

Algebra och talteori

MMGL31

Föreläsning 13
VT 2010

Samuel Bengmark

Repetition

- Vilka m kan skrivas $m=a^2+b^2$

Idag

- Gaussiska heltal

Gausiska heltal

Definition

Mängden $\mathbb{Z}[i]=\{a+bi; a,b \in \mathbb{Z}\}$ kallas de Gaussiska heltalen.

De Gaussiska heltalen är en delmängd av de komplexa talen. Man kan alltså addera och multiplicera dem.

Addition: $(a+ib)+(c+id) = (a+c)+(b+d)i$

Multiplikation: $(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i$

$\mathbb{Z}[i]$ är en ring.

Addition

- Slutet: $(a+ib)+(c+id) = (a+c)+(b+d)i \in \mathbb{Z}[i]$
- Identitet: $0+0i=0$
- Invers: $(a+bi)+(-a+(-b)i)=0$
- Associativt: klart då delmängd av $\mathbb{C}$.

Multiplikation

- Slutet: $(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Z}[i]$
- Identitet: $1+0i=1$
- Associativt: klart då delmängd av $\mathbb{C}$.

Distributiva lagen: klart då delmängd av $\mathbb{C}$.

$\mathbb{Z}[i]^*$

Givet $(a+bi)$ hitta $(c+di)$ så att

$$1 = (a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i \\ \Leftrightarrow ac-bd=1 \text{ och } ad+bc=0.$$

Betrakt två fall:

1. $a \neq 0$: $d = -bc/a$. Får $1 = (ac-b(-bc/a)) = (a^2c+b^2c)/a = (a^2+b^2)c/a$. Enda möjligheten är $c/a=1$, $a=\pm 1$, $b=0$, dvs $a+bi=\pm 1$
2. $b \neq 0$: $c = -ad/b$. Får $1 = (a(-ad/b)-bd) = -d(b(a^2+b^2))$. Enda möjligheten är $-b/d=1$, $b=\pm 1$, $a=0$, dvs $a+bi=\pm i$.

Slutsats $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$

Definition Inverterbara element kallas enheter.

Delbarhet

Definition

Vi säger att $c+di$ delar $a+bi$ om det finns $e+fi \in \mathbb{Z}[i]$ så att $(a+bi) = (c+di)(e+fi)$. Vi skriver då att $c+di \mid a+bi$.

Exempel

- $1+i \mid 1+3i$ eftersom $1+3i = (1+i)(2+i)$
- $3+4i \mid 25$ eftersom $25 = (3+4i)(3-4i)$
- $1+i \mid 2$ eftersom $2 = (1+i)(1-i)$
- $w \in \mathbb{Z}[i]^*$ delar varje Gausiska heltal $a+bi$ eftersom $a+bi = w(a+bi)w^{-1}$,
 $\text{tex } i \mid 1+i$ eftersom $1+i = i(1+i)i^{-1} = i(1+i)(-i) = i(1-i)$.

Gäller unik faktorisering?

- Vi ser att $(3+0i)(3+0i) = 9 = (0+3i)(0-3i)!$
- Säger detta att vi inte har unik faktorisering?
- Nej, faktoriseringarna skiljer sig bara på inverterbara faktorer (enheter): $3 \cdot 3 = 3 \cdot 3 \cdot 1 = 3 \cdot 3 \cdot i \cdot (-i) = 3i(-3i)$.

Jämför med $3 \cdot 3 = (-3)(-3)$ i $\mathbb{Z}$, där -1 är inverterbar. ($\mathbb{Z}^* = \{\pm 1\}$.)

Slutsats: Vi kan bara förvänta oss unik faktorisering om vi inte bara bortser från ordningen på faktorerna utan också bortser från inverterbara faktorer, så kallade enheter.

Gäller unik faktorisering om vi bortser från inverterbara faktorer?

Vi såg att

$$(3+4i)(3-4i) = 25 = 5 \cdot 5.$$

Säger detta att vi inte har unik faktorisering?

Bara om alla faktorerna är irreducibla.

Är dom det?

Vilka är de irreducibla talen i $\mathbb{Z}[i]$?

Vi skall nu introducera begreppet norm som ger kommer att hjälpa oss svara på ovanstående fråga, men också mer allmänt hjälpa oss att se vilka tal som delar vilka.

Norm

Definition: $N(a+bi) = a^2 + b^2$. $N(z)$ kallas normen av z .

Obs:

1. $N(a+bi) = |a+bi|^2$, dvs avståndet till origo i kvadrat.
2. $N(a+bi)$ är alltid ett naturligtal, dvs ett tal i $\mathbb{N}$.

Två satser

Sats $N((a+bi)(c+di)) = N(a+bi)N(c+di)$

Bevis

$$\begin{aligned} N((a+bi)(c+di)) &= N(ac-bd + (ad+bc)i) = (ac-bd)^2 + (ad+bc)^2 = \\ &= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 = a^2(c^2+d^2) + b^2(d^2+c^2) = \\ &= (a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di) \end{aligned}$$

Sats $a+bi \in \mathbb{Z}[i]^* \Leftrightarrow N(a+bi)=1$.

Bevis

- $a+bi \in \mathbb{Z}[i]^* \Rightarrow (a+bi)(c+di)=1 \Rightarrow N(a+bi)N(c+di)=1 \Rightarrow 1=N(a+bi)$
- Omvänt om $1=N(a+bi)=a^2+b^2$ är $a+bi \in \{1, -1, i, -i\}$ dvs $a+bi \in \mathbb{Z}[i]^*$

Kan $1+2i$ faktoriseras?

Antag att $1+2i = (a+bi)(c+di)$. Då skulle
 $5 = N(1+2i) = N(a+bi)N(c+di)$, dvs en av normerna måste vara 1 därmed är denna faktor en enhet, dvs ett inverterbart tal.

Slutsats: $1+2i$ är irreducibelt.

När normen är ett primtal i $\mathbb{Z}$

Sats (extrasatsen :-)

Om $N(z)$ är ett primtal tal i $\mathbb{Z}$ så är z irreducibelt i $\mathbb{Z}[i]$.

Bevis

Antag $z=vw$ och att $N(z) = p$, ett primtal. Vi får då att
 $p = N(z) = N(v)N(w)$.

Alltså måste $N(v)$ eller $N(w)$ vara 1 eftersom p är irreducibelt i $\mathbb{Z}$. Alltså kommer en av faktorerna vara en inverterbart och därmed är z irreducibelt.

Kan 3 faktoriseras?

- Antag att $3=(a+bi)(c+di)$
- Då får vi att
 $9 = N(3) = N((a+bi)(c+di)) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2)$
- Ingen faktor skall ha norm 1 för då är det en enhet. Alltså måste $3 = a^2+b^2$.
- Är det möjligt?
- Nej ty $3 \not\equiv_4 1$. Därför vet vi att 3 inte kan skrivas som en summa av två kvadrater.

Slutsats: 3 är irreducibelt i $\mathbb{Z}[i]$.

De irreducibla talen i $\mathbb{Z}[i]$.

1. $1+i$ är irreducibelt
2. Om $p \in \mathbb{Z}$ är ett primtal och $p \equiv_4 3$ så är p det irreducibelt i $\mathbb{Z}[i]$.
3. Om $p \in \mathbb{Z}$ är ett primtal och $p \equiv_4 1$ och $p = u^2 + v^2$ så är $u+iv$ irreducibelt i $\mathbb{Z}[i]$.

Bevis

1. $N(1+i)=2$ och 2 är ett primtal i $\mathbb{Z}$, alltså är $1+i$ irreducibelt i $\mathbb{Z}[i]$ enligt .
2. $p^2 = N(p) = N((a+bi)(c+di)) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2) \Rightarrow a^2+b^2=p$ vilket är omöjligt om $p \equiv_4 3$.
3. $N(u+iv)=p$ gör $u+iv$ irreducibelt.