Relationer

- Relation mellan objekt $\Rightarrow$ egenskap som de besitter tillsammans
- Fyra viktiga egenskaper:
  - Reflexivitet
  - Symmetri
  - Anti-symmetri
  - Transitivitet

Reflexivitet

- Relation R på mängd A
- R reflexiv om:

  för alla $x \in A$, $(x, x) \in R$ dvs $\underline{xRx}$

Symmetri

- Relation R på mänd A
- R symmetrisk om:

  för alla $(x, y) \in A$, $(x,y) \in R \Rightarrow (y, x) \in R$ dvs $\underline{xRy \Rightarrow yRx}$

Anti-symmetri

- Relation R på mängd A
- R anti-symmetrisk om:

  för alla $(x, y) \in A$, $(x,y) \in R$ och $(y,x) \in R \Rightarrow x = y$

  dvs $\underline{xRy \text{ och } yRx \Rightarrow x = y}$
- OBS! Anti-symm $\neq$ icke symm

Transitivitet

- Relation R på mängd A
- R transitiv om:

  för alla $(x, y, z) \in A$, $(x,y) \in R$ och $(y,z) \in R \Rightarrow (x,z) \in R$

  dvs $\underline{xRy \text{ och } yRz \Rightarrow xRz}$.

Två typer av relationer

- Ekvivalensrelation om R: reflexiv, symmetrisk, transitiv
- Partialordning om R: reflexiv, anti-symmetrisk, transitiv

Ex 2017-05-30 uppgift 7

Låt mängden $A = \{(a,b) \mid a \in \mathbb{N}, b \in \mathbb{Z}\}$

Definiera relation R på A genom $(a,b) R (c,d)$ om det finns något x_0 så att, för alla $x \geq x_0$ $ax+b \leq cx+d$. Visa att R är en partialordning.

Lösning

Partialordning $\Rightarrow$ reflexiv, anti-symmetrisk, transitiv.

Reflexiv?

- För alla $(a,b) \in A$ så ska $(a,b) R (a,b)$.
- Ska finnas något tal x_0, så att för $x \geq x_0$

  $ax+b \leq \underline{ax+b}$ motsv. $cx+d$ i relationen $(a,b) R (c,d)$
- Välj ex. $x_0 = 0$. För alla $x \geq 0$ så gäller $ax+b \leq ax+b$. OK!

Anti-symmetrisk?

- För alla $(a,b) \in A$ och $(c,d) \in A$ så ska $(a,b) R (c,d)$ och $(c,d) R (a,b) \Rightarrow$ $(a,b) = (c,d)$.
- $(a,b) R (c,d) \Rightarrow$ finns något x_1 så att för $x \geq x_1$: $ax+b \leq cx+d$ (1)

  $(c,d) R (a,b) \Rightarrow$ finns något x_2 så att för $x \geq x_2$: $cx+d \leq ax+b$ (2)
- Vi antar $x_1 > x_2$, och väljer $x \geq x_1$, då får vi:

  $ax+b \leq cx+d$, ty $x \geq x_1$ från (1)

  $cx+d \leq ax+b$, ty $x \geq x_1 \geq x_2$ från (2)
- Men $ax+b \leq cx+d \leq ax+b \Rightarrow ax+b = cx+d \Rightarrow (a,b) = (c,d)$ OK!
- På samma sätt för $x_2 > x_1$.

Transitiv?

- För alla $(a,b) \in A$, $(c,d) \in A$, $(e,f) \in A$ så ska $(a,b) R (c,d)$ och $(c,d) R (e,f) \Rightarrow$ $(a,b) R (e,f)$.
- $(a,b) R (c,d) \Rightarrow$ finns något x_1 så att för $x \geq x_1$: $ax+b \leq cx+d$ (3)

  $(c,d) R (e,f) \Rightarrow$ finns något x_2 så att för $x \geq x_2$: $cx+d \leq ex+f$ (4)
- Vi antar $x_1 > x_2$ och väljer $x = x_1$. Då får vi: (Analogt för $x_2 > x_1$)

  $ax+b \leq cx+d$, ty $x \geq x_1$ från (3)

  $cx+d \leq ex+f$, ty $x \geq x_1 \geq x_2$ från (4)
- Men $ax+b \leq cx+d \leq ex+f \Rightarrow ax+b \leq ex+f \Rightarrow (a,b) R (e,f)$ OK

Svar: R är reflexiv, anti-symmetrisk, transitiv $\Rightarrow R$ är partialordning

Ex 2017-08-17 uppgift 6

Vi har meddelandet ESTETISK på alfabetet $\{E, S, T, I, K\}$.

Vi har prefixkoder $P = \{P(E), P(S), P(T), P(I), P(K)\}$ där varje $P(i)$ är

- en binär följd med någon längd ex: $P(E) = 00$, $P(S) = 01$
- inget $P(i)$ är början på något annat $P(i)$ ex: $P(E) = 00 \Rightarrow P(S) \neq \underbrace{00}_{P(E)}1$

Kostnaden $c(P)$ är totallängden av $P(E)P(S)P(T) \ldots P(ESTETISK)$

ex: $\underbrace{00}_{P(E)}\ \underbrace{01}_{P(S)}\ \underbrace{10}_{P(T)}\ \underbrace{00}_{P(E)}$ längd 8, så $c(P) = 8$

Definiera relation R som att $P \mathcal{R} P'$ om $\underbrace{c(P) = c(P')}_{\text{meddelanden har samma längd}}$

Visa att R är en ekvivalensrelation

Lösning

Ekvivalensrelation $\Rightarrow$ reflexiv, symmetrisk, transitiv

Reflexiv

Är $P \mathcal{R} P$? $\underbrace{c(P) = c(P)}_{P \mathcal{R} P}$, så ja!

Symmetrisk

$P \mathcal{R} P' \Rightarrow P' \mathcal{R} P$? $c(P) = c(P') \Rightarrow \underbrace{c(P') = c(P)}_{P' \mathcal{R} P}$, så ja!

Transitiv

$P \mathcal{R} P'$ och $P' \mathcal{R} P'' \Rightarrow P \mathcal{R} P''$? $\begin{cases} c(P) = c(P') \\ c(P') = c(P'') \end{cases} \Rightarrow \underbrace{c(P) = c(P'')}_{P \mathcal{R} P''}$

så ja!

$\therefore$ $\mathcal{R}$ är en ekvivalensrelation.

E	S	T	E	T	I	S	K
↓	↓	↓	↓	↓	↓	↓	↓
P(E)	P(S)	P(T)	P(E)	P(T)	P(I)	P(S)	P(K)
↓	↓	↓	↓	↓	↓	↓	↓
00	01	10	00	10	110	01	111

2017-08-17 uppgift 7

Anti-symmetrisk?

- $P \mathcal{R} P'$ och $P' \mathcal{R} P \Rightarrow P = P'$?
- Låt $P = \{P(E) = 00, P(S) = 01, \ldots \text{(som ovan)}\}$
  $P' = \{P(E) = 01, P(S) = 00, \ldots \text{(som ovan)}\}$
- $c(P)$ = totallängd av $P(ESTETISK)$ = totallängd av $P'(ESTETISK) = c(P')$
  $c(P') = c(P)$ på samma sätt.
  Men $P \neq P'$ ty $P(E) \neq P'(E)$. Dvs $\not\Rightarrow P = P' \Rightarrow$ ej anti-symm

Modulo-räkning

- $a \equiv b \mod m \iff ax \equiv bx \mod m$, x heltal
- $a \equiv b \mod m \iff (a \bmod m) \equiv b \mod m$

speciellt gäller: $a^n \equiv b \mod m \iff (a \bmod m)^n \equiv b \mod m$

- $a \equiv b \mod m \iff a^n \equiv b^n \mod m$ (modulo bevaras vid exponentiation)

Ex 2017-10-28 uppgift 6

Visa att $(1^2)^n + (3^2)^n + (5^2)^n + (7^2)^n + (9^2)^n + (11^2)^n + (13^2)^n + (15^2)^n \equiv 0 \mod 8$

Lösn

- Reducera alla termer mod 8!

$1^2 \equiv 1 \Rightarrow (1^2)^n \equiv 1^n \mod 8$ $\qquad 7^2 \equiv 49 \equiv 1 \mod 8 \Rightarrow (7^2)^n \equiv 1^n \mod 8$

$3^2 \equiv 9 \equiv 1 \Rightarrow (3^2)^n \equiv 1^n \mod 8$

$5^2 \equiv 25 \equiv 1 \Rightarrow (5^2)^n \equiv 1^n \mod 8$

- $(1^2)^n + (3^2)^n + (5^2)^n + (7^2)^n + (9^2)^n + (11^2)^n + (13^2)^n + (15^2)^n \equiv 0 \mod 8$

$\iff 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \equiv 8 \equiv 0 \mod 8$ v.s.v.

Ex 2015-08-20 uppgift 6

Hitta det minsta positiva heltalet x som uppfyller:

$x^2 + x \equiv 1 \mod 5$

$x^2 + x \equiv 5 \mod 7$

$x^2 + x \equiv 3 \mod 13$

Lösn

- $x^2 + x \equiv 1 \mod 5 \Rightarrow$ behöver testa $0, 1, 2, 3, 4$ ty $5 \equiv 0 \mod 5$, $6 \equiv 1 \mod 5$, $7 \equiv 2 \mod 5$
- Testar $0^2 + 0 \equiv 0 \not\equiv 1 \mod 5$

$1^2 + 1 \equiv 2 \not\equiv 1 \mod 5$

$2^2 + 2 \equiv 6 \equiv 1 \mod 5 \Rightarrow x \equiv 2 \mod 5$

- Testar $x^2 + x \equiv 5 \mod 7$

$0^2 + 0 \equiv 0 \not\equiv 5 \mod 7$

$1^2 + 1 \equiv 2 \not\equiv 5 \mod 7$

$2^2 + 2 \equiv 6 \not\equiv 5 \mod 7$

$3^2 + 3 \equiv 12 \equiv 5 \mod 7 \Rightarrow x \equiv 3 \mod 7$

- Testar $x^2 + x \equiv 3 \mod 13$

$0^2 + 0 \equiv 0 \not\equiv 3 \mod 13$

$\vdots$

$6^2 + 6 \equiv 36 \equiv 3 \mod 13 \Rightarrow x \equiv 6 \mod 13$

$\left.\right\}$ $x \equiv 2 \mod 5$, $x \equiv 3 \mod 7$, $x \equiv 6 \mod 13$

Använd KRS

Kinesiska restsatsen (KRS)

Givet system av kongruenser:

$$x \equiv b_1 \mod n_1$$
$$x \equiv b_2 \mod n_2$$
$$\vdots$$
$$x \equiv b_k \mod n_k$$

och $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

samt $N_i = \frac{N}{n_i}$, $i = 1, 2, \ldots, k$ $N_i = N$ delat på motsv. lilla n_i

samt x_i lösning till $N_i x_i \equiv 1 \mod n_i$, $i = 1, 2, \ldots, k$ (x_i kallas multiplikativ invers)

då är $x = b_1 N_1 x_1 + b_2 N_2 x_2 + \ldots + b_k N_k x_k$ en lösning till systemet.

entydigt bestämd modulo N $\Rightarrow x \equiv x' \mod N$

Ex: 2016-08-18 uppgift 5

Bestäm $73^{1567} \mod 990$

Lösn:

Idé: För stort att beräkna direkt. Använd KRS.

Låt $N = 990$

- N består av $n_1 \cdot n_2 \cdot \ldots \cdot n_k \Rightarrow$ faktorisera N.

$$N = 9 \cdot 110 = \underbrace{9}_{n_1} \cdot \underbrace{5}_{n_2} \cdot \underbrace{2}_{n_3} \cdot \underbrace{11}_{n_4}$$

$$\Rightarrow \begin{cases} n_1 = 9 \\ n_2 = 5 \\ n_3 = 2 \\ n_4 = 11 \end{cases} \Rightarrow \begin{cases} N_1 = N/n_1 = 990/9 = 110 \\ N_2 = N/n_2 = 990/5 = 198 \\ N_3 = N/n_3 = 990/2 = 495 \\ N_4 = N/n_4 = 990/11 = 90 \end{cases}$$

- Saknar $b_1, b_2, b_3, b_4 \Rightarrow$ beräkna dessa:

Låt $x = 73^{1567}$

$$x \equiv \underbrace{b_1 \mod n_1}_{= b_1 \mod 9} \Rightarrow x \equiv b_1 \mod 9$$

$$x \equiv \underbrace{b_2 \mod n_2}_{= b_2 \mod 5} \Rightarrow x \equiv b_2 \mod 5$$

$$x \equiv \underbrace{b_3 \mod n_3}_{= b_3 \mod 2} \Rightarrow x \equiv b_3 \mod 2$$

$$x \equiv \underbrace{b_4 \mod n_4}_{= b_4 \mod 11} \Rightarrow x \equiv b_4 \mod 11$$

Beräkna kongruenser

b_1: $73^{1567} \equiv b_1 \mod 9$

$73^{1567} \equiv (73 \mod 9)^{1567} \equiv 1^{1567} \equiv 1 \mod 9 \quad \Rightarrow b_1 = 1$

$a \equiv b \mod m \iff (a \mod m) \equiv b \mod m$

b_2: $73^{1567} \equiv b_2 \mod 5$

$73^{1567} \equiv (73 \mod 5)^{1567} \equiv 3^{1567} \mod 5$

Idé: Upprepad exponentiering: Leta efter $\pm 1 \mod 5$ "Ersätt basen"

$3^1 \equiv 3 \mod 5$

$3^2 \equiv 9 \equiv -1 \mod 5$

$3^{1567} \equiv (3^2)^{783} \cdot 3 \equiv (-1)^{783} \cdot 3 \equiv (-1) \cdot 3 \equiv -3 \equiv 2 \mod 5$

$\Rightarrow b_2 = 2$

b_3: $73^{1567} \equiv b_3 \mod 2$

$73^{1567} \equiv (73 \mod 2)^{1567} \equiv 1^{1567} \equiv 1 \mod 2 \Rightarrow b_3 = 1$

b_4: $73^{1567} \equiv b_4 \mod 11$

$73^{1567} \equiv (73 \mod 11)^{1567} \equiv 7^{1567} \mod 11$

Upprepad exponentiering:

$7^1 \equiv 7 \mod 11$

$7^2 \equiv 7^1 \cdot 7 \equiv 49 \equiv 5 \mod 11$

$7^3 \equiv 7^2 \cdot 7 \equiv 5 \cdot 7 \equiv 35 \equiv 2 \mod 11$

$7^4 \equiv 7^3 \cdot 7 \equiv 2 \cdot 7 \equiv 14 \equiv 3 \mod 11$

$7^5 \equiv 7^4 \cdot 7 \equiv 3 \cdot 7 \equiv 21 \equiv -1 \mod 11$

$7^{1567} \equiv (7^5)^{313} \cdot 7^2 \equiv (-1)^{313} \cdot 7^2 \equiv -1 \cdot 7^2 \equiv -49 \equiv 6 \mod 11$

$\Rightarrow b_4 = 6$

Vi vet:

$x \equiv 1 \mod 9$, $N_1 = 110$

$x \equiv 2 \mod 5$, $N_2 = 198$

$x \equiv 1 \mod 2$, $N_3 = 495$

$x \equiv 6 \mod 11$, $N_4 = 90$

Söker x_i från
$$\begin{cases} N_1 x_1 \equiv 1 \mod n_1 \\ N_2 x_2 \equiv 1 \mod n_2 \\ N_3 x_3 \equiv 1 \mod n_3 \\ N_4 x_4 \equiv 1 \mod n_4 \end{cases}$$

Beräkna multiplikativa inverser x_i

x_1: $\begin{cases} N_1 = 110 \\ n_1 = 9 \end{cases} \Rightarrow 110 x_1 \equiv 1 \mod 9$

Reducera basen $\Rightarrow 110 x_1 \equiv (110 \mod 9) x_1 \equiv \underbrace{2 x_1 \equiv 1 \mod 9}$

"Skala upp" $\Rightarrow 2x_1 \equiv 1 \mod 9 \Leftrightarrow$

Antingen Euklides algoritm eller skala upp och reducera modulo 9.

Vill göra $2x_1$ till $\underset{\sim}{a \cdot x_1}$ där $a \equiv \pm 1 \mod 9$

$\Leftrightarrow 4 \cdot 2x_1 \equiv 4 \cdot 1 \mod 9$

$\Leftrightarrow 8 x_1 \equiv 4 \mod 9$

$\Leftrightarrow$ / $8 \equiv -1 \mod 9$ /

$\Leftrightarrow (-1) x_1 \equiv 4 \mod 9$

$\Leftrightarrow x_1 \equiv -4 \equiv 5 \mod 9$ //

x_2: $\begin{cases} N_2 = 198 \\ n_2 = 5 \end{cases} \Rightarrow 198 x_2 \equiv 1 \mod 5$

Reducera basen $\Rightarrow 198 x_2 \equiv (198 \mod 5) x_2 \equiv 3 x_2 \equiv 1 \mod 5$

Skala upp $\Rightarrow 3x_2 \equiv 1 \mod 5$

$\Leftrightarrow 2 \cdot 3 x_2 \equiv 2 \cdot 1 \mod 5$

$\Leftrightarrow 6 x_2 \equiv 2 \mod 5$

$\Leftrightarrow$ / $6 \equiv 1 \mod 5$ /

$\Leftrightarrow x_2 \equiv 2 \mod 5$ //

x_3: $\begin{cases} N_3 = 495 \\ n_3 = 2 \end{cases} \Rightarrow 495 x_3 \equiv 1 \mod 2$

Reducera basen $\Rightarrow 495 x_3 \equiv (495 \mod 2) x_3 \equiv 1 \cdot x_3 \equiv 1 \mod 2$

$\Leftrightarrow x_3 \equiv 1 \mod 2$ //

x_4: $\begin{cases} N_4 = 90 \\ n_4 = 11 \end{cases} \Rightarrow 90 x_4 \equiv 1 \mod 11$

Reducera basen $\Rightarrow 90 x_4 \equiv (90 \mod 11) x_4 \equiv 2 \cdot x_4 \equiv 1 \mod 11$

Skala upp $\Rightarrow 2x_4 \equiv 1 \mod 11$

$\Leftrightarrow 6 \cdot 2 x_4 \equiv 6 \cdot 1 \mod 11$

$\Leftrightarrow 12 x_4 \equiv 6 \mod 11$

$\Leftrightarrow$ / $12 \equiv 1 \mod 11$ /

$\Leftrightarrow x_4 \equiv 6 \mod 11$ //

Vi vet:

$$\left.\begin{array}{lll} x_1 = 5 & b_1 = 1 & N_1 = 110 \\ x_2 = 2 & b_2 = 2 & N_2 = 198 \\ x_3 = 1 & b_3 = 1 & N_3 = 495 \\ x_4 = 6 & b_4 = 6 & N_4 = 90 \end{array}\right\}$$

Svar: $73^{1567} \equiv \underbrace{b_2 N_2 x_2}$

$\equiv 1 \cdot 110 \cdot 5 + 2 \cdot 198 \cdot 2$

$+ 1 \cdot 495 \cdot 1 + 6 \cdot 90 \cdot 6$

$\equiv 5077 \equiv 127 \mod 990$