Talteori, Föreläsning 11

Gaussiska heltal

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet
Föreläsningsanteckningar på kurshemsidan `http://courses.mai.liu.se/GU/TATA54/`

Sammanfattning

Definition
- Norm
- Delbarhet, enheter, irreducible element, primtal

Divisionsalgoritmen
- Divisionsalgoritmen i $\mathbb{Z}$
- Rationalisering av nämnare
- Största gemensamma delare
- Euklides algoritm

Unik faktorisering
- Irreducibla är Gaussiska primtal
- Alla GH är ändlig produkt GP

Gaussiska primtal

Summa av två kvadrater

Pytagoriska tripplar

Congruences
- Representatives, transversals
- Fermat and euler

Definition

- $z = a + ib \in \mathbb{C}$
- konjugat $\overline{z} = a - ib$
- norm $N(z) = z\overline{z} = a^2 + b^2$

Lemma

$N(zw) = N(z)N(w)$

Bevis.

$\overline{zw} = \overline{z}\,\overline{w}$ □

Definition

$\mathbb{Z}[i] = \{ a + ib | a, b \in \mathbb{Z} \}$

Lemma

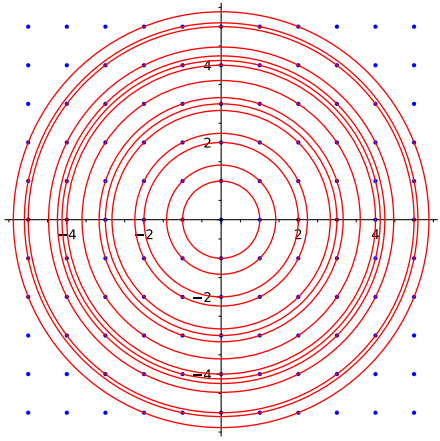
- $\mathbb{Z}[i]$ *delring till* $\mathbb{C}$
- *Ej delkroppp* ($1/2 \notin \mathbb{Z}[i]$)
- *Integritetsområde (inga nolldelare)*
- *Huvudidealområde*
- *Euklidisk*

Lemma

Om $N(\alpha) = n$ så $v_p(n)$ jämn för alla $p \equiv 3 \mod 4$. Om $n \in \mathbb{N}_+$ uppfyller att $v_p(n)$ jämn för alla $p \equiv 3 \mod 4$, så är n normen av något $\alpha \in \mathbb{Z}[i]$.

Bevis.

Om $\alpha = a + ib$ så $n = N(\alpha) = a^2 + b^2$ summa två kvadrater. Alltså förekommer varje $p \equiv 3 mod 4$ med jämn multiplicitet, och omvänt. $\square$


4
2
−4
−2
2
4
−2
−4

Definition

$\alpha, \beta \in \mathbb{Z}[i]$

- $\alpha|\beta$ omm finns $\gamma \in \mathbb{Z}[i]$ s.a. $\beta = \gamma\alpha$
- α är inverterbar (är en *enhet*) om $\alpha|1$
- α, β är *associerade* om $\alpha|\beta$ och $\beta|\alpha$
- α är *irreducibel* om varje delare antingen en enhet eller associerad till α
- α är ett (Gaussiskt) primtal om $\alpha|\beta_1\beta_2$ medför att $\alpha|\beta_1$ eller $\alpha|\beta_2$ (eller för all del båda)

Definition

$\mathbb{Q}[i] = \{ a + bi \,|\, a, b \in \mathbb{Q} \}$

Lemma

- $\mathbb{Z}[i]$ *delring till* $\mathbb{Q}[i]$*, som är delkropp till* $\mathbb{C}$*, och som är en kvadratisk kroppsutvidgning av* $\mathbb{Q}$
- $\mathbb{Q}[i]$ *är fraktionskroppen till* $\mathbb{Z}[i$ *precis som* $\mathbb{Q}$ *är det för* $\mathbb{Z}$*, dvs den är den minsta kropp som innehåller* $\mathbb{Z}[i]$
- *Så om* $\alpha, \beta \in \mathbb{Z}[i]$*, med* $\beta \neq 0$*, så gäller alltid att* $\frac{\alpha}{\beta} \in \mathbb{Q}[i]$*, med* $\frac{\alpha}{\beta} \in \mathbb{Z}[i]$ *endast om* $\beta | \alpha$

Exempel

$$\frac{2+3i}{1-i} = \frac{(2+3i)(1+i)}{(1+i)(1-i)} = \frac{-1+5i}{2} = \frac{-1}{2} + \frac{5}{2}i \in \mathbb{Q}[i] \setminus \mathbb{Z}[i],$$

så $1-i \not| 2+3i$.
Å andra sidan så

$$\frac{3-i}{1-i} = \frac{(3-i)(1+i)}{(1+i)(1-i)} = \frac{4+2i}{2} = 2+i \in \mathbb{Z}[i],$$

varför $1-i|3-i$.

Lemma

$\alpha|\beta$ *medför att* $N(\alpha)|N(\beta)$

Bevis.

Normen är multiplikativ. □

Korollarium

- $N(\alpha) = 1$ *omm* α *enhet omm* $\alpha \in \{\pm 1, \pm i\}$
- *Om* $N(\alpha)$ *ett (rationellt) primtal, så* α *irreducibelt.*

Bevis.

- $1 = N(1) = N(\alpha\frac{1}{\alpha}) = N(\alpha)N(\frac{1}{\alpha})$, så eftersom $N(\alpha)$ och $N(\frac{1}{\alpha})$ positiva heltal så är de båda 1.
- Om $\alpha = \beta\gamma$ med $N(\beta), N(\gamma) > 1$, så $N(\alpha) = N(\beta)N(\gamma)$, motsägelse.

□

Lemma

$u, v \in \mathbb{Z}[i]$ associerade omm $u = \alpha v$ för någon enhet $\alpha \in \mathbb{Z}[i]$, i.e. omm $u \in \{\pm v, \pm iv\}$

Lemma

Om $u, v \in \mathbb{Z}[i]$ associerade så $N(u) = N(v)$.

Exempel

Om $\alpha = 3 + 4i$ så $N(\alpha) = N(\overline{\alpha}) = 3^2 + 4^2 = 25$, met $\alpha \not| \overline{\alpha}$ eftersom

$$\frac{3-4i}{3+4i} = \frac{(3-4i)^2}{25} = \frac{9-16-24i}{25} = \frac{-7}{25} + \frac{-24}{25}i \notin \mathbb{Z}[i]$$

Också sant att $\overline{\alpha} \not| \alpha$.

Exempel

- $7/3 \in \mathbb{Q}$
- $7/3 = 2 + 1/3$
- $7 = 2 * 3 + 1$
- Kvot 2, rest 1
- $a = bq + r$, $0 \leq r < b$
- $q = \lfloor a/b \rfloor$, $r = a - bq$
- Kan även välja q till heltalen närmast a/b, och $|r| \leq b/2$
- $8/3 = 2 + 2/3 = 3 - 1/3$
- $8 = 2 * 3 + 2 = 3 * 3 - 1$

Teorem (Divisionsalgoritm)

Om $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, *så finns (ej nödv. unika)* $\gamma, \rho \in \mathbb{Z}[i]$ *s.a.*

1. $\alpha = \gamma\beta + \rho$,
2. $N(\rho) < N(\beta)$, *(kan få till* $N(\rho) \leq \frac{1}{2}N(\beta)$*)*

Bevis.

Beräkna

$$\frac{\alpha}{\beta} = \frac{r}{t} + \frac{s}{t}i \in \mathbb{Q}[i]$$

som tidigare. Låt u, v vara närmaste heltal till $\frac{r}{t}$ och $\frac{s}{t}$. Låt $\gamma = u + iv$, $\rho = \alpha - \gamma\beta$. □

Exempel

$$\frac{1+8i}{2-4i} = \frac{(1+8i)(2+4i)}{20} = \frac{-30+20i}{20} = \frac{-3}{2} + i$$

Tar vi $\gamma = -1 + i$ så $\rho = -1 + 2i$, med norm 5.

Tar vi $\gamma = -2 + i$ så $\rho = 1 - 2i$, också norm 5.

Teorem

Låt $\alpha, \beta \in \mathbb{Z}[i]$. För $\gamma \in \mathbb{Z}[i]$ så är följande påståenden likvärdiga:

1. $\gamma|\alpha$, $\gamma|\beta$ *och om* $\rho|\alpha$, $\rho|\beta$ *så* $\rho|\gamma$
2. $\gamma|\alpha$, $\gamma|\beta$ *om om* $\rho|\alpha$, $\rho|\beta$ *så* $N(\rho) \leq N(\gamma)$
3. $\gamma = u\alpha + v\beta$ *för några* $u, v \in \mathbb{Z}[i]$, *och om* $\rho = f\alpha + g\beta$ *för några* $f, g \in \mathbb{Z}[i]$ *så* $\gamma|\rho$
4. $\gamma = u\alpha + v\beta$ *för några* $u, v \in \mathbb{Z}[i]$, *och om* $\rho = f\alpha + g\beta$ *för några* $f, g \in \mathbb{Z}[i]$ *så* $N(\rho) \leq N(\gamma)$

Bevis.

Som för heltalen; byt $|\cdot|$ mot $N(\cdot)$. □

Definition

Vi säger att γ är en största gemensamm delare till α och β.

Lemma

Två olika sgd till α, β är alltid associerade.

Definition

$\alpha, \beta \in \mathbb{Z}[i]$ är relativt prima om $\gcd(\alpha, \beta) = 1$ (eller enhet); annorlunda uttryckt, om ekvationen

$$u\alpha + v\beta = 1$$

är lösbar $\mathbb{Z}[i]$.

Lemma

Om $\alpha = \gamma\beta + \rho$ *med* $N(\rho) < N(\beta)$, *så* $\gcd(\alpha, \beta) = \gcd(\beta, \rho)$

Teorem (Euklides algoritm)

Iterera ovanstående, får sgd. Samla ihop termer, får Bezout-uttryck.

Anmärkning

Kvoter och rester ej unika, ovanstående fungerar ändå!

Exempel

$$
\begin{aligned}
11+3i &= (1-i)(1+8i)+2-4i \\
1+8i &= (-1+i)(2-4i)+1-2i \\
2-4i &= 2(1-2i)+0
\end{aligned}
$$

så

$$
\begin{aligned}
\gcd(11+3i, 1+8i) = 1-2i &= (1)(1+8i)+(1-i)(2-4i) = \\
&= (1)(1+8i)+(1-i)((11+3i)+(-1+i)(1+8i)) = \\
&= (1-i)(11+3i)+(1+(1-i)(-1+i))(1+8i)
\end{aligned}
$$

Lemma

Om $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, $\alpha | \beta\gamma$, $\gcd(\alpha, \beta) = 1$, *så* $\alpha | \gamma$.

Bevis.

Eftersom $\alpha | \beta\gamma$ så kan vi skriva $\beta\gamma = \alpha w$ för något $w \in \mathbb{Z}[i]$. Eftersom $\gcd(\alpha, \beta) = 1$, så

$$1 = u\alpha + v\beta,$$

så

$$\gamma = \gamma u\alpha + \gamma v\beta = \alpha\gamma u + \alpha wv = \alpha(u\gamma + wv).$$

□

Lemma

Om $\alpha \in \mathbb{Z}[i]$ är irreducibel, så är det ett Gaussiskt primtal.

Bevis.

Antag att $\alpha | ab$. Eftersom α är irreducibel, så är $\gcd(\alpha, a) = 1$. Det tidigare lemmat ger nu att $\alpha | b$. □

Lemma

Om $\alpha \in \mathbb{Z}[i]$ är ett Gaussiskt primtal, så är det irreducibelt.

Bevis.

Antag, för att få en motsägelse, att α är reducibelt, dvs $\alpha = ab$ med $N(a), N(b) < N(\alpha)$. Då $\alpha | ab$ men $\alpha \nmid a$, $\alpha \nmid b$, vilket motsäger att α är ett Gaussiskt primtal. □

Teorem

Varje $\alpha \in \mathbb{Z}[i]$ kan skrivas som en ändlig produkt av Gaussiska primtal.

Bevis.

Om α är irreducibel, så är det ett GP, klart.
Om $\alpha = ab$ med $N(a), N(b) < N(\alpha)$, så kan vi mha induktion skriva a och b som ändliga produkter av GP. Kombinera. $\square$

Teorem (Unik faktorisering)

Om $0 \neq \alpha \in \mathbb{Z}[i]$, *så*

$$\alpha = \pi_1 \cdots \pi_s$$

där π_i *är GP. Om vidare*

$$\alpha = q_1 \cdots q_t$$

är en annan factorisering av α *som produkt av GP, så* $t = s$, *och det finns en pemutation* $\sigma \in S_s$ *så att* $q_j = \epsilon_j \pi_{\sigma(j)}$ *för* $1 \leq j \leq s$, *med* $N(\epsilon_j) = 1$.

Bevis.

Precis som för heltalen. □

Exempel

Märk att ett (rationellt) primtal p inte behöver vara ett Gaussiskt primtal. Till exempel så har vi att

$$5 = (1 + 2i)(1 - 2i) = (2 - i)(2 + i)$$

Här är $(1 + 2i)$ och $2 - i$ associerade, liksom $1 - 2i$ och $2 + i$, så de två faktoriseringarna är ekvivalenta.

Exempel

Låt $\alpha = 3 + 4i$. Då $N(\alpha) = 9 + 16 = 25 = 5^2$. Så antingen är α GP, eller så $\alpha = uv$ med $N(u) = N(v) = 5$.
Vilka Gaussiska heltal kan ha norm 5? Uttömmande prövning hittar

$$1 + 2i, 1 - 2i, -1 + 2i, -1 - 2i, 2 + i, 2 - i, -2 + i, -2 - i$$

och vi ser att

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

Teorem

- *Varje $\alpha \in \mathbb{Z}[i]$ med jämn norm är delbar med $1+i$*
- *2 är ej GP*

Bevis.

- Antag att $N(a+ib) = (a+ib)(a-ib) = a^2+b^2 = 2c$. Eftersom $(1+i)(1-i) = 2$, så har vi att

$$(a+ib)(a-ib) = (1+i)(1-i)c = (1+i)^2 ic$$

  Men $N(1+i) = 2$, och $1+i$ är alltså GP. Från unik faktorisering ser vi att $1+i$ delar $a+ib$ eller $a-ib$.
  Men om $1+i$ delar $a-ib$ så kommer $1-i$ att dela $a+ib$, och $1+i$ är associerad med $1-i$.
- $2 = (1+i)(1-i)$.

□

Lemma

Låt π vara ett GP. Då $\pi | p$ för ett unikt rationellt primtal p.

Bevis.

Sätt $N(\pi) = \pi\overline{\pi} = n$, och faktorisera i rationella primtal, $n = p_1 \cdots p_r$. Då

$$\pi | p_1 p_2 \cdots p_r \quad \Longrightarrow \quad \pi | p_j \text{ något } p_j$$

Men $\pi\alpha \in \mathbb{Z}$ omm $\alpha = \overline{\pi}c$, $c \in \mathbb{Z}$; om $\pi\overline{\pi}c = p$ är rationellt primtal, så $c = \pm 1$. $\square$

Teorem

Ett rationellt primtal p är reducibelt i $\mathbb{Z}[i]$ omm det är en summa av två kvadrater (på heltal).

Bevis.

- Antag $p = \alpha\beta \in \mathbb{Z}[i]$, α, β ej enheter. Då $N(p) = p^2 = N(\alpha\beta) = N(\alpha)N(\beta)$. Alltså $N(\alpha) = N(\beta) = p$. Skriv $\alpha = a + ib$, då $p = N(a + ib) = a^2 + b^2$, så p är en summa av två kvadrater.
- Antag att $p = a^2 + b^2$, $a, b \in \mathbb{Z}$. Sätt $\alpha = a + ib$. Då är

$$p = (a + ib)(a - ib) = \alpha\overline{\alpha}$$

en icke-trivial faktorisering av p.

□

Korollarium

Varje rationellt primtal $p \equiv 3 \mod 4$ *är ett GP.*

Bevis.

Sådana kan ej skrivas som en summa av två kvadrater. □

Korollarium

Ett rationellt primtal $p \equiv 1 \mod 4$ har precis två olika icke-associerade Gaussiska primfaktorer. in $\mathbb{Z}[i]$.

Bevis.

Vi vet att

$$p = a^2 + b^2 = (a + ib)(a - ib)$$

där $a + ib$ och $a - ib$ har primtalsnorm, och alltså är Gaussiska primtal. De är inte associerade, hävdar vi.

1. Om $a + ib = 1(a - ib)$ så $b = 0$, alltså $p = a^2$, vilket motsäger att p rationellt primtal.
2. Om $a + ib = -(a - ib)$ så $a = 0$.
3. Om $a + ib = i(a - ib) = b + ia$ så $a = b$, alltså $p = a^2 + b^2 = 2a^2$, en motsägelse.
4. Om $a + ib = -i(a - ib) = -b - ia$ så $a = -b$ så $p = a^2 + b^2 = 2b^2$, en motsägelse.

□

Korollarium

Låt p vara ett rationellt primtal.

- *Om $p = 2$ så $p = 2 = -(1+i)^2$*
- *Om $p \equiv 1 \mod 4$ så $p = \pi\overline{\pi}$, där π och $\overline{\pi}$ är icke-associerade GP*
- *Om $p \equiv 3 \mod 4$ så är p GP.*

Teorem

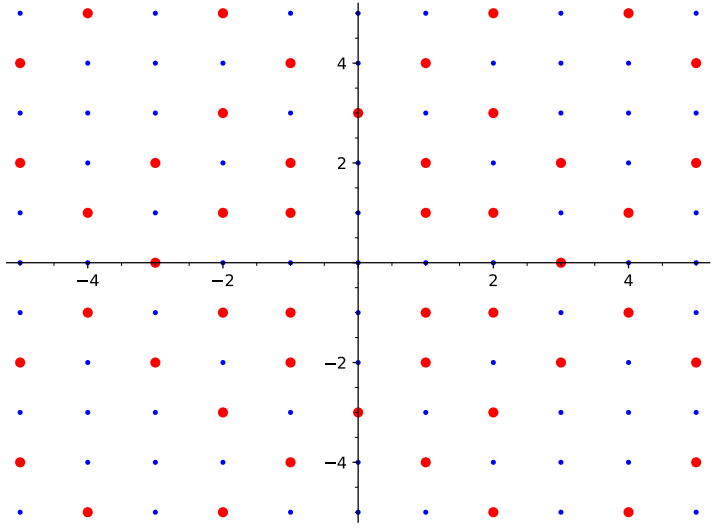
Varje GP α är associerad till antingen

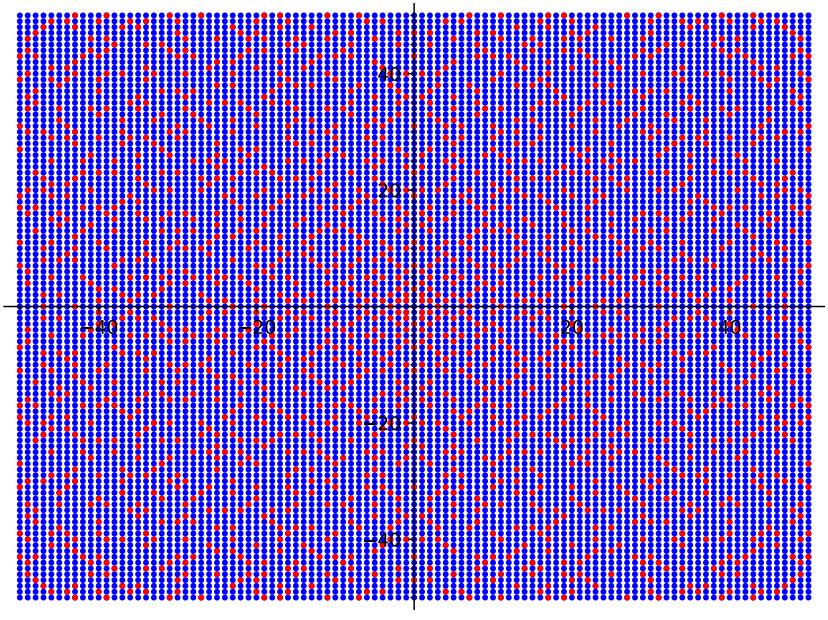
1. $1 + i$
2. π *eller* $\overline{\pi}$, *där* $N(\pi) = p$ *är rationellt primtal med* $p \equiv 1 \mod 4$,
3. p, *där* p *rationellt primtal,* $p \equiv 3 \mod 4$.

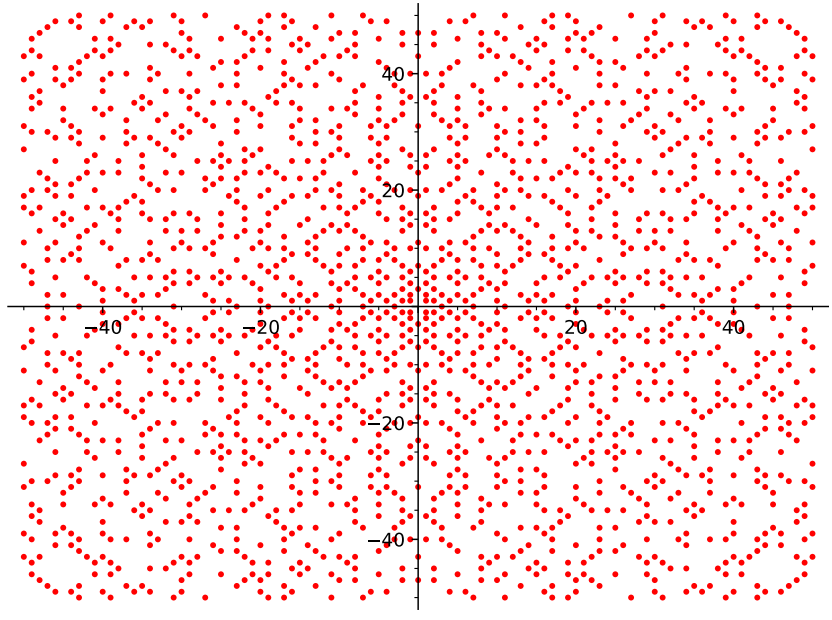
Bevis.

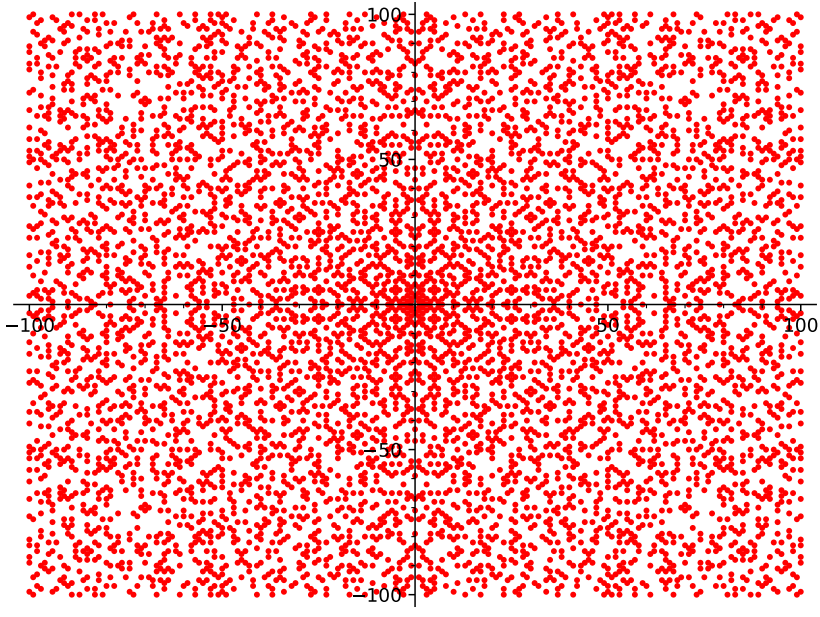
- Varje GP α delar något rationellt primtal p
- Antingen $p = 2$, $p \equiv 1 \mod 4$, eller $p \equiv 3 \mod 4$
- Vi vet hur dessa olika fall faktoriseras i $\mathbb{Z}[i]$

□


4
2
−4
−2
2
4
−2
−4


40
20
−40
−20
20
40
−20
−40


40
20
−40
−20
20
40
−20
−40


100
50
−100
−50
50
100
−50
−100

Teorem

Om ett rationellt primtal p är en summa av två kvadrater, säg $p = a^2 + b^2$, så är detta skrivsätt väsentligen unikt: a^2 och b^2 är unikt bestämda (upp till omkastning).

Bevis.

- $p = a^2 + b^2 = (a + ib)(a - ib)$
- $N(a + ib) = N(a - ib) = p$, så $a + ib$, $a - ib$ GP
- Antag att $p = c^2 + d^2 = (c + id)(c - id)$.
- Från unik faktorisering så $a + ib = u(c + id)$, u enhet, eller $a + ib = u(c - id)$.
- I det första fallet, om $u = 1$, så $c = -a$ och $d = -b$, så $c^2 = a^2$ och $d^2 = b^2$

□

Teorem

Låt det positiva heltalet n ha (rationell) primfaktorisering

$$n = 2^m \prod_{j=1}^{s} p_j^{e_j} \prod_{k=1}^{t} q_k^{f_k}$$

med p_j rationella primtal $\equiv 1 \mod 4$, och $q_k \equiv 3 \mod 4$; vidare är alla f_k jämna. Då ges antalet sätt att skriva n som en summa av två kvadrater, tagande i beaktning ordning och tecken,

$$4 \prod_{j} (e_j + 1)$$

Bevis.

- Räknar antalet sätt att factorisera $n = u^2 + v^2 = (u + iv)(u - iv)$ i $\mathbb{Z}[i]$
- $2^m = i^m(1 - i)^{2m}$
- $p_j = (a_j + ib_j)(a_j - ib_j)$, produkt icke-associerade GP
- Så $n = \epsilon(1 - i)^{2m} \prod_{j=1}^{s}(a_j + ib_j)(a_j - ib_j) \prod_{k=1}^{t} q_k^{f_k}$
- Faktorn $u + iv$ är, från unik faktorisering, på formen $\epsilon_0(1 - i)^w \prod_{j=1}^{s}(a_j + ib_j)^{g_j}(a_j - ib_j)^{h_j} \prod_{k=1}^{t} \ell_k$ med $0 \leq w \leq 2m$, $0 \leq g_j \leq e_j$, $0 \leq h_j \leq e_j$, $0 \leq \ell_k \leq f_k$
- $u - iv = \overline{u + iv} = \overline{\epsilon_0}(1 - i)^w \prod_{j=1}^{s}(a_j - ib_j)^{g_j}(a_j + ib_j)^{h_j} \prod_{k=1}^{t} \ell_k$
- $n = (u + iv)(u - iv) = 2^w \prod_{j=1}^{s} p_j^{g_j + h_j} \prod_{k=1}^{t} q_k^{2\ell_k}$
- Så $w = m$, $g_j + h_j = e_j$, $2\ell_k = f_k$, ϵ_0 enhet
- Så $e_j + 1$ val för g_j, 4 val för ϵ_0.

□

Exempel

$$n = 5^2 = (2+i)^2(2-i)^2$$

Möjliga faktorer $u + iv$ är

$$(2+i)^2 = 3+4i,\ i(2+i)^2 = -4+3i,\ i^2(2+i)^2 = -3-4i,\ i^3(2+i)^2 = 4-3i,$$
$$(2+i)(2-i) = 5$$
$$(2-i)^2 = 3-4i$$

samt 6 till, får $n = (\pm 5)^2 + 0^2 = (\pm 3)^2 + (\pm 4)^2 = (\pm 4)^2 + (\pm 3)^2$.

Exempel

$$13 = (2+3i)(2-3i),$$

med faktorer

$$2+3i, -3+2i, -2-3i, 3-2i, 2-3i, 3+2i, -2+3i, -3-2i$$

Alltså

$$5^2 * 13 = (2+i)^2(2-i)^2(2+3i)(2-3i),$$

en möjlig faktor är

$$(2+i)^2(2+3i) = (3+4i)(2+3i) = -6+17i$$

så

$$5^2 * 13 = (-6)^2 + 17^2.$$

Teorem

Låt $4F(n)$ beteckna antalet sätt att skriva n som summa av kvadrater. Då är F multiplikativ, med värden på primtalspotenser

- $F(2^m) = 1$,
- *om* $q \equiv 3 \mod 4$ *så* $F(q^{2f}) = 1$ *och* $F(q^{2f+1}) = 0$
- *om* $p \equiv 1 \mod 4$ *så* $F(p^e) = e + 1$

Kom ihåg

Definition

- Heltalslösningar till $a^2 + b^2 = c^2$ kallas Pytagoriska tripplar (PT)
- Om $\gcd(a, b, c) = 1$ så primitiv Pytagorisk trippel (PPT)

Lemma

- *Om* (a, b, c) *PPT, så* $\gcd(a, b) = 1$, $a \not\equiv b \mod 2$, *c udda*
- *Antag a udda, b jämn, då har vi parametrisering*

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2$$

med $u > v > 0$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

Låt oss visa detta mha Gaussiska heltal!

Bevisskiss

- $c^2 = a^2 + b^2 = (a + ib)(a - ib)$
- Visa först att $\gcd(a + ib, a - ib) = 1 \in \mathbb{Z}[i]$. Låt δ vara sgd.
- δ delar $a + ib, a - ib$, så delar $2a$ och $2ib$, så delar $2b$.
- δ relativt primt till $2 = -i(1 + i)^2$ eftersom
  1. $1 + i$ primt
  2. $1 + i$ delar δ omm $N(\delta)$ jämn
  3. $\delta^2 | c^2$ så $N(\delta)^2 | c^4$; emellertid så är c udda
  4. Så $\gcd(\delta, 1 + i) = 1$, alltså $\gcd(\delta, 2) = 1$
- Så $\delta | 2a \implies \delta | a$, och $\delta | 2b \implies \delta | b$.
- Eftersom $\gcd(a, b) = 1 \in \mathbb{Z}$ får vi från Bezout att $1 = ra + sb$, alltså ger Bezout i $\mathbb{Z}[i]$ att $\gcd(a, b) = 1 \in \mathbb{Z}[i]$.

Bevis (forts)

- Så $\delta = 1$, och $\gcd(a + ib, a - ib) = 1$.
- $c^2 = a^2 + b^2 = (a + ib)(a - ib)$, med $\gcd(a + ib, a - ib) = 1$. Från unik faktorisering så $a + ib = \varepsilon(u + iv)^2$, med ε enhet.
- På liknande sätt får vi att $a - ib$ associerad till kvadrat.
- $-1 = i^2$ kan absorberas, så kan anta $\varepsilon \in \{1, i\}$.
- $\varepsilon = 1$ ger $a + ib = u^2 - v^2 + 2uvi$, $\varepsilon = i$ ger $a + ib = i(u^2 - v^2) + 2uv$.
- Konvention: a udda, antag första fallet.
- Kontrollera: $u > v$, olika pariter, relativt prima.

Vi tittar på enn liknande Diofantisk ekvation:

Teorem

Heltalslösningarna till

$$a^2 + b^2 = c^3$$

med $\gcd(a, b) = 1$ *kan parametriseras av*

$$a = m^3 - 3mn^2, \qquad b = 3m^2n - n^3, \qquad c = m^2 + n^2$$

med $\gcd(m, n) = 1$, m, n *olika paritet.*

Bevis.

Beviskiss

- $c^3 = a^2 + b^2 = (a + ib)(a - ib)$
- $a + ib$ perfekt kub, så

$$a + ib = (m + in)^3 = m^3 + 3m^2ni - 3mn^2 - in^3 = m^3 - 3mn^2 + (3m^2n - n^3)i$$

□

Exempel

En annan Diofant (Rosen 14.3.8):

- $$y^3 = x^2 + 1 = (x + i)(x - i)$$
- $x + i, x - i$ relativt prima
- $$x + i = (r + si)^3 = r^3 - 3rs^2 + i(3r^2 s - s^3)$$
- $x = r(r^2 - 3s^2)$, $1 = s(3r^2 - s^2)$
- Så $s = 1$ eller $s = -1$
- Om $s = 1$ så $1 = 3r^2 - 1$, $3r^2 = 2$, omöjligt
- Om $s = -1$ så $1 = -3r^2 + 1$, $3r^2 = 0$, $r = 0$, $x = 0$, $y = 1$
- Unik lösning $(x, y) = (0, 1)$.