KVADRATNA CELA ŠTEVILA

$D \in \mathbb{Z}$, $D \neq \alpha^2$ (v resnici se "dobro omejimo na primer, ko D ni deljiv z nobenim kvadratom")

$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D};\ a, b \in \mathbb{Z}\}$

Zgled:

1) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$.

2) $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1};\ a, b \in \mathbb{Z}\} = \{a + bi;\ a, b \in \mathbb{Z}\}$

Kolobar Gaussovih celih števil

Računanje: $(a + b\sqrt{D}) \pm (c + d\sqrt{D}) = (a \pm c) + (b \pm d)\sqrt{D}$

$(a + b\sqrt{D})(c + d\sqrt{D}) = ac + bdD + (ad + bc)\sqrt{D}$

Opomba: $(a + b\sqrt{D})(c + d\sqrt{D}) = 0 \iff$ eden od faktorjev je enak 0 $\left((a^2 - b^2D)(c + d\sqrt{D}) = 0 \Rightarrow a^2 = b^2D \Rightarrow D = \alpha^2\right)$

Opomba: Obrnjeno kvadratna cela števila definiramo malce drugače: vzamemo vsa tista števila iz $\mathbb{Q}[\sqrt{D}]$ (za D ki ni kvadrat), ki so ničla kakega polinoma oblike $x^2 + px + q$ za $p, q \in \mathbb{Z}$. (algebrsko cela števila)

$\alpha \in \mathbb{Q}[\sqrt{D}]$ ničla $x^2 + px + q = 0 \Rightarrow x^2 + px + q = (x - \alpha)(x - \bar{\alpha})$

BŠS: j, k, l imajo največjega skupnega faktorja

$\alpha = \frac{j + k\sqrt{D}}{l}$ $\quad \bar{\alpha} = \frac{j - k\sqrt{D}}{l}$

$p = -\frac{2j}{l}$, $q = \frac{j^2 - k^2D}{l^2} \in \mathbb{Z}$

Če $l = 1 \Rightarrow p, q \in \mathbb{Z}$ ✓

(privzamemo $l = 2$) $l > 1 \Rightarrow \gcd(j^2, l^2) \mid k^2D \Rightarrow \gcd(j, l)^2 \mid D$

ker D ni deljiv z nobenim kvadratom $\Rightarrow \gcd(j, l) = 1$

ker je $p \in \mathbb{Z} \Rightarrow k$ sodo

ker je $q \in \mathbb{Z} \Rightarrow 4 \mid j^2 - k^2 D$

j je liho (saj je tuje z k) $\Rightarrow k$ liho

$\Rightarrow j^2 \equiv k^2 \equiv 1 \pmod 4 \quad \Rightarrow \quad D \equiv 1 \,(4)$

zato: če $D \equiv 1 \,(4)$ $\quad \alpha = \frac{j + k\sqrt{D}}{2}$; j, k poj.

v tem primeru namesto $\mathbb{Z}[\sqrt{D}]$ raje opisano $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$

① Kako merimo „velikost" takih števil?

v $\mathbb{Z}$: $|a|$

v $\mathbb{Z}[x]$: stopnja polinoma

v $\mathbb{Z}[\sqrt{D}]$: norma

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Z}$$

Zgledi: $\mathbb{Z}[i]$: $N(a+bi) = a^2+b^2$

$\mathbb{Z}[\sqrt{2}]$: $N(a+b\sqrt{2}) = a^2-2b^2$

$\mathbb{Z}[\sqrt{-2}]$: $N(a+b\sqrt{-2}) = a^2+2b^2$

Zgled: $\mathbb{Z}[\sqrt{2}]$

$N(7+6\sqrt{2}) = -23$

$N(11+7\sqrt{2}) = 23$

} imenlo za „velikost" števila je absolutna vrednost norme

Izrek: $\alpha, \beta \in \mathbb{Z}[\sqrt{D}] \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta)$

Dokaz: $\alpha = a + b\sqrt{D}$

$\beta = c + d\sqrt{D}$

$$\alpha\beta = ac + bdD + (ad + bc)\sqrt{D}$$

$$N(\alpha\beta) = (ac + bdD)^2 - D(ad + bc)^2 =$$

$$= a^2c^2 + b^2d^2D^2 + 2abcdD - a^2d^2D - b^2c^2D - 2abcdD$$

$$= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D$$

$$N(\alpha)N(\beta) = (a^2 - b^2D)(c^2 - d^2D)$$ ☐

Zgled: Lahko se zgodi, da bolo norma števila ni norma nobenega kvadratičnega celega št.:

$\mathbb{Z}[i]$: $N(a+bi) = a^2 + b^2$

$N(1) = 1$

$N(1+i) = 2$

$N(a+bi) \neq 3$

6, 7, 11

⊙ Kaj so obrnljivi elementi v $\mathbb{Z}[\sqrt{D}]$? α obrnljiv $\Leftrightarrow |N(\alpha)| = 1$

$\Rightarrow \alpha\beta = 1$

$N(\alpha)N(\beta) = N(1) = 1 \quad \Rightarrow \quad N(\alpha) = \pm 1$

$\Leftarrow N(\alpha) = \pm 1 \quad \Rightarrow \quad \alpha = a + b\sqrt{D}$

$(a+b\sqrt{D})(a-b\sqrt{D}) = \pm 1$

$\Rightarrow (a+b\sqrt{D})^{-1} = \pm(a-b\sqrt{D})$

Zgled: $\mathbb{Z}[\sqrt{3}]$

$N(2+\sqrt{3}) = 4-3 = 1 \quad \Rightarrow \quad 2+\sqrt{3}$ obrnljiv

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

Kdaj je $N(a+b\sqrt{D}) = a^2 - Db^2 = \pm 1$

· če je $D < 0$:

$D = -1$: $1, -1, i, -i$; $D \neq -1$: možno le za $a = \pm 1$ in $b = 0$

· če je $D > 0$: $a^2 - Db^2 = 1$ Pellova enačba

trivialna rešitev $a = \pm 1$, $b = 0$; ali obstajajo netrivialne rešitve?

za $D = 2$: $a^2 - 2b^2 = 1$: rešitve $a = 3, b = 2$

$a = 17, b = 12$

$a = 577, b = 408$

To enačbo so študirali že 400 BC v Indiji in Grčiji,

saj iz $a^2 - 2b^2 = 1$ sledi $\frac{a^2}{b^2} = 2 + \frac{1}{b^2} \Rightarrow \frac{a}{b} \doteq \sqrt{2}$

tj. $\frac{3}{2}$, $\frac{17}{12}$, $\frac{577}{408}$ so približki za $\sqrt{2}$

Arhimed je našel približek za $\sqrt{3}$: $\frac{1351}{780}$

Ni sicer razložil svojih metod, vendar se ta približek lahko dobi na enak način, torej kot rešitev Pellove enačbe

$$x^2 - 3y^2 = 1 .$$

Ker je $(a+b\sqrt{D})(c+d\sqrt{D}) = (ac+bdD) + (ad+bc)\sqrt{D}$ in smo pokazali, da je norma multiplikativna, velja

$$(a^2 - Db^2)(c^2 - Dd^2) = (ac + Dbd)^2 - D(ad+bc)^2$$

Brahmagupta-jeva identiteta

če obstaja ena netrivialna rešitev Pellove enačbe $\Rightarrow$ obstaja ∞ rešitev

izkaže se, da ima Pellova enačba vedno neskončno rešitev (Lagrange)
(če D ni kvadrat)

Iskalo so netrivialne rešitve zelo velike:

npr.: „najmanjša" rešitev pri $D = 313$ je
(|a| je minimalen)

$$a = 32\,188\,120\,829\,134\,849$$

$$b = 1\,819\,380\,158\,564\,160$$

Opomba: $a^2 - Db^2 = -1$ ni nujno rešljiva za D, ki ni kvadrat

Opomba: če namesto $\mathbb{Z}[\sqrt{D}]$ gledamo $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$,

ko je $D \equiv 1 \pmod 4$, se stvari malce spremenijo

v $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ (Eisensteinova cela števila)

so npr. obrnljivi elementi ± 1 in $\frac{\pm 1 \pm \sqrt{-3}}{2}$

⊙ Razcepi kvadratnih celih števil

Kaj bi pomenilo, da je element „nerazcepen"?

$$\alpha\beta = 1 \quad \Rightarrow \quad x = x(\alpha\beta) = (x\alpha)\cdot\beta$$

x je nerazcepen, če iz $x = \alpha\beta$ sledi, da je α ali β obrnljiv el.

x je razcepen, če ni nerazcepen

Trditev: x je razcepen $\Leftrightarrow$ $x = \alpha\beta$, kjer je $|N(\alpha)| < |N(x)|$ in $|N(\beta)| < |N(x)|$.

Zgled: $\mathbb{Z}[\sqrt{3}]$

$$11 = (1 + 2\sqrt{3})(-1 + 2\sqrt{3})$$

$$N(1+2\sqrt{3}) = 1 - 12 = -11$$

$$N(11) = 121$$

Torej je 11 razcepen element (čeprav je praštevilo!)

Kako prepoznati nerazcepne elemente?

Izrek: Če je $|N(x)|$ praštevilo, je x nerazcepen

Dokaz: $x = \alpha\beta \Rightarrow N(x) = N(\alpha)N(\beta) \Rightarrow |N(x)| \overset{\in \mathbb{P}}{=} |N(\alpha)|\,|N(\beta)|$

α, β nista enoti $\Rightarrow |N(\alpha)|, |N(\beta)| > 1$ ▯

Zgled: $\mathbb{Z}[\sqrt{2}]$

$N(1+3\sqrt{2}) = 1 - 18 = -17 \Rightarrow 1+3\sqrt{2}$ nerazc.

$N(1-2\sqrt{2}) = 1 - 8 = -7 \Rightarrow 1-2\sqrt{2}$ nerazc.

$N(3+\sqrt{2}) = 9 - 4 = 5 \Rightarrow 3+\sqrt{2}$ nerazc.

Pozor: Obrat izreka ne velja

- $\mathbb{Z}[i]$: $N(3) = 9 \notin \mathbb{P}$

  Toda 3 je nerazcepen

  $3 = \alpha\beta \Rightarrow N(\alpha) = \pm 3$, $N(\beta) = \pm 3$

  ne obstaja

- posebno $3 + \sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ je nerazcepen: $N(3+\sqrt{5}) = 4$

  Če je razcepen, mora obstajati el. z normo 2

  $a^2 - 5b^2 = 2$:

  - če je a sodo, je b sodo $\Rightarrow$ leva stran delj. s 4 $\times$
  - če je a liho, je b liho $\Rightarrow$

    $(2k+1)^2 - 5(2l+1)^2$ je spet delj. s 4 $\times$

Izrek: Vsak $x \in \mathbb{Z}[\sqrt{D}]$, za katerega je $|N(x)| > 1$, je produkt nerazcepnih elementov.

Dokaz: z indukcijo na $|N(x)|$

$|N(x)| = 2$: x nerazcepen po prejšnjem izreku

Predpostavimo, da za vsi x z $|N(x)| \in \{1, \dots, k\}$ produkti nerazcepnih elementov in izberimo x z $|N(x)| = k+1$

če x nerazcepen $\Rightarrow$ ✓

če x razcepen: $x = \alpha\beta$, $|N(\alpha)|, |N(\beta)| < |N(x)|$

$\Rightarrow \alpha$ in β sta produkta nerazcepnih elementov ☐

Kako najti faktorizacijo? „težko"

Zgled: $7+\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$

$N(7+\sqrt{5}) = 49-5 = 44 = 2^2 \cdot 11$

Vemo že, da element z normo 2 v $\mathbb{Z}[\sqrt{5}]$ ne obstaja,

zato je $7+\sqrt{5} = \alpha\beta$, $N(\alpha) = \pm 4$, $N(\beta) = \pm 11$

$11 = 16 - 5 \cdot 1 = 4^2 - 5 \cdot 1^2$

$\Rightarrow 11 = (4+\sqrt{5})(4-\sqrt{5})$

$\Rightarrow$ sumimo, da je $4+\sqrt{5}$ ali $4-\sqrt{5}$ je faktor v $7+\sqrt{5}$

(ali je to mujo res? DA, ič gre za „kolobar z enolično faktorizacijo")

Poskusimo

$$\frac{7+\sqrt{5}}{4-\sqrt{5}} = \frac{(7+\sqrt{5})(4+\sqrt{5})}{11} = \frac{33+11\sqrt{5}}{11} = 3+\sqrt{5}$$

$\Rightarrow 7+\sqrt{5} = (4-\sqrt{5})(3+\sqrt{5})$

↑ norma 11 ↖ norma 4

Zgled: $3+i \in \mathbb{Z}[i]$

$N(3+i) = 10 = 2 \cdot 5$

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

$$\frac{3+i}{1+i} = \frac{(3+i)(1-i)}{2} = 2-i$$

$$\Rightarrow 3+i = (1+i)(2-i).$$

Ali je taka faktorizacija enolična?

Kaj sploh pomeni „enolična"?

Ignoriramo vrstni red

Če je $\alpha\beta = 1$ potem:

$$x = x_1 x_2$$

$$x = x_1 \alpha x_2 \beta$$

Zgled:

$\mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$N(2) = 4 \qquad N(3) = 9$

$N(1+\sqrt{-5}) = 6 = N(1-\sqrt{-5})$

$N(a+b\sqrt{-5}) = a^2 + 5b^2 \neq 2, 3$

$\Rightarrow 2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ nerazcepni elementi

Toda $2 \cdot$ enota $\neq 1 \pm \sqrt{-5}$

↑ norma 1

$\mathbb{Z}[\sqrt{D}]$ ima enolično faktorizacijo, če je

$\alpha_1 \alpha_2 \cdots \alpha_r = \beta_1 \beta_2 \cdots \beta_s$, kjer so α_i, β_j nerazcepni elementi

sledi $r = s$ in obstoji taki obrnljivi elementi $u_1, \ldots, u_r$, da z primerni preureditvi velja

$\alpha_i = \beta_i u_i$ za vse i.

Ali je za kakšen D faktorizacija enolična?

Kako se dokaže, da je faktorizacija enolična v naravnih številih?

$\cdot$ $p_1 p_2 = q_1 q_2$

$p_1 \mid q_1 q_2 \Rightarrow p_1 \mid q_1$ ali $p_1 \mid q_2$

$\Rightarrow p_1 = q_1$ ali $p_1 = q_2$

Ali za nerazcepne elemente velja ta lastnost?

Zgled: $\mathbb{Z}[\sqrt{-5}]$

2 je nerazcepen (kot vemo), ni praelement:

$2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6$

$N(2) = 4, \quad N(1 \pm \sqrt{-5}) = 6$

$\Rightarrow 2 \nmid 1 \pm \sqrt{-5}$

Zgled: $\mathbb{Z}[\sqrt{-3}]$

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$

Ali $2 \mid 1 \pm \sqrt{-3}$?

$1 \pm \sqrt{-3} = (a + b\sqrt{-3}) \cdot 2 \Rightarrow 2a = 1$ $\lightning$

Opomba: Podobno se da videti za vsak $\mathbb{Z}[\sqrt{-D}]$, kjer je $D \geq 3$ in ni kvadrat.

Definirano: $\alpha \in \mathbb{Z}[\sqrt{D}]$ je praelement če iz dobimo iz iz

$\alpha \mid \beta\gamma$ sledi $\alpha \mid \beta$ ali $\alpha \mid \gamma$

Izrek: Vsak praelement je nerazcepen.

Dokaz: α praelement

naj bo $\alpha = xy$ razcep

Potem $\alpha \mid x$ ali $\alpha \mid y$

BŠS: $\alpha \mid x \Rightarrow x = \alpha\beta$

$\Rightarrow \alpha = \alpha\beta y \Rightarrow \alpha(1 - \beta y) = 0 \Rightarrow \beta y = 1$

↯ ničelni-mi ☺

Izrek: Vsak nerazcepen element je praelement $\Leftrightarrow$

faktorizacija je enolična.

Dokaz: ($\Rightarrow$): enako kot v $\mathbb{Z}$

($\Leftarrow$): Naj bo α nerazcepen in α je praelement

$\alpha \mid xy \Rightarrow xy = \alpha \cdot r$

razcepimo na nerazc. (endimo)

$\Rightarrow$ α nastopa v razcepu za x ali v razcepu za y

$\Rightarrow \alpha$ deli x ali α deli y □

Velja: Če v kolobarju lahko vsaki skupni delitelj dveh elementov zapišemo kot njuno linearno kombinacijo (ekvival.: kolobar je Evklidski), potem je vsak nerazcepen element tudi praelement.

Dokaz: α nerazc.

naj bo $\alpha \mid \beta\gamma$

označimo $\delta = \gcd(\alpha, \beta) = x\alpha + y\beta$

ker je α nerazc., je δ enota ali $\delta = \alpha$ do enote natančno

v drugem primeru $\alpha \mid \beta$

v prvem: $1 = x\alpha + y\beta$

$\gamma = \underbrace{x\alpha\gamma + y\beta\gamma}_{\text{deli. z } \alpha} \Rightarrow \alpha \mid \gamma$ □

Zgled: $\mathbb{Z}[i]$ je Evklidski kolobar

(razlog je po prejšnjem $\mathbb{Z}[i]$ kolobar z enolično faktorizacijo)

Vse kar potrebujemo, da kolobar izpolnjuje Evklidov algoritem je

$$\pi, \omega \in \mathbb{Z}[i], \quad N(\pi) > N(\omega) \Rightarrow$$

$\pi = q\omega + r$ za neka $q, r \in \mathbb{Z}[i]$ in $N(r) < N(\omega)$

$$\frac{\pi}{\omega} = \frac{\pi\bar{\omega}}{|\omega|^2} \in \mathbb{C}$$

$$x + iy = \underbrace{\alpha + i\beta}_{q \in \mathbb{Z}[i]} + x' + iy' \quad ; |x'|, |y'| \leq \frac{1}{2}$$

$$\pi = \omega q + \underbrace{(x' + iy')\omega}_{r} \Rightarrow r \in \mathbb{Z}[i]$$

$$N(r) = N(\omega) N(x' + iy') \leq N(\omega)\left(\frac{1}{4} + \frac{1}{4}\right) \leq N(\omega) \cdot \frac{1}{2} < N(\omega)$$

□

Zgled: Lezhože rešitve $\mathbb{Z}[\sqrt{-3}]$ nima enoličnega razcepa,

$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ pa ga ima.

$$2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

$$N(a + b\omega) = a^2 - ab + b^2$$

$$\omega = \frac{1 + \sqrt{-3}}{2}$$

Če definiramo $\omega = \begin{cases} \frac{1+\sqrt{D}}{2}; & \text{za } D \equiv 1 \pmod 4 \\ \sqrt{D}; & \text{sicer} \end{cases}$, D brez kvadratov

potem vsaja za $D<0$ evklidsk razcep $\mathbb{Z}[\omega]$ natanko naslednji „kobaji"

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

za $D>0$:

$D = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31,$
$33, 37, 38, 41, 43, 46, 47$

vsi do $D=50$

ni znan kriterij za sploščen D

ni znano niti ali jih je neskončno

Dodatek: Kaj so nerazc. el. v $\mathbb{Z}[i]$?

(1) $p \equiv 3 \ (4)$: če $p = \alpha\beta$

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

$\alpha = a + bi \Rightarrow a^2 + b^2 \equiv 3 \ (4)$ $\Rightarrow p$ nerazc.
$\in \{0,1\}$ $\in \{0,1\}$

(2) $p = 2$: $2 = (1+i)(1-i)$

- $\alpha + \beta i$: $\alpha^2 + \beta^2$ je prost. $(\Rightarrow \equiv 1 \ (4))$

$1+i$, $1-i$ nerazc.

(3) $p \equiv 1 \ (4)$

Wilsonov izrek : p prost. $\Rightarrow (p-1)! \equiv -1 \ (p)$

(Dokaz: $\exists p$ je polje $\Rightarrow$ vsak el. ima inverz, ne kateremu se pokrajo, razen tistih, ki so sami sebi inverzni : $a \cdot a = 1 \Rightarrow a^2 - 1 = 0 \Rightarrow (a-1)(a+1) = 0$
$\Rightarrow a = \pm 1 \Rightarrow$ produkt je -1)

$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{p+3}{2} \cdot \ldots \cdot p-1 =$

$= 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \left(p - \frac{p-1}{2}\right)\left(p - \frac{p-3}{2}\right) \ldots (p-1) =$

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

$\frac{p-1}{2}$ je sodo, zato je $a := \left(\frac{p-1}{2}\right)! : a^2 \equiv -1 \ (p)$

$\Rightarrow p \mid a^2 + 1 = (a+i)(a-i)$

Če je p nerazc. ($\Rightarrow$ praelement) $\Rightarrow p \mid a+i$ ali $p \mid a-i$
BSS: $(a+i) = p(c+di) \Rightarrow pd = 1$ ↯
$\Rightarrow p$ razc.

$\Rightarrow a+bi$; $N(a+bi) = a^2+b^2 = p \equiv 1 \ (4)$
je nerazcepen

Zgled: Zapiši 2025 kot vsoto dveh kvadratov

$2025 = x^2+y^2 = (x+yi)(x-yi)$

$2025 = 45^2 = 3^4 \cdot 5^2 = 9^2(1+2i)^2(1-2i)^2 = 9^2(-3+4i)(-3-4i)$

$= (-27+36i)(-27-36i) = 27^2+36^2$ eden način

(ni je razcep enolicen do množenja z $\pm 1, \pm i$
$\Leftarrow$ nepremeni rezultat)

(Število je vsota 2 kvadratov $\Leftrightarrow$ vsi prost. delitelji $\equiv 3(4)$ in 2 nastopajo v sodi potenci in obstaja vsaj 1 prost. delitelj $\equiv 1 \ (4)$ v razcepu)

naslednje leto, ki bo vsota 2 kvadratov bo 2036

$2036 = 4 \cdot 509 = 4(5+22i)(5-22i) = (10+44i)(10-44i)$

$= 10^2+44^2$

$2041 = 13 \cdot 157 = (2+3i)(2-3i)(11+6i)(11-6i) =$

$= (4+45i)(4-45i) = 4^2+45^2$

$= (40+21i)(40-21i) = 40^2+21^2$

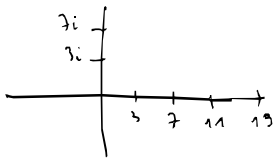
$2005 = 5 \cdot 401 = (1+2i)(1-2i)(20+i)(20-i) =$

$= 18+41i = 22+39i$

Dobath: neresični problemi v $\mathbb{Z}[i]$

① Kdaj je $\mathbb{Z}[i]$ Gaussovih celih števil a norma manjša od danega števila? ≈ ploščina πr^2

②



← ∞ Gaussovih praštevil

Ali ∃ še kaka praštevila v ravnini, ki ležijo ∞ Gaussovih praštevil?

③ Ali lahko pridemo do neskončno, če se sprehajamo po kompl. ravnini in se ponikamo le po Gaussovih praštevilih? (in so razdalje omejene z nekim fiksnim številom)

za praštevila to ni res: ∃ pf velike sestavljene zaporedne praštevilske: $n!+2, n!+3, \dots, n!+n$ so vsa sestavljena ($k|k$, $k|2$, $k|3$, …, $k|n$), torej je razlika vsaj n

·) trdimo je, da $\forall k>0$ ∃ Gaussovo celo število, ki ima najbližjega soseda na razdalji $>k$ (vendar tako se nastopa mnogo na poti od 0 do ∞)
npr.: 20 785 207 je GP, ki ima sosedo 17 do najbl. GP

·) z računalnikom: ne da se priti do sos. z razd. ≤ 6