Sist
F14

Modulär aritmetik

$x \equiv y \pmod m$, $x \equiv_m y$

"x är kongruent med y modulo m"

betyder $m \mid x-y$

ex.

$6 \cdot 11 \equiv_{16} 2$, $9 + 13 \equiv_{17} 5$

ofta skrivet

$6 \cdot 11 = 2$ i $\mathbb{Z}_{16}$, $9 + 13 = 5$ i $\mathbb{Z}_{17}$

$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\} = \{[0]_m, [1]_m, \dots\}$

$+$, $\cdot$: "räkna i $\mathbb{Z}$, tag rest vid div m."

$x_1 \equiv_m y_1$, $x_2 \equiv_m y_2 \Rightarrow x_1 + x_2 \equiv_m y_1 + y_2$

$x \equiv \theta(x) \pmod 9$

$\theta(x)$: x:s siffersumma (bas 10)

spec.

$9 \mid x \iff 9 \mid \theta(x)$

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

x kallas r:s invers, r^{-1}

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

speciellt: alla utom 0 inverterbara i $\mathbb{Z}_p$, p primtal

$rx = 1$ i $\mathbb{Z}_m$ omm $rx - km = 1$,

så r^{-1} fås med Euklides algoritm

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

lika som linjära ekvationer i $\mathbb{Z}_m$

$ax \equiv b \ (\mathrm{mod}\ m)$, $ax = b$ i $\mathbb{Z}_m$

$\Updownarrow$

det finns ett heltal k så att

$$ax - km = b$$

en linjär diofantisk ekvation,

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

kan lösas med Euklides algoritm

har d olika lösningar $(\mathrm{mod}\ m)$

(spec. om a inverterbar i $\mathbb{Z}_m$,

entydig lösning $(\mathrm{mod}\ m)$)

Låt $m_1, \dots, m_k \in \mathbb{N}$, $\text{sgd}(m_i, m_j) = 1 \quad (i \neq j)$

$F: \mathbb{Z} \to \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$ med

$F(a) = ([a]_{m_1}, \dots, [a]_{m_k})$

uppfyller

$$F(a) = F(b) \Leftrightarrow a \equiv_m b, \quad m = m_1 \dots m_k$$

så

$f: \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$

$f([a]_m) = ([a]_{m_1}, \dots, [a]_{m_k})$

är en 1-1-funktion

$|\mathbb{Z}_m| = |\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}|$, så f är på

$f(a+b) = f(a) + f(b)$, $f(ab) = f(a) f(b)$

(komponentvis) (komponentvis)

dvs f är en isomorfi

$$f^{-1}([a_1]_{m_1}, \dots, [a_k]_{m_k}) = [y_1 a_1 + \dots + y_k a_k]_m$$

där $[y_i]_{m_j} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$

Kinesiska restsatsen

Om $m_1, \dots, m_k \in \mathbb{N}$, $\text{sgd}(m_i, m_j) = 1 \quad (i \neq j)$

har systemet

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \\ \vdots \\ x \equiv_{m_k} a_k \end{cases}$$

en lösning, unik mod $m = m_1 \cdot \dots \cdot m_k$,

för alla $a_1, \dots, a_k \in \mathbb{Z}$

$$x \equiv_m y_1 a_1 + \dots + y_k a_k$$

för vissa $y_1, \dots, y_k$, oberoende av $a_1, \dots, a_k$

$$y_i \equiv \begin{cases} 1 & (\text{mod } m_i) \\ 0 & (\text{mod } m_j) \quad j \neq i \end{cases}$$

Låt U_m vara mängden av inverterbara element i $\mathbb{Z}_m$

$$x, y \in U_m \Rightarrow xy,\ x^{-1} \in U_m$$

$$\phi(m) = |U_m| = |\{x \in \mathbb{Z} \mid 1 \le x \le m,\ \text{sgd}(x,m)=1\}|$$

Eulers ϕ-fkn

Sats (Euler): $y \in U_m \Rightarrow y^{\phi(m)} = 1$ i $\mathbb{Z}_m$

så $\text{sgd}(y,m) = 1 \Rightarrow y^{\phi(m)} \equiv_m 1$

Sats (Fermat): $y \in \mathbb{Z}_p, y \neq 0 \Rightarrow y^{p-1} = 1$ i $\mathbb{Z}_p$, p primtal

så $p \nmid y \Rightarrow y^{p-1} \equiv_p 1$

och $y^p \equiv_p y$, alla $y \in \mathbb{Z}$

Kvadratiska kongruenser

$$x^2 + cx + d \equiv_m 0$$

kvadratkomplettering (om m udda / c jämnt)

ger $(x+a)^2 \equiv_m b$

lösbar för vissa b, inte andra