Föreläsning 11

Anteckning...	TMV200 Föreläsningar		
Skapad:	2020-12-01 13:15	**Ändrad:**	2020-12-01 15:02
Författare:	hchristian.johansson@gmail.com		

TMV200 1/12-20

Resten av kursen:

Talteori

Teorin om heltalen ("diskreta" talsystem)

Delbarhet: Låt $a, b \in \mathbb{Z}$.

Vi säger att a delar b om det finns ett $m \in \mathbb{Z}$ så att $am = b$.

Skriver $a \mid b$ om a delar b, $a \nmid b$ om a inte delar b.

(Informellt: a delar b om b/a är ett heltal, eller $a = b = 0$).

Delbarhet är en relation på $\mathbb{Z}$.

Några egenskaper (5.4 i boken)

1) $a \mid 0$ $\forall a \in \mathbb{Z}$.

2) $a \mid a$ $\forall a \in \mathbb{Z}$ (reflexivitet)

3) $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$ $\forall a,b,c \in \mathbb{Z}$ (transitivitet)

4) $0 \nmid a$ om $a \neq 0$.

5) Låt $a,b,c \in \mathbb{Z}$. Då gäller $(a \mid b \wedge a \mid c) \iff a \mid mb+nc$ $\forall m,n \in \mathbb{Z}$.

$mb+nc$ kallas för en linjär kombination av b och c.

Försök gärna visa 5) som övning.

För att summera: Delbarhet är reflexiv och transitiv.

Den är "nästan antisymmetrisk":

Sats (5.7 i boken) Om $a \mid b$ och $b \mid a$, så gäller antingen $a = b$ eller $a = -b$.

Bevis: Fall 1: $a = 0$: Då gäller $0 \mid b \Rightarrow b = 0$ så $a = b = -b$.

Fall 2: $a \neq 0$: $a \mid b \Rightarrow \exists m \in \mathbb{Z}: am = b$.
$b \mid a \Rightarrow \exists n \in \mathbb{Z}: bn = a$.

Alltså är $a = bn = (am)n = amn \Rightarrow$

$\Rightarrow 1 = mn$, $m,n \in \mathbb{Z}$.
$a \neq 0$

På måste $m = n = 1$ eller $m = n = -1$.

Om $m = n = 1$ får vi $a = b$, om $m = n = -1$ får vi $a = -b$. □

Division med rest

Divisionsalgoritmen:

Divisionsalgoritmen

Låt $a, b \in \mathbb{Z}_+$. Då finns det unika $q, r \in \mathbb{N}$ så att

$$a = bq + r \quad \text{och} \quad 0 \leq r < b.$$

q kallas för kvoten och r för resten.

Hur hittar man q? q är det största talet så att $a - qb$ är ≥ 0. r är då definierat som $a - bq$.

Ex: $a = 13$, $b = 4$, $13 = 4 \cdot 3 + 1$, $q = 3$, $r = 1$.

$a = 75$, $b = 13$ $\quad 75 = 5 \cdot 13 + 10$, $q = 5$, $r = 10$.

Gemensamma delare

Def: Låt $a, b \in \mathbb{Z}$, inte bägge $= 0$.

En gemensam delare av a och b är ett $d \in \mathbb{Z}$ så att $d \mid a$ och $d \mid b$.

En gemensam delare uppfyller $d \leq \max(a, -a, b, -b)$ så det finns en största gemensamma delare till a och b (obs! 1 är alltid en gemensam delare).

Skrivs: $\gcd(a, b)$. Alltid positiv.

Ex: $a = 4$, $b = 6$.

4 har positiva delare 1, 2, 4.

6 har positiva delare 1, 2, 3, 6.

d.v.s. $2 = \gcd(4, 6)$.

Sats (5.14 i boken)

1) $\text{sgd}(a,0) = a \qquad \forall a \in \mathbb{Z}_+$.

2) $\forall a,b,n \in \mathbb{Z}, \quad \text{sgd}(a+nb, b) = \text{sgd}(a,b)$.

Bevis: 1) $a \mid a$ och $a \mid 0$, så a är en gemensam delare.
Om $d \mid a$ så är $d \leq a$. Alltså är $a = \text{sgd}(a,0)$.

2) Vi visar att (a,b) och $(a+nb,b)$ har samma gemensamma delare, det följer då att $\text{sgd}(a,b) = \text{sgd}(a+nb,b)$.

Om $d \mid a \wedge d \mid b$, så får vi $d \mid a+nb$ (se nr 5) under egenskaper i början), så

$d \mid a+nb$ och $d \mid b$.

Andra hållet: $d \mid a+nb \wedge d \mid b \Rightarrow$

$\Rightarrow d \mid (a+nb)-nb$, dvs $d \mid a$.

Så $d \mid a \wedge d \mid b$.

Alltså har (a,b) och $(a+nb,b)$ samma delare. □

Euklides algoritm

$a,b \in \mathbb{Z}_+$, $a \geq b$. Genom upprepad division med rest får vi

$$\begin{aligned}
a &= b q_1 + r_1, && 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2, && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

Slutar när $r_k = 0$

Då är $\gcd(a,b) = r_n$

Bevis: $\gcd(a,b) = \gcd(\overbrace{a - bq_1}^{= r_1}, b) =$

$= \gcd(r_1, b) = \gcd(r_1, \underbrace{b - r_1 q_2}_{= r_2}) = \gcd(r_1, r_2) = \dots$

$\dots = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1} - r_n q_{n+1}, r_n) =$

$= \gcd(0, r_n) = r_n$. □

Ex 1) $a = 6$, $b = 4$.

$6 = 4 \cdot 1 + 2$

$4 = 2 \cdot 2 + 0$ $\Rightarrow$ $\gcd(6,4) = 2$.

2) $a = 876$, $b = 204$

$876 = 204 \cdot 4 + 60$

$204 = 60 \cdot 3 + 24$

$60 = 24 \cdot 2 + 12$

$24 = 12 \cdot 2 + 0$ $\Rightarrow$ $\gcd(876, 204) = 12$.

Bezouts identitet: Låt $a, b \in \mathbb{Z}$. Då finns $m, n \in \mathbb{Z}$ så att $\gcd(a,b) = ma + nb$.

Kan hitta m och n genom att "gå baklänges" i Euklides algoritm.

Ex $a = 876$, $b = 204$. $\gcd(876, 204) = 12$

Hitta $m, n \in \mathbb{Z}$ så att $12 = 876m + 204n$.

$876 = 204 \cdot 4 + 60$

$$204 = 60 \cdot 3 + 24$$
$$60 = 24 \cdot 2 + 12$$
$$24 = 12 \cdot 2.$$

Nu: "gå baklänges":

$$12 = 60 - 24 \cdot 2 =$$
$$= 60 - (\underbrace{204 - 60 \cdot 3}_{=24}) \cdot 2 =$$
$$= 60 - 204 \cdot 2 + 60 \cdot 6 =$$
$$= 60 \cdot 7 - 204 \cdot 2 =$$
$$= (\underbrace{876 - 4 \cdot 204}_{=60}) \cdot 7 - 204 \cdot 2 =$$
$$= 876 \cdot 7 - 28 \cdot 204 - 2 \cdot 204 =$$
$$= 876 \cdot 7 - 30 \cdot 204$$

Så $12 = 876 \cdot 7 - 30 \cdot 204$

dvs $m = 7$, $n = -30$ funkar.

Linjära diofantiska ekvationer (i två variabler).

Skall titta på hur man löser ekvationer av typen

$$ax + by = c$$

där $a, b, c \in \mathbb{Z}$ är givna heltal och vi söker lösningar $x, y \in \mathbb{Z}$.

Ex $2x + 4y = 1$ saknar lösningar med $x, y \in \mathbb{Z}$:

$2 \mid 2x + 4y \quad \forall x, y \in \mathbb{Z}$ men $2 \nmid 1$.

Sats (5.22 i boken)

$ax + by = c$ lösbar i heltal $x, y \iff \gcd(a, b) \mid c$.

Hur kan man hitta en lösning om $\text{sgd}(a,b) \mid c$?

Sätt $d = \text{sgd}(a,b)$ och $r = \frac{c}{d} \in \mathbb{Z}$.

Enligt Bezouts identitet finns $m, n \in \mathbb{Z}$ så att

$$am + bn = d$$

Multiplicera med r : $amr + bnr = dr = c$

Så $x = mr$ och $y = nr$ är en lösning.

m, n, d hittas genom Euklides algoritm.

Ex

$$3x + 7y = 2$$

$$\left.\begin{aligned} 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}\right\} \Rightarrow \text{sgd}(7,3) = 1,$$ så det finns lösningar.

Baklänges i Euklides algoritm:

$$1 = 7 - 3 \cdot 2$$

$$\Rightarrow \quad 2 = 7 \cdot 2 - 3 \cdot 4,$$ så $x = -4$, $y = 2$ är en lösning.

Notera att $x = -11$, $y = 5$ också är en lösning:

$$3(-11) + 7 \cdot 5 = -33 + 35 = 2.$$

Sats (5.25) Om $\text{sgd}(a,b) = 1$ och $r, s \in \mathbb{Z}$ är sådana att

$$ar + bs = c$$

Då är

$$\{ (x,y) = (r - bm, s + am) \mid m \in \mathbb{Z} \}$$

mängden av alla lösningar till ekvationen $ax + by = c$.

I exemplet ovan är $(-4, 2)$ en lösning till $3x + 7y = 2$.

Vi får (nya) lösningar

$$(-4 - 7m, 2 + 3m) \quad \text{för alla } m \in \mathbb{Z}.$$

$m = 0$ ger $(-4, 2)$, $m = 1$ ger $(-11, 5)$, dvs den andra lösningen ovan.