(Diskret matte D, ht13: F9, to 19 sep 2013)

## 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 $3 \mid x \Leftrightarrow 3 \mid \theta(x)$.

**Definition**: $r \in \mathbb{Z}_m$ är **inverterbart** om 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 $sgd(r, m) = 1$ (i $\mathbb{Z}$).

**Linjära kongruenser = linjära ekvationer i $\mathbb{Z}_m$**:

$ax \equiv b \pmod m \ \Leftrightarrow\ ax = b$ i $\mathbb{Z}_m \ \Leftrightarrow\ ax - km = b$ för något $k \in \mathbb{Z}$,
så ekvationen är lösbar omm $d = \text{sgd}(a, m) \mid b$.
Då finns $d$ olika lösningar $\pmod m$, dvs $d$ olika lösningar i $\mathbb{Z}_m$.

$ax \equiv ay \pmod m \ \Leftrightarrow\ x \equiv y \pmod m$ **om** $sgd(a, m) = 1$

$ax \equiv ay \pmod{an} \ \Leftrightarrow\ x \equiv y \pmod n$

$a \nmid y \ \Rightarrow ax \not\equiv y \pmod{an}$.