kongruensräkning

(klockräkning
resträkning)

kl. 7 just nu
vad är klockan
om 50 timmar?

$50 \equiv 2 \pmod{12}$

modulo-
räkning

det är tisdag idag.
vilken dag är det
om 30 dagar?

7 veckodagar

0 = sön, 1 = mån, 2 = tis,
.... 6 = lör

$2 + 30$
$\equiv 2 + 2 \pmod 7$ → torsdag

kongruent
med

$16 + 35 \equiv 0 \pmod 3$
$1 + 2 \equiv 3 \equiv 0$

$16 \cdot 35 \equiv 2 \pmod 3$
$1 \cdot 2 \equiv 2$

$2^{303} \equiv 3 \pmod 5$

$2^4 = 16 \equiv 1$

$2^{303} = 2^{4 \cdot 75 + 3}$
$= (2^4)^{75} \cdot 2^3$
$\equiv 1^{75} \cdot 2^3 = 2^3 = 8 \equiv 3 \pmod 5$

om vi vet $a_1 \equiv a_2 \pmod{m}$

då vet vi

- $a_1 + b \equiv a_2 + b \pmod{m}$
- $a_1 \cdot b \equiv a_2 \cdot b \pmod{m}$

då vet vi INTE

- ~~$b^{a_1} \equiv b^{a_2} \pmod{m}$~~ $\quad 2^1 \not\equiv 2^4 \pmod{3}$, $2 \not\equiv 16 \pmod{3}$
- ~~$a_1/b \equiv a_2/b \pmod{m}$~~ $\quad 2 \cdot 3 \equiv 2 \cdot 5 \pmod{4}$, $3 \not\equiv 5 \pmod{4}$

def. $a_1 \equiv a_2 \pmod m$

- a_1 och a_2 har samma rest vid delning med m
- $m \mid a_1 - a_2$

<u>om</u> $a_1 \equiv a_2 \pmod m$, <u>då</u> $m \mid a_1 - a_2$

$(a_1 + b) - (a_2 + b) = a_1 - a_2$

↑ m delar ↑ m delar

m delar

$a_1 \cdot b - a_2 \cdot b =$

$(a_1 - a_2) \cdot b$

↑ m delar

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

$x \in \mathbb{Z}$

↖ det finns oändligt många lösningar när $\gcd(m_1, m_2) = 1$

↘ Pulverizer!

↓

hitta u, v

$$x = b \cdot\cdot u \cdot m_1 + a \cdot\cdot v \cdot m_2$$

$$\equiv b \pmod{m_2} \qquad \equiv a \pmod{m_1}$$

$m_1 \cdot u + m_2 \cdot v = 1$

↓

$m_1 \cdot u \equiv 1 \pmod{m_2}$

$m_2 \cdot v \equiv 1 \pmod{m_1}$

en första lösning:

$$\boxed{x = b \cdot u \cdot m_1 + a \cdot v \cdot m_2}$$

$$\equiv a \cdot v \cdot m_2$$

$$\equiv a \pmod{m_1}$$

$$\equiv b \cdot u \cdot m_1$$

$$\equiv b \pmod{m_2}$$

alla lösningar:

$$\boxed{x_k \equiv x \pmod{m_1 \cdot m_2}}$$

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

pulverizer : hitta u, v

$3 \cdot u + 5 \cdot v = 1$

$u = 2, \; v = -1$

$x = 3 \cdot 3 \cdot u + 2 \cdot 5 \cdot v$

$= 18 + -10$

$= 8$

$8 + 3 \cdot 5 = 23$

$23 + 3 \cdot 5 = 48$

alla lösningar:

$x_k = 8 + k \cdot 3 \cdot 5 \quad (k \in \mathbb{Z})$

$x \equiv 8 \pmod{15}$

oändligt många lösningar

$x \in \mathbb{Z}$

"Det finns saker vars antal är okänt. "kvoten" "resten"

$x \equiv 2 \pmod 3$ Om vi räknar i 3:or, har vi 2 kvar. $23 = 7 \cdot 3 + 2$

$x \equiv 3 \pmod 5$ Om vi räknar i 5:or, har vi 3 kvar. $23 = 4 \cdot 5 + 3$

$x \equiv 2 \pmod 7$ Om vi räknar i 7:or, har vi 2 kvar. $23 = 3 \cdot 7 + 2$

Hur många saker finns det?" — (23)

oändligt många lösningar

- Sunzi i "Sunzi Suanjing"

~300 e.kr.

$$\begin{cases} X \equiv 2 \pmod 3 \\ X \equiv 3 \pmod 5 \\ X \equiv 2 \pmod 7 \end{cases} \quad \Big\} \quad \cdots\cdots \rightarrow \quad \begin{cases} X \equiv 8 \pmod{15} \\ X \equiv 2 \pmod 7 \end{cases}$$

pulverizer hitta u, v

$15 \cdot u + 7 \cdot v = 1$

$u = 1 \,,\; v = -2$

$X \equiv 23 \pmod{105}$

$X = 2 \cdot 15 \cdot u + 8 \cdot 7 \cdot v$

$= 30 - 112$

$= -82$

"kinesiska restsatsen"

$X \equiv -82 \pmod{7 \cdot 15}$

$X \equiv -82 \pmod{105}$

$X \equiv 23 \pmod{105}$

$(23 \equiv -82 + 105)$

$23, \; 128, \; 233, \; \cdots$

$+105 \quad +105$

$a \equiv b \pmod m$ $\equiv$ är en relation

ett predikat med 2 argument av samma typ

relationer R över A

reflexiv : $\forall x : A \,.\, R(x,x)$

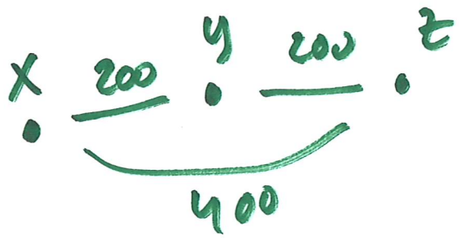
symmetrisk : $\forall x,y : A \,.\, (R(x,y) \Rightarrow R(y,x))$

transitiv : $\forall x,y,z : A \,.\, (R(x,y) \wedge R(y,z) \Rightarrow R(x,z))$

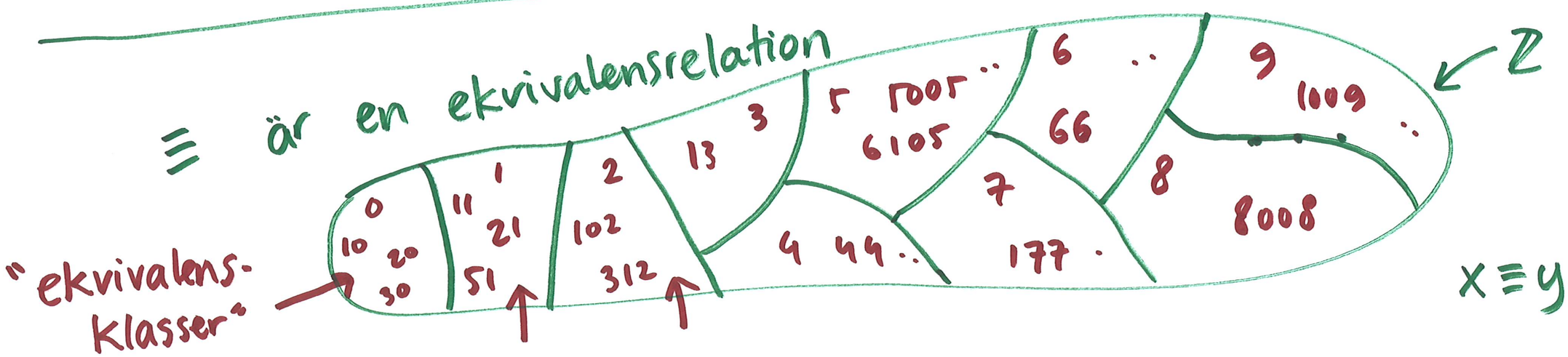
ekvivalens = alla 3 samtidigt

(exempel : $\equiv$ är en ekvivalens)

	$x \equiv y$	$x \leq y$	syskon	bor ihop	bor $\leq$ 200m ifrån
reflexiv $R(x,x)$	ja	ja	nej	ja	ja
symmetrisk $R(x,y) \Rightarrow R(y,x)$	ja	nej	ja	ja	ja
transitiv $R(x,y) \wedge R(y,z) \Rightarrow R(x,z)$	ja	ja	ja (helsyskon)	ja	nej
ekvivalens	ja!	nej!	nej	ja	nej



$\equiv$ är en ekvivalensrelation



$m = 10$

$x \equiv y \pmod{m}$