(Diskret matte F, ht17: F2, ti 31 okt 2017)

Den **linjära diofantiska** (dvs vi söker heltalslösningar x, y) **ekvationen**

$$\boldsymbol{mx + ny = c} \qquad \boldsymbol{m, n, c} \text{ heltal}$$

är lösbar **omm** $\text{sgd}(m, n) \mid c$.

Om villkoret är uppfyllt, inte $m = n = 0$, och $d = \text{sgd}(m, n) = am + bn$ med $a, b \in \mathbb{Z}$ ges **alla** lösningar till ekvationen av $\begin{cases} x = \frac{c}{d}a + \frac{n}{d}k \\ y = \frac{c}{d}b - \frac{m}{d}k \end{cases}$, $k \in \mathbb{Z}$.

Den "normala" metoden för att lösa en sådan ekvation är att göra som i beviset för satsen, dvs bestämma $\text{sgd}(m, n) = d$ (med Euklides algoritm), dividera ekvationen med d, uttrycka 1 som en linjärkombination av (den nya) ekvationens koefficienter och multiplicera med dess högerled för att få en heltalslösning. **Eulers metod** (inte behandlad i boken) tar med högerledet från början och leder i allmänhet till mindre tal i den första lösningen.
Säg t.ex. att vi söker alla heltalslösningar till ekvationen $108x + 33y = 78$.
Euklides algoritm: $108 = 33 \cdot 3 + 9,\ 33 = 9 \cdot 3 + 6,\ 9 = 6 \cdot 1 + 3,\ 6 = 3 \cdot 2 + 0$, så $d = \text{sgd}(108, 33) = 3$.
Division med d ger den ekvivalenta ekvationen $36x + 11y = 26$, där $\text{sgd}(36, 11) = 1$.
"Normala" metoden:
Från ovan: $36 = 11 \cdot 3 + 3,\ 11 = 3 \cdot 3 + 2,\ 3 = 2 \cdot 1 + 1,\ (2 = 1 \cdot 2 + 0)$ och "baklänges" ger det $1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = -11 + 4 \cdot 3 = -11 + 4(36 - 3 \cdot 11) = 4 \cdot 36 - 13 \cdot 11$.
Multiplikation med 26 ger att $x_0 = 4 \cdot 26 = 104,\ y_0 = (-13) \cdot 26 = -338$ löser ekvationen.
Om x, y löser ekvationen blir $36(x - x_0) + 11(y - y_0) = 26 - 26 = 0$, så $36(x - x_0) = -11(y - y_0)$ och $11 \mid (x - x_0)$ (ty $\text{sgd}(11, 36) = 1$), $x = x_0 + 11k$, k ett heltal. Det ger $y - y_0 = -36k$ och insättning visar att dessa x, y också löser ekvationen för alla heltal k.
Eulers metod:
Lös ut den obekanta med (till beloppet) lägst koefficient: $y = \frac{26}{11} - \frac{36x}{11} = 2 - 3x + \frac{4-3x}{11}$.
x, y är en heltalslösning omm x och $z = \frac{4-3x}{11}$ är heltal, så omm x, z heltal med $3x + 11z = 4$, dvs $x = \frac{4}{3} - \frac{11z}{3} = 1 - 3z + \frac{1-2z}{3}$, så omm $z, u = \frac{1-2z}{3}$ heltal, dvs omm z, u är heltal med $2z + 3u = 1$, dvs $z = -u + \frac{1-u}{2}$, så omm $u, k = \frac{1-u}{2}$ heltal, så $u = 1 - 2k$, där k är ett godtyckligt heltal.
Insättning ger $z = -(1 - 2k) + \frac{1-(1-2k)}{2} = -1 + 3k$, $x = 1 - 3(-1 + 3k) + \frac{1-2(-1+3k)}{3} = 5 - 11k$ och $y = 2 - 3(5 - 11k) + \frac{4-3(5-11k)}{11} = -14 + 36k$.
Båda metoderna ger samma lösningar (med olika k, $k_{\text{normal}} = -k_{\text{Euler}} - 9$).

Aritmetikens fundamentalsats:
Varje heltal ≥ 1 kan på ett entydigt (bortsett från ordningen) sätt uttryckas som en produkt av primtal. (1 är "den tomma produkten".)

[Beviset för satsen bygger på möjligheten till division med en rest som är "mindre" än divisorn. Det gör att motsvarande sats om entydig (nästan) faktorisering gäller också för polynom och gaussiska heltal (faktoriseringarna kan här skilja sig åt dels vad gäller ordningen och dels faktorer som är konstanter respektive $1, i, -1, -i$).]

Om $m = p_1^{s_1} \dots p_k^{s_k}, n = p_1^{t_1} \dots p_k^{t_k}$ är
$\text{sgd}(m, n) = p_1^{min(s_1,t_1)} \dots p_k^{min(s_k,t_k)}$ och $\text{mgm}(m, n) = p_1^{max(s_1,t_1)} \dots p_k^{max(s_k,t_k)}$.

Sats (Euklides):
Det finns oändligt många primtal.

(I själva verket är serien $\sum_{p \text{ primtal}} \frac{1}{p}$ divergent, så primtalen ligger "ganska tätt".)

Modulär aritmetik

$$\boldsymbol{x \equiv y \pmod{m}}, \quad \text{eller} \quad \boldsymbol{x \equiv_m y}$$

betyder $m|(x-y)$ och läses "x är kongruent med y modulo m".

Mängden av alla heltal, $\mathbb{Z}$, delas in i m st klasser av kongruenta tal:

$$[0]_m = \{0, \pm m, \pm 2m, \dots\},$$
$$[1]_m = \{1, \pm m + 1, \pm 2m + 1, \dots\},$$
$$\vdots$$
$$[m-1]_m = \{-1, \pm m - 1, \pm 2m - 1, \dots\}.$$

Mängden av dessa ("heltalen modulo m"): $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$.

Sats: $x_1 \equiv_m x_2,\ y_1 \equiv_m y_2 \ \Rightarrow\ x_1 + y_1 \equiv_m x_2 + y_2,\ x_1 y_1 \equiv_m x_2 y_2$.

Så vi kan **definiera** $+$ och $\cdot$ på $\mathbb{Z}_m$:

$$[a]_m \circ [b]_m = [a \circ b]_m \quad \text{för} \quad \circ = +, \cdot$$

Vi skriver oftast $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ och räknar $+$ och $\cdot$ "som vanligt men med rest mod m".

Man finner $\boldsymbol{x \equiv \theta(x) \pmod 9}$, där $\theta(x)$ är x:s siffersumma (i bas 10), speciellt $9 \mid x \Leftrightarrow 9 \mid \theta(x)$, vilket gör det lätt att avgöra om $9 \mid x$.
(Det följer att också $x \equiv \theta(x) \pmod 3$ och $3 \mid x \Leftrightarrow 3 \mid \theta(x)$.)
Obs att $\theta(x \circ y) \equiv_9 x \circ y \equiv_9 \theta(x) \circ \theta(y)$ för $\circ = +, \cdot$, så

$$\boldsymbol{x \cdot y = z \Rightarrow \theta(x) \cdot \theta(y) \equiv_9 \theta(z)} \text{ och } \boldsymbol{x + y = z \Rightarrow \theta(x) + \theta(y) \equiv_9 \theta(z).}$$

(Detta kan användas för att kontrollera beräkningar, ty $\theta(x) \circ \theta(y) \not\equiv_9 \theta(z) \Rightarrow x \circ y \neq z$.
Man kan också använda siffersummans siffersumma etc, $\theta(\theta(\dots\theta(x)\dots))$ i stället för $\theta(x)$.)

Definition: $r \in \mathbb{Z}_m$ är **inverterbart** omm det finns $x \in \mathbb{Z}_m$ med $rx = 1$ i $\mathbb{Z}_m$. Detta x kallas r^{-1}, r:s **invers**.

$rx = 1$ i $\mathbb{Z}_m$ omm $rx - km = 1$ för något $k \in \mathbb{Z}$, så r^{-1} kan bestämmas med Euklides algoritm.

Sats: $r \in \mathbb{Z}_m$ är inverterbart omm $\text{sgd}(r, m) = 1$ (i $\mathbb{Z}$).

U_m: mängden av inverterbara element i $\mathbb{Z}_m$.
$x, y \in U_m \ \Rightarrow\ xy, x^{-1} \in U_m$