(SF1662 Diskret matte, vt15: F4, to 29 jan 2015)

Modulär aritmetik

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

betyder $m|(x-y)$ (dvs att x och y ger samma principala rest vid division med m) och läses "x är kongruent med y modulo m".

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

Varje heltal är kongruent med precis ett av $0, 1, 2, \ldots, m-1$ (i fallet $m = 2$ är alla jämna tal kongruenta med 0 och de udda med 1) och att räkna **modulo m** innebär att "räkna som vanligt, men bara behålla resten mod m".
Man låter $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ och skriver t.ex.

$$4 \cdot 6 \equiv 3 \pmod{7}, \ \ 4 \cdot 6 \equiv_7 3 \ \text{ eller } \ 4 \cdot 6 = 3 \text{ i } \mathbb{Z}_7.$$

Ex. Om $x = (x_n x_{n-1} \ldots x_1 x_0)_{10}$ fås

$$x \equiv_9 x_n + x_{n-1} + \ldots + x_1 + x_0 = \theta(x),\ x\text{:s siffersumma.}$$

och $9 \mid x \Leftrightarrow 9 \mid \theta(x)$ och på samma sätt $3 \mid x \Leftrightarrow 3 \mid \theta(x)$.

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

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

Speciellt om **p primtal**: y i $\mathbb{Z}_p,\ y \neq 0 \Rightarrow y$ inverterbart i $\mathbb{Z}_p$.

Om $1 = ar + bm$ (fås med Euklides algoritm) är $r^{-1} = a$ i $\mathbb{Z}_m$.

Linjära kongruenser (mod m), dvs **linjära ekvationer i $\mathbb{Z}_m$**,

$$ax \equiv b \pmod{m} \ \text{ eller, ekvivalent, } \ ax = b \text{ i } \mathbb{Z}_m.$$

De är ekvivalenta med att för något heltal k gäller (dvs vår välkända diofantiska ekvation för heltalen x, k)

$$ax - mk = b,$$

vilken ju har lösningar (fås med Euklides algoritm) omm för $d = \text{sgd}(a, m)$ gäller $d \mid b$. Om $d = 1$ (dvs a inverterbart i $\mathbb{Z}_m$) finns alltid precis en lösning i $\mathbb{Z}_m$. Om x_0 är en lösning ges den allmänna lösningen av $x = x_0 + q\frac{m}{d},\ q$ heltal, så det finns d olika lösningar (mod m).

Följande regler för att handskas med linjära kongruenser kan formuleras:

$$\begin{cases} ax \equiv_m ay & \Leftrightarrow \quad x \equiv_m y & \textbf{om } \text{sgd}(a, m) = 1 \\ ax \equiv_{an} ay & \Leftrightarrow \quad x \equiv_n y & \\ ax \equiv_{an} y & \text{olösbar om } a \nmid y & \end{cases}$$

Detta hanns inte med:

$$\text{Om } \text{sgd}(m, n) = 1 \text{ gäller } a \equiv b \pmod{mn} \Leftrightarrow \begin{cases} a \equiv b \pmod{m}, \\ a \equiv b \pmod{n}. \end{cases}$$