Forrige gang: * Div alg: gitt $a,b \in \mathbb{Z}$ med $b>0$ så finnes unike $q,r \in \mathbb{Z}$ med $a = qb+r$ og $0 \leq r \leq b-1$

* Egenskaper ved delelighet (Teorem 2.2).

Def: La $a,b \in \mathbb{Z}$ med minst en av dem ulik 0

(1) Den <u>største felles divisoren</u> til a og b er det største positive tallet som deler begge; betegnes $\gcd(a,b)$. Så $d = \gcd(a,b)$ hvis

(i) $d|a$ og $d|b$

(ii) hvis $c|a$ og $c|b$ så må $c \leq d$

(2) Tallene a og b er <u>relativt primiske</u> dersom $\gcd(a,b) = 1$.

Eksempel: $\gcd(24,20) = 4$, $\gcd(24,6) = 6$, $\gcd(10,9) = 1$ (9 og 10 er rel. pr.)

<u>Teorem 2.4/2.5/2.6 m/Korollar</u>

(1) Det finnes $x,y \in \mathbb{Z}$ slik at $\gcd(a,b) = ax+by$

(2) $\gcd(a,b)=1 \iff$ det finnes $x,y \in \mathbb{Z}$ slik at $ax+by=1$

(3) $\gcd(a,b)=d \Rightarrow \gcd(a/d, b/d) = 1$

(4) Hvis $a|c$, $b|c$ og $\gcd(a,b)=1$, så vil $ab|c$

(5) (Euklids lemma) Hvis $a|bc$ og $\gcd(a,b)=1$, så må $a|c$

Bevis: (1) Se på følgende mengde:

$$S = \{ax+by \mid x,y \in \mathbb{Z} \text{ og } ax+by > 0\}$$

Da er $S \neq \emptyset$ (vis dette). Siden $S \subseteq \mathbb{N}$ garanterer Velordningsprinsippet at S inneholder et minste element $d = ax_0+by_0$. Skal vise at $d = \gcd(a,b)$.

Div alg gir $a = qd+r$ hvor $0 \leq r \leq d-1$, som gir

$$r = a-qd = a-q(ax_0+by_0) = a(1-qx_0)+b(-y_0)$$

Hvis $r>0$ er da $r \in S$, en motsigelse siden $r \leq d-1$ og d er det minste elt i S. Så $r=0$, altså vil $d|a$. Tilsvarende vil $d|b$. La nå $c \in \mathbb{Z}$ være slik at $c|a$ og $c|b$. Da gir Teorem 2.2(g) at $c|(ax+by)$ $\forall x,y \in \mathbb{Z}$. Spesielt vil $c|d$, så $c \leq d$. Dette viser at $d = \gcd(a,b)$

(2) Hvis $\gcd(a,b)=1$ følger det fra (1) at $\exists\, x,y \in \mathbb{Z}$ med $ax+by=1$. Anta motsatt at slike x,y finnes, og la $d = \gcd(a,b)$. Siden $d|a$ og $d|b$, gir Teorem 2.2(g) at $d|(ax+by)$, dvs $d|1$. Siden $d \geq 1$ er da $d=1$.

(3) Hvis $\gcd(a,b)=d$ gir (1) at $\exists\, x,y\in\mathbb{Z}$ med $d=ax+by$.
Da får vi
$$1=(a/d)x+(b/d)y$$
og fra (2) ser vi da at $\gcd(a/d, b/d)=1$ (merk at $a/d$ og $b/d$ er heltall siden $d|a$ og $d|b$).

(4) Anta $a|c$ og $b|c$. Da $\exists\, q_1,q_2\in\mathbb{Z}$ med $c=q_1a$ og $c=q_2b$.
Hvis i tillegg $\gcd(a,b)=1$, finnes fra (1) $x,y\in\mathbb{Z}$ med $1=ax+by$.
Dette gir
$$c=cax+cby=(q_2b)ax+(q_1a)by=ab(q_2x+q_1y)$$
så $ab|c$

(5) Hvis $a|bc$ så $\exists\, q\in\mathbb{Z}$ med $bc=qa$. Hvis i tillegg $\gcd(a,b)=1$
finnes $x,y\in\mathbb{Z}$ med $ax+by=1$, som gir
$$c=cax+cby=cax+(qa)y=a(cx+qy)$$
så $a|c$. □

Merk: (1) Som for induksjonsprinsippet og div alg er det Velordningsprinsippet som er grunnlaget.

(2) La $d=\gcd(a,b)$. Da er (vis dette)
$$\{dq \mid q\in\mathbb{Z}\}=\{ax+by \mid x,y\in\mathbb{Z}\}$$

Eksempler: (1) $\gcd(24,20)=4$ og $4=24\cdot 1+20\cdot(-1)$
$\gcd(120,66)=6$ og $6=120\cdot 5+66\cdot(-9)$

(2) Siden $1=49\cdot(-2)+33\cdot 3$ er $\gcd(33,49)=1$

(3) $\gcd(120,66)=6$ så $\gcd(120/6, 66/6)=1$, dvs $\gcd(20,11)=1$.

(4) $4|60$ og $5|60$, så siden $\gcd(4,5)=1$ vil $4\cdot 5|60$, dvs $20|60$
$6|60$ og $15|60$, men $6\cdot 15\nmid 60$ (og $\gcd(6,15)\neq 1$)

(5) $6\mid 15\cdot 4$ men $6\nmid 15$ og $6\nmid 4$ (og $\gcd(6,15)\neq 1\neq\gcd(6,4)$)
$6\mid 5\cdot 12$ og $\gcd(6,5)=1$, så $6|12$

(6) Oppg 2.3.20(f), utvidet versjon:
$$\gcd(a,b)=1 \implies \gcd(a^m,b^n)=1 \quad \forall\, m,n\geq 1$$
Hvis $1=\gcd(a,b)$ så $\exists\, x,y\in\mathbb{Z}$ med $1=ax+by$. Gir
$$1=(ax+by)^m=\binom{m}{0}(ax)^m+\binom{m}{1}(ax)^{m-1}(by)^1+\binom{m}{2}(ax)^{m-2}(by)^2+\cdots$$
$$=a^m\cdot(mx^m)+b\cdot k$$
så $\gcd(a^m,b)=1$. Samme argument gir da $\gcd(a^m,b^n)=1$.

Skal se: Gitt $a, b, c$, har ligningen

$$ax + by = c$$

heltallsløsninger? Hvis ja, kan vi finne dem? Dette blir temaet i Seksjon 2.5.

Eksempler: (1) Ligningen

$$15x + 6y = 24$$

har heltallsløsn, blant annet $x = 8, y = -16$ siden $15 \cdot 8 + 6 \cdot (-16) = 24$

(2) Ligningen

$$15x + 6y = 25$$

har ingen heltallsløsn. Hvorfor?

**Teorem 2.9** (Første del)

La $a, b, c \in \mathbb{Z}$. Da har ligningen

$$ax + by = c$$

heltallsløsninger hvis og bare hvis $\gcd(a, b)$ deler $c$.

Bevis: La $d = \gcd(a, b)$. Fra Teorem 2.4 vet vi at $\exists\, x_0, y_0 \in \mathbb{Z}$ med

$$ax_0 + by_0 = d.$$

Hvis $d \mid c$, er $c = qd$ for en $q \in \mathbb{Z}$, som gir

$$a(qx_0) + b(qy_0) = qd = c$$

Så da er $ax + by = c$ løsbar. Motsatt, hvis ligningen er løsbar, finnes $x_1, y_1 \in \mathbb{Z}$ med $ax_1 + by_1 = c$. Fra Teorem 2.2 vil $d \mid (ax_1 + by_1)$, siden $d \mid a$ og $d \mid b$. Så $d \mid c$. □