Algebra och talteori

MMGL31

Föreläsning 11/3

VT 2011

Samuel Bengmark

Repetition

Vilka p kan skrivas $p=a^2+b^2$?

- Såg enkelt att $p=a^2+b^2 \Rightarrow p \equiv_4 1$

Omvänt

- $p \equiv_4 1 \Rightarrow$ -1 är QR i $\mathbb{Z}_p$, dvs det finns tal A så att $-1 \equiv_p A^2$, mao $A^2+1 = A^2+1^2 = mp$ för något m.
- Fermats nedstegsmetod minskar m till 1.

Fermats nedstegsmetod

- $A^2+B^2 = Mp$
- Bilda $u \equiv_M A$ och $v \equiv_M B$ $-M/2 \leq u,v \leq M/2$
- Då är $u^2+v^2=rM$ för $1 \leq r < M$ eftersom
  - $u^2+v^2 \equiv_M A^2+B^2 \equiv_M 0$ dvs $u^2+v^2=rM$ för något r
  - $r=(u^2+v^2)/M \leq ((M/2)^2+(M/2)^2)/M = M/2 < M$
  - om r=0 vore u=v=0, dvs $A \equiv_M B \equiv_M 0$ dvs $A^2+B^2 \equiv_M 2\ 0$ dvs M|p, men eftersom M<p måste då M=1 och vi vore redan klara.
- Bilda $A_1=(uA+vB)/M$ och $B_1=(vA-uB)/M$.
  - Heltal ty $uA+vB \equiv_M A^2+B^2=Mp \equiv_M 0$ och $vA-uB \equiv_M BA-AB \equiv_M 0$
- $A_1^2+B_1^2=rp$, där r<M
  - $A_1^2+B_1^2=((uA+vB)/M)^2 + ((vA-uB)/M)^2 = (u^2+v^2)(A^2+B^2)/M^2 = (rM)(Mp)/M^2 = rp$
- Upprepa tills r=1.

Slutsats och fortsättning

$p=a^2+b^2 \Leftrightarrow p \equiv_4 1$

Vad gäller för sammansatta tal?

Sammansatta tal

- Om p och q kan skrivas som summor av två kvadrater så kan pq också göras det, enligt Brahmagupta-Fibonacci.

  $(u^2+v^2)(A^2+B^2)=(uA+vB)^2+(vA-uB)^2$

Slutsats

Om $m=k^2p_1p_2..p_k$, $p_i \equiv_4 1$ och alla olika så kan m skrivas som en summa av två kvadrater.

Ex $5=2^2+1^2$ & $5 \equiv_4 1$

$13=3^2+2^2$ $\quad 13 \equiv_4 1$

$5 \cdot 13 = (2^2+1^2)\cdot(3^2+2^2) =$

$= (2\cdot 3+1\cdot 2)^2 + (2\cdot 2-1\cdot 3)^2 =$

$= 8^2+1^2$

Ex $3 \cdot 5 \cdot 13$ går ej att skriva som två kvadrater

Ex $3^2 \cdot 5 \cdot 13 = 3^2(8^2+1^2) = (8\cdot 3)^2+(1\cdot 3)^2$

Ex $3^3 \cdot 5 \cdot 13$ går ej

Udda faktor av $p \equiv_4 3$?

- Antag $n=x^2+y^2$ samt att $p \equiv_4 3$ uppkommer $2j+1$ (ett udda antal) gånger i primtalsfaktoriseringen av n.
- Låt $d=SGD(x,y)$ där p förekommer i k gånger i primtalsfaktoriseringen av d. Bilda $a=x/d$ och $y=y/d$.
- Bilda $m=a^2+b^2$. Då kommer p|m eftersom $2j+1-2k$ är udda och ickenegativt.
- p∤a ty annars skulle $p|b^2=m-a^2$ och $SGD(a,b)\neq 1$. Alltså har $az \equiv_p b$ lösning då $SGD(a,p)=1$.
- $m=a^2+b^2=a^2+(az)^2=a^2(1+z^2)$.
- Modulo p innebär detta att $0 \equiv_p a^2(1+z^2)$.
- Då $SGD(a,p)=1$ är a inverterbart och $0 \equiv_p 1+z^2$ dvs -1 är QR i $\mathbb{Z}_p$, vilket är en motsägelse då $p \equiv_4 3$.

Slutsats

N kan skrivas som summan av två kvadrater omm $n=k^2p_1p_2..p_k$ där $p_i \equiv_4 1$ eller $p_i=2$.

Följdsats

Hypotenusan i en pytagoreisk trippel måste vara på formen $c=k^2p_1p_2..p_k$ där $p_i \equiv_4 1$ eller $p_i=2$

Bevis: Minns att en av parametriseringarna gav $(a,b,c)=(u^2-v^2,2uv,u^2+v^2)$

Generaliseringar

- Vilka tal kan skrivas som summa av tre kvadrater?
  - $2 = 1^2+1^2+0^2$
  - $3 = 1^2+1^2+1^2$
  - $5 = 2^2+1^2+0^2$
  - 7 = (dvs ej alla)
  - $11= 3^2+1^2+1^2$
- Vilka kan skrivas som summa av fyra kvadrater?
  - $7=2^2+1^2+1^2+1^2$
  - alla tal kan skrivas som summa av fyra kvadrater.

Resten av kursen

Nästan som att snabbt gå igenom hela kursen igen!

- Introducerar Gaussiska heltal
- Delbarhet, irreducibla tal, unik faktoruppdelning.
- Kongruensräkning och summa av två kvadrater kommer till stor nytta.

Gausiska heltal

Definition
Mängden $Z[i]=\{a+bi;\ a,b\in \mathbb{Z}\}$ 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 $\mathbb{C}$.

$(a+ib)\cdot((c+id)+(e+if)) = (a+ib)(c+id) + (a+ib)(e+if)$

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 och ad+bc=0.

Betrakat två fall:

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

Exempel
- 1+i | 1+3i eftersom 1+3i = (1+i)(2+i)
- 3+4i | 25 eftersom 25 = (3+4i)(3-4i)
- 1+i | 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},
  tex i | 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): $3\cdot3=3\cdot3\cdot1=3\cdot 3\cdot i\cdot(-i)= 3i(-3i)$.

Jämför med $3\cdot3=(-3)(-3)$ i $\mathbb{Z}$, där -1 är inverterbar. ($\mathbb{Z}^*=\{\pm1\}$.)

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=5·5.
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 heltal, dvs ett tal i $\mathbb{Z}$.

Två satser

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

Bevis

$$N((a+bi)(c+di)) = N(ac-bd+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 =$$
$$= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 = a^2(c^2+d^2)+b^2(d^2+c^2) =$$
$$(a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di)$$

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 skivas 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+vi)=p gör a+bi irreducibelt.