Sist
F4

Modulär aritmetik

$x \equiv y \pmod m$, $x \equiv_m y$ betyder $m \mid x-y$

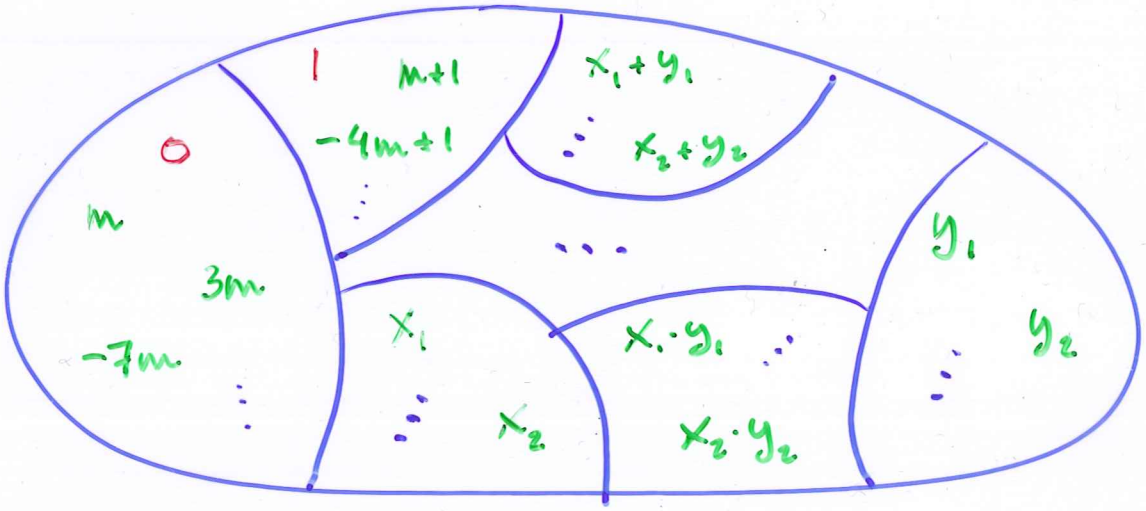
"x är kongruent med y modulo m"

dvs x och y ger samma principala rest vid division med m

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

$x_1 + y_1 \equiv_m x_2 + y_2$

$x_1 \cdot y_1 \equiv_m x_2 \cdot y_2$



$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

$7 \cdot 9 = 3 : \mathbb{Z}_{12} \Leftrightarrow 7 \cdot 9 \equiv 3 \pmod{12}$

"räkna som vanligt, behåll resten mod m"

Ex. $X = (x_n x_{n-1} \dots x_0)_{10}$ ger

$X \equiv_9 x_n + x_{n-1} + \dots + x_0 = \Theta(x)$ x:s siffersumma,

speciellt $9 \mid X \Leftrightarrow 9 \mid \Theta(x)$

p.s.s. $3 \mid X \Leftrightarrow 3 \mid \Theta(x)$

Definition: r i $\mathbb{Z}_m$ är inverterbart omm det finns x i $\mathbb{Z}_m$ med $rx = 1$ i $\mathbb{Z}_m$,

$x = r^{-1}$, r:s invers

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

Om p primtal, y i $\mathbb{Z}_p$ inverterbart omm $y \neq 0$

Om $1 = ar + bm$ är $r^{-1} = a$ i $\mathbb{Z}_m$

↑ fås med Euklides algoritm

Linjära kongruenser $(\mathrm{mod}\ m)$

$$ax \equiv b \pmod{m}$$

dvs linjära ekvationer i $\mathbb{Z}_m$

$$ax = b \quad \text{i } \mathbb{Z}_m$$

ekvivalent med

$$ax - mk = b$$

lösbar omm $d = \mathrm{sgd}(a, m) \mid b$

då allmänna lösningen

$$x = x_0 + k\frac{m}{d}, \quad k \text{ heltal}$$

så d olika lösningar i $\mathbb{Z}_m$

Om $\mathrm{sgd}(m, n) = 1$:

$$a \equiv b \pmod{mn} \Leftrightarrow \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$$