i}{\sqrt{2}}\right)^\alpha = 2^{\frac{\alpha}{2}}\, e^{2\pi i \phi_2}$



$\frac{1+i}{\sqrt{2}} = e^{2\pi i \cdot \frac{1}{8}}$

Ali parno α, $\alpha = 2\alpha_1$, $\alpha_1 \in \mathbb{Z}$, $e^{2\pi i \frac{2\alpha_1}{8}} = e^{i\frac{\pi}{2}\alpha_1} \in \{\pm 1, \pm i\}$ pa ovu fazu možemo da "ubacimo" u t.

Za neparno α, $\alpha = 2\alpha_1 + 1$ imamo fazu $e^{2\pi i \cdot \frac{1}{8}}$. Dakle, možemo uzeti

$$\phi_2 := \begin{cases} 0, & \text{ako je } \alpha \in 2\mathbb{Z} \\ \frac{1}{8}, & \text{ako je } \alpha \in 2\mathbb{Z}+1 \end{cases}$$

1. nejednakost:

Pretpostavimo da imamo $\underline{m+1}$ celobrojnih tačaka

$$a_s + i b_s = \sqrt{n}\cdot e^{2\pi i\left(\frac{\phi_2^{\circ}}{2} + \sum_p \gamma_p^s \phi_p + \frac{t^s}{4}\right)}, \qquad s\in\{1,2,\dots,m+1\}$$

$\frac{\phi_2^{\circ}}{2}$ → zavisi samo od α tj. od n
(i dakle isto je za sve tačke na krugu)

$\gamma_p^s,\ t^s \leftarrow$ gornji indeksi (nisu stepeni)

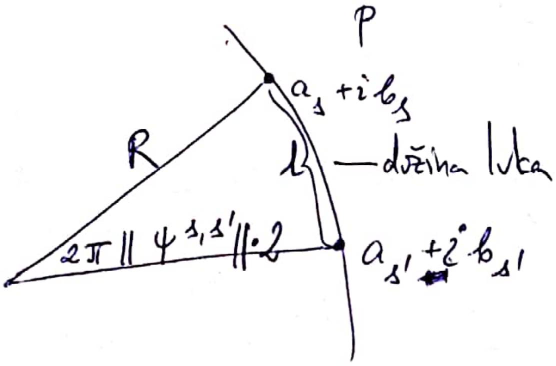
koje sve leže na luku dužine $\sqrt{2}\cdot R^{\theta}$.

- Za svaka dva $s, s' \in \{1,2,\dots,m+1\}$ imamo

$$\gamma_p^s \equiv \beta_p \equiv \gamma_p^{s'} \pmod 2$$

- Definišemo ugao

$$\psi^{s,s'} := \sum_p \frac{\gamma_p^s-\gamma_p^{s'}}{2}\phi_p + \frac{t^s-t^{s'}}{8}$$



$\|\psi^{s,s'}\|$ – rastojanje do najbližeg celog broja

$$2\|\psi^{s,s'}\| = \frac{l}{2\pi R} \le \frac{\sqrt{2}\,R^{\theta}}{2\pi R}$$ tj.

$$\boxed{\|\psi^{s,s'}\| \le \frac{1}{2\pi\sqrt{2}}R^{\theta-1}} \qquad (2)$$

2. nejednakost (donja ocena):

- Ako je $t^s \equiv t^{s'} \pmod 2$ onda je

$$\frac{t^s - t^{s'}}{8} =: \frac{t^{s,s'}}{4} \quad \text{za neko} \quad t^{s,s'} \in \mathbb{Z}$$

U ovom slučaju ugao $2\pi \| \varphi^{s,s'} \|$ korespondira reprezentaciji broja

$$\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{2}} = \square + \square \qquad (3)$$

- Ako je $t^s \not\equiv t^{s'} \pmod 2$, onda je

$$\frac{t^s - t^{s'}}{8} = \frac{1}{8} + \frac{t^{s,s'}}{4} \quad \text{za neko} \quad t^{s,s'} \in \mathbb{Z}.$$

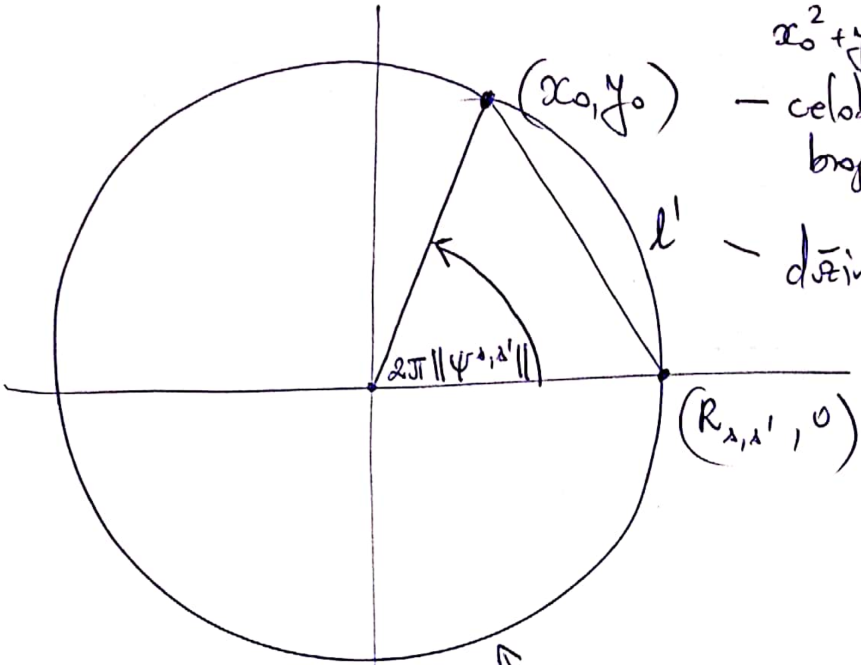
U ovom slučaju ugao $2\pi \| \varphi^{s,s'} \|$ korespondira reprezentaciji broja

$$2 \cdot \prod p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{2}} = \square + \square \qquad (4)$$

- Lako se proverava da ako je $\varphi^{s,s'} \in \mathbb{Z}$ tj. $\| \varphi^{s,s'} \| = 0$, da je onda $t^s = t^{s'}$ i $\gamma_p^s = \gamma_p^{s'}$, za sve p tj. da su $a_s + ib_s = a_{s'} + ib_{s'}$.

Dakle, ako je $s \neq s'$, onda je $\| \varphi^{s,s'} \| > 0$, i imamo sledeću sliku:

$$x_0^2+y_0^2=R_{s,s'}^2$$



(x_0,y_0) — celobrojna tačka koja odgovara broju iz (3) ili (4)

l' — dužina luka između ove dve tačke

krug poluprečnika

$$R_{s,s'} := 2^{\frac{\nu}{2}}\prod_p p^{\frac{|\gamma_p^s-\gamma_p^{s'}|}{4}}$$

gde je $\nu=\begin{cases}0, & \text{ako } t_s\equiv t_{s'} \pmod 2\\ 1, & \text{ako } t_s\not\equiv t_{s'} \pmod 2\end{cases}$

Onda je

$$l' > \left(\text{rastojanje između } (R_{s,s'},0) \text{ i } (x_0,y_0)\right)$$
$$=\sqrt{(x_0-R_{s,s'})^2+y_0^2} \ge \sqrt{y_0^2} \ge 1$$

jer je $y_0\neq 0$, jer je $\|\psi^{s,s'}\|>0$

pa dobijamo

$$\boxed{\|\psi^{s,s'}\| = \frac{l'}{2\pi R_{s,s'}} > \frac{1}{2\pi R_{s,s'}} \ge \frac{1}{2\pi\cdot\sqrt{2}\prod_p p^{\frac{|\gamma_p^s-\gamma_p^{s'}|}{4}}}} \qquad (5)$$

za svaki par $s\neq s'$.

• Uparujući gornju ocenu (2) i donju ocenu (5) za sve $s \neq s'$ dobijamo

$$\boxed{R^{\theta-1} > \frac{1}{\prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}}}} \qquad (6)$$

• Imamo $\binom{m+1}{2} = \frac{(m+1)m}{2}$ parova različitih tačaka $\{s, s'\}$ na našem luku, i za svaki imamo odgovarajuću ocenu (6). Kad ih sve pomnožimo, dobijamo

$$\left(\prod_{\substack{s,s' \\ s \neq s'}} \prod_p p^{\frac{|\gamma_p^s - \gamma_p^{s'}|}{4}} \right)^{-1} < R^{(\theta-1)\frac{(m+1)m}{2}}$$

Ovde hoćemo da nađemo donju ocenu za l. s. Izraz u zagradi je

$$\left(\prod_p p^{\sum_{s,s'} |\gamma_p^s - \gamma_p^{s'}|} \right)^{\frac{1}{4}}$$

pa očigledno treba da maksimizujemo vrednosti

$$\sum_{s,s'} |\gamma_p^s - \gamma_p^{s'}|$$

uz uslove da je za svako s:

$$|\gamma_p^s| \leq \beta_p, \qquad \gamma_p^s \equiv \beta_p \pmod 2$$

(L.12) $\beta, k \in \mathbb{N}$. Za sve izbore

$r_1, \dots, r_k \in \mathbb{Z}$ takve da je $|r_i| \le \beta$ i $r_i \equiv \beta \pmod 2$, $\forall i$

važi

$$\sum_{1 \le i < j \le k} |r_i - r_j| \le \frac{k^2 - \delta(k)}{2} \beta$$

gde je $\delta(k) = \begin{cases} 0, & \text{za } k \text{ parno} \\ 1, & \text{za } k \text{ neparno} \end{cases}$.

Neka su tačke uređene po veličini:

$-\beta \le r_1 \le r_2 \le \dots \le r_{k-1} \le r_k \le \beta$. Onda je

$$\sum_{1 \le i < j \le k} |r_i - r_j| = \sum_{1 \le i < j \le k} (r_j - r_i) =$$

$$= (k+1) r_k + ((k-2)-1) r_{k-1} + \dots + ((k-j-1)-j) r_{k-j} + \dots - (k-1) r_1$$

$$= \sum_{j=0}^{k-1} (k-1-2j) r_{k-j}$$

Npr. za k parno, prvih $\frac{k}{2}$ koeficijenata je >0, a poslednjih $\frac{k}{2}$ koef. je <0, pa se max očigledno dostiže za

$$r_k = r_{k-1} = \dots = r_{\frac{k}{2}+1} = \beta \quad ; \quad r_{\frac{k}{2}} = r_{\frac{k}{2}-1} = \dots = r_2 = r_1 = -\beta \quad ;$$

$$\max = 2 \sum_{j=0}^{\frac{k}{2}-1} (k-1-2j) \beta = 2\beta \left(\frac{k}{2}(k-1) - 2 \cdot \frac{\left(\frac{k}{2}-1\right)\frac{k}{2}}{2} \right)$$

$$= \frac{k^2}{2} \beta .$$

Slično i za neparno k. ◢

Završetak dokaza: Na osnovu L.12 dobijamo

$$R^{(\theta-1)\frac{(m+1)m}{2}} > \left(\prod_p p^{\frac{(m+1)^2-\delta(m+1)}{2}\beta_p}\right)^{-\frac{1}{4}} \qquad (7)$$

Podsetimo se:

$$R=\sqrt{n}=\underbrace{\overset{\text{proizvod prostih oblika } 4k+3}{k}\cdot 2^{\frac{\alpha}{2}}}_{\geq 1}\prod_{p\equiv 1 \,(\mathrm{mod}\, 4)} p^{\frac{\beta_p}{2}} \geqslant \prod_{p\equiv 1(4)} p^{\frac{\beta_p}{2}} \longleftrightarrow$$

$$\left(\prod_p p^{\frac{\beta_p}{2}}\right)^{-1} \geqslant R^{-1},$$ pa iz (7) sledi

$$R^{(\theta-1)\frac{(m+1)m}{2}} > R^{-\frac{(m+1)^2-\delta(m+1)}{4}}$$

odakle je

$$\theta > 1 - \frac{(m+1)^2-\delta(m+1)}{2(m+1)m} = \frac{1}{2}-\frac{1}{4\left\lfloor\frac{m}{2}\right\rfloor+2}$$

pa luk dužine tačno $R^{\frac{1}{2}-\frac{1}{4\lfloor\frac{m}{2}\rfloor+2}}$ ne može sadržati $m+1$ tačaka. ◢

Dakle

- svaki luk dužine $\sqrt{2}\cdot R^{\frac{2}{5}}$ sadrži najviše 4 celobrojne tačke
- svaki luk dužine $\sqrt{2}\cdot R^{\frac{3}{7}}$ sadrži najviše 6 celobrojnih tačaka

itd.