Matematik, KTH
Bengt Ek
Mars 2012
preliminär version

Material till kursen SF1662, Diskret matematik:

Mer om faktorisering

"Aritmetikens fundamentalsats" säger att varje naturligt tal utom 0 kan faktoriseras i primtal på, bortsett från ordningen mellan faktorerna, precis ett sätt (talet 1 är då "den tomma produkten", produkten av inga primtal alls). Här skall vi visa hur (nästan) samma bevis kan användas för att visa motsvarande för de **gaussiska heltalen** $\mathbb{Z}[\boldsymbol{i}]$, dvs alla komplexa tal med både real- och imaginärdel heltaliga, och för **polynom** med koefficienter bland de rationella talen $\mathbb{Q}$, de reella talen $\mathbb{R}$, de komplexa talen $\mathbb{C}$ eller $\mathbb{Z}_p$, p primtal.

Entydig faktorisering av heltal, igen

Vi börjar med att formulera om aritmetikens fundamentalsats lite och påminna oss beviset för den. Med denna omformulering blir det lätt att formulera en "abstraktare" sats, som direkt ger resultaten för $\mathbb{Z}[i]$ och $F[x]$, där F kan vara (t.ex.) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ eller $\mathbb{Z}_p$ (p primtal).

Definition: En **enhet** (eng. unit) bland heltalen är ett heltal u som har en multiplikativ invers, dvs det finns ett heltal u^{-1} så att $uu^{-1} = 1$. De enda enheterna bland heltalen är tydligen 1 och -1. Två heltal som skiljer sig med en faktor som är en enhet (dvs är $\pm$ varandra) kallas **associerade**.

Definition: Ett **irreducibelt element** bland heltalen är ett heltal π som inte är en enhet och bara kan faktoriseras med hjälp av enheter, dvs om $\pi = a \cdot b$ med a, b heltal är precis en av a och b 1 eller -1, dvs en enhet (om både a och b är enheter är $a \cdot b$ också det).
De irreducibla elementen bland heltalen är tydligen alla p och $-p$, p primtal.

Vårt huvudresultat för heltalen är nu (vi skall som sagt ovan se att motsvarande gäller för de gaussiska heltalen $\mathbb{Z}[i]$ och polynomen $F[x]$):

Sats (entydig faktorisering): Varje heltal utom 0 kan skrivas som en produkt av irreducibla element och en enhet (1 är produkten av 0 st irreducibla element). Faktoriseringen är **väsentligen unik**, dvs de irreducibla elementen i två faktoriseringar är parvis associerade.

T.ex. $-20 = (-1)\cdot 2\cdot 2\cdot 5 = (-2)\cdot 2\cdot 5 = (-1)\cdot(-5)\cdot(-2)\cdot 2 = (-2)\cdot(-5)\cdot(-2)$ etc. I alla faktoriseringarna av -20 i enheter och irreducibla element ingår precis två irreducibla element som är associerade med 2 och ett som är associerat med 5.

Satsen visas på samma sätt som vi tidigare i kursen gjorde för de naturliga talen (där det förstås inte finns andra enheter än 1, så a, b är associerade omm $a = b$).
Vi utgick från satsen om **division med rest**:

Om n, $d \in \mathbb{Z}$, $d \neq 0$ finns q, $r \in \mathbb{Z}$ med $n = qd + r$ och $|r| < |d|$.

Vi definierar **delbarhet** som att $m \mid n$ omm det finns q så att $n = qm$ och då en **största gemensam delare** till två heltal enligt

Definition: Om m, n är heltal, är en största gemensam delare, sgd (eng. gcd), till m och n ett heltal d så att

i) $d \mid m$, $d \mid n$ gemensam delare
ii) $c \mid m$, $c \mid n \Rightarrow c \mid d$ "störst"

(Jämfört med tidigare släpper vi alltså villkoret att $d \geq 0$.)

Med satsen om division visas då

Sats: För alla heltal m, n finns en största gemensam delare $\boldsymbol{d = sgd(m, n)}$ och $\boldsymbol{d = am + bn}$ för några heltal a, b. Alla största gemensamma delare till m, n är associerade (följer av att de är delare till varandra).

Största gemensamma delare kan bestämmas med **Euklides algoritm**
($sgd(m, n) = sgd(n, m) = sgd(\pm m, \pm n)$.)

$$
\begin{aligned}
m &= q_1 n + r_1 && 0 \leq |r_1| < |n| \\
n &= q_2 r_1 + r_2 && 0 \leq |r_2| < |r_1| \\
r_1 &= q_3 r_2 + r_3 && 0 \leq |r_3| < |r_2| \\
&\vdots \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} && 0 \leq |r_{k-1}| < |r_{k-2}| \\
r_{k-2} &= q_k r_{k-1} + 0
\end{aligned}
$$

vilket ger (en)

$$\boldsymbol{sgd(m, n) = r_{k-1}}.$$

Genom att "lösa ut" fås som förut att $d = am + bn$ för några heltal a, b.

Följdsats: Om d, m, n är heltal så att $d \mid mn$ och $sgd(d, m)$ är enheter (d och m är **relativt prima**), så $d \mid n$.

Med induktion visas att alla heltal är associerade till produkter av irreducibla element och med följdsatsen ovan att de irreducibla elementen som används i två sådana faktoriseringar av ett heltal är parvis associerade, dvs satsen om entydig faktorisering av heltal.

Entydig faktorisering i $\mathbb{Z}[i]$ och $F[x]$, då

Nu skall vi se hur man får motsvarande entydiga faktorisering för de **gaussiska heltalen** $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ och **polynom med koefficienter i F**, $F[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \mid a_n, \ldots, a_0 \in F,\ n \in \mathbb{N}\}$, där F kan vara $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ eller $\mathbb{Z}_p$ (p primtal).

Låt nu M stå för någon av $\mathbb{Z}[i]$ och dessa $F[x]$.
I M kan vi addera och multiplicera element och det finns element 0 och 1 i M så att man kan räkna "som vanligt", dvs med samma allmänna räkneregler som i $\mathbb{Z}$.

Närmare bestämt:
För alla $s, t, u \in M$ gäller

$s + t \in M$	$s \cdot t \in M$
$(s + t) + u = s + (t + u)$	$(s \cdot t) \cdot u = s \cdot (t \cdot u)$
$s + t = t + s$	$s \cdot t = t \cdot s$
$s + 0 = s$	$s \cdot 1 = s$
det finns $-s \in M$ med $s + (-s) = 0$	$s \cdot (t + u) = s \cdot t + s \cdot u$

Dessa "räkneregler" gör att M är vad som kallas en **kommutativ ring med etta**.
Vi kan nu definiera begreppen enhet, associerade element och irreducibelt element i M liksom i $\mathbb{Z}$, men egenskaperna ovan räcker inte för att ge entydig faktorisering i M.

Exempel: $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ är en kommutativ ring med etta (dvs den uppfyller reglerna ovan, kontrollera gärna det), men där gäller inte entydig faktorisering, ty $6 = (1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \cdot 3$, där $1 \pm i\sqrt{5}, 2, 3$ alla är irreducibla och $1 + i\sqrt{5}$ inte är associerad med 2 eller 3.

Däremot gäller entydig faktorisering om man har en motsvarighet till satsen om division med rest:

Definition: En **euklidisk valuation** ν på M är en funktion så att
1. $\nu(s) \in \mathbb{N}$ om $s \in M \setminus \{0\}$ och $\nu(0) = -\infty$,
2. för alla $s, d \in M$, $d \neq 0$ finns q, $r \in M$ med
$$s = qd + r \text{ och } \nu(r) < \nu(d),$$
3. för alla $s, t \in M \setminus \{0\}$ gäller $\nu(s) \leq \nu(st)$.

(Symbolen $-\infty$ uppfyller förstås $-\infty < a$ för alla naturliga tal a.)

En kommutativ ring med en euklidisk valuation kallas en **euklideisk ring** och beviset för existens av sgd och användningen av Euklides algoritm fungerar som för heltalen. De ger som för heltalen att entydig faktorisering gäller som i $\mathbb{Z}$.

$\mathbb{Z}$, $\mathbb{Z}[i]$ och $F[x]$ är euklidesika ringar, med $\nu(n) = |n|$ för $n \in \mathbb{Z} \setminus \{0\}$, $\nu(z) = |z|^2$ för $z \in \mathbb{Z}[i] \setminus \{0\}$ och $\nu(f) = f$:s grad (dvs det största n med $a_n \neq 0$) om $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[x] \setminus \{0\}$.

De gaussiska heltalen $\mathbb{Z}[i]$

Enheterna i $\mathbb{Z}[i]$ är ju de inverterbara elementen, dvs 1, -1, i och $-i$. De är alltså precis de $z \in \mathbb{Z}[i]$ som uppfyller $\nu(z) = 1$.

De irreducibla elementen i $\mathbb{Z}[i]$ kallas **gaussiska heltal**. Hur känner man då igen dem?
Låt g vara ett gaussiskt primtal. Om man primfaktoriserar (i $\mathbb{Z}$) det reella heltalet $\nu(g)$ fås $\nu(g) = g\bar{g} = p_1 \cdot p_2 \cdot \ldots \cdot p_n$, men detta är också en produkt i $\mathbb{Z}[i]$, så det irreducibla elementet g delar någon faktor, $g \mid p_k$, något k. Kalla p_k för p. Då fås också $\bar{g} \mid p$ och alltså $|g|^2 \mid p^2$ och det reella heltalet $|g|^2$ måste vara någon av de positiva delarna till p^2, dvs 1, p eller p^2. Eftersom g inte är en enhet är $|g| \neq 1$.

För alla primtal $p \equiv_4 1$ finns (enligt en sats av Fermat från 1640) två (reella) heltal a, b så att $p = a^2 + b^2$, dvs $p = (a + bi)(a - bi)$ och g är associerat med $a + bi$ eller $a - bi$ (entydig faktorisering), $|g|^2 = p$. Beviset för Fermats sats ger vi inte här.
Om $p = 2$ är g associerat med $1 + i$, ty $2 = (1 + i)(1 - i)$.
Om $p \equiv_4 3$ är $|g|^2 = a^2 + b^2 \neq p$ (ty $a^2, b^2 \equiv_4 0$ eller 1) och $g = u \cdot p$, u en enhet (entydig faktorisering, $g \mid g\bar{g} = p^2$, så $g \mid p$ och $|g| = p$), dvs g och p är associerade.

Det finns alltså **tre typer av gaussiska heltal**:

- $a + bi$, där $a, b \in \mathbb{Z}$ och $a^2 + b^2 = p$, ett (reellt) primtal som är $\equiv_4 1$,
- associerade med $1 + i$ (dvs $\pm(1 \pm i)$),
- associerade med p, ett reellt primtal som är $\equiv_4 3$ (dvs $\pm p$ eller $\pm ip$).

Får att **faktorisera ett gaussiskt heltal z** i irreducibla faktorer (gaussiska primtal) kan man alltså:
Faktorisera $|z|^2$ i reella primtal, $|z|^2 = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ och

- för varje $p_k \equiv_4 1$, finn $a_k, b_k \in \mathbb{Z}$ så att $p_k = a_k^2 + b_k^2$. Då är minst en av $a_k \pm b + ki$ en (prim)faktor i z,
- för varje $p_k = 2$ finns en (prim)faktor $1 + i$ i z,
- för varje p_k^2 med $p_k \equiv_4 3$ (de finns alltid parvis i $|z|^2$) finns en (prim)faktor p_k i z.

Exempel: För att faktorisera $z = 44835 - 33075i$, beräkna och faktorisera reellt $|z|^2 = 44835^2 + 33075^2 = 3104132850 = 2 \cdot 3^2 \cdot 5^2 \cdot 7^4 \cdot 13^2 \cdot 17$.
3^2 ger faktorn 3 och 7^4 ger faktorn 7^2 ($3, 7 \equiv_4 3$) och 2 ger faktorn $1 + i$. 5^2 ger två faktorer $2 \pm i$ (enklare förstås att börja med att bryta ut $5 = (2 + i)(2 - i)$ ur z), 13^2 ger två termer $3 \pm 2i$ och 17 ger en faktor $4 \pm i$. Man får testa om det i varje fall skall vara + eller −. Man finner $z = 3 \cdot 7^2(1 + i)(2 + i)(2 - i)(3 - 2i)^2(4 - i)$.

Polynomen $F[x]$

Se föreläsningssammanfattningen för F6.