Diskretne strukture UNI
Vaje 9

1. Na množici naravnih števil $\mathbb{N}$ definiramo relacijo R:

$$xRy \quad \Leftrightarrow \quad 5 \text{ deli } x + 4y.$$

Pokaži, da je R ekvivalenčna relacija in določi ekvivalenčne razrede.

- R refleksivna? $\forall x : xRx$?
  $\forall x :$ 5 deli $x + 4x$?
  $\forall x :$ 5 deli $5x$? Ja, 5 vedno deli $5x$.

- R simetrična? $\forall x \forall y : (xRy \Rightarrow yRx)$?
  $\forall x \forall y :$ (5 deli $x+4y \Rightarrow$ 5 deli $y+4x$) ? Ja. Če 5 deli $x+4y$, potem deli tudi
  $5(x+y) - (x+4y) = 5x+5y-x-4y = y+4x$. ∎

- R tranzitivna? $\forall x \forall y \forall z : (xRy \wedge yRz \Rightarrow xRz)$?
  $\forall x \forall y \forall z :$ (5 deli $x+4y$ in 5 deli $y+4z \Rightarrow$ 5 deli $x+4z$) ? Ja, če 5 deli $x+4y$ in $y+4z$, potem deli tudi vsoto
  $(x+4y)+(y+4z) = x+4z+5y$.
  Potem pa deli tudi
  $(x+4y)+(y+4z)-5y = x+4z$,
  ker deli vse člene na levi.

$\Rightarrow$ Ker je R refleksivna, simetrična in tranzitivna, je ekvivalenčna.

Ekvivalenčni razredi?

$$\boxed{\begin{aligned}[x] &= \{a \in A ; aRx\} \\ &= \{a \in A ; xRa\}\end{aligned}}$$

$[x] = \{m \in \mathbb{N} ; mRx\} = \{m \in \mathbb{N} ; 5 \text{ deli } m+4x\}$ ⟶ Lepši? Uporabimo tega.
$\quad = \{m \in \mathbb{N} ; xRm\} = \{m \in \mathbb{N} ; 5 \text{ deli } x+4m\}$

$[0] = \{m ; 5 \text{ deli } 0+4m\} = \{0, 5, 10, 15, \dots\}$
$[1] = \{m ; 5 \text{ deli } 1+4m\} = \{1, 6, 11, 16, \dots\}$
$\vdots$

Isti rezultat.

$[0] = \{m ; 5 \text{ deli } m\} = \{0, 5, 10, 15, 20, \dots\}$
$[1] = \{m ; 5 \text{ deli } m+4\} = \{1, 6, 11, 16, 21, \dots\}$
$[2] = \{m ; 5 \text{ deli } m+8\} = \{2, 7, 12, 17, \dots\}$
$[3] = \{m ; 5 \text{ deli } m+12\} = \{3, 8, 13, 18, \dots\}$
$[4] = \{m ; 5 \text{ deli } m+16\} = \{4, 9, 14, 19, \dots\}$

Vsako naravno število je v eni od teh množic.

$\mathbb{N} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$

2. Na množici $A = \{0, 1, 2, \ldots, 11\}$ definiramo relacijo

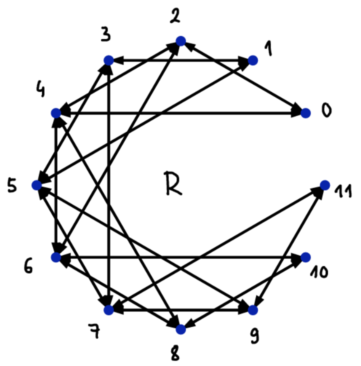
$$xRy \quad \Leftrightarrow \quad |x - y| \in \{2, 4\}$$

(a) Nariši grafe relacije R, R^2 in R^+

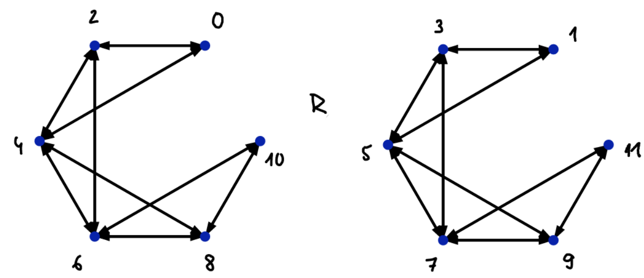
(b) Katere izmed relacij so refleksivne, simetrične, tranzitivne?

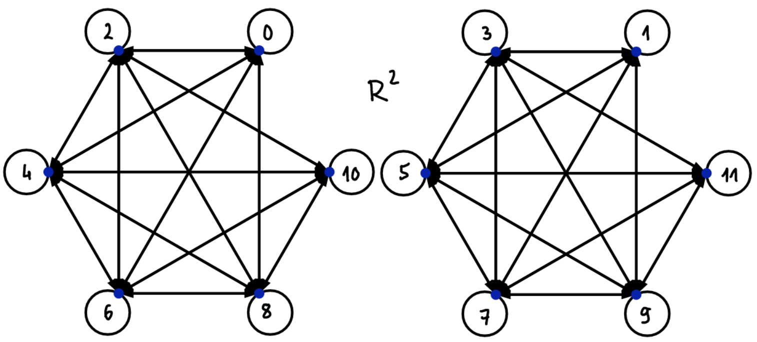
(c) Določi ekvivalenčne razrede tistih od relacij R, R^2 in R^+, ki so ekvivalenčne.

(a) Nariši grafe relacije R, R^2 in R^+



Ker lahko gremo le 2 ali 4 mesta naprej ali nazaj, $\rightsquigarrow$ ne moremo priti iz sodih števil v liha ali obratno.





$i \downarrow$ \ $j \leftarrow$	0	2	4	6	8	10	1	3	5	7	9	11
0	1	1	1	1	1	0	0	0	0	0	0	0
2	1	1	1	1	1	1	0	0	0	0	0	0
4	1	1	1	1	1	1	0	0	0	0	0	0
6	1	1	1	1	1	1	0	0	0	0	0	0
8	1	1	1	1	1	1	0	0	0	0	0	0
10	0	1	1	1	1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	1	1	1	1	1	0
3	0	0	0	0	0	0	1	1	1	1	1	1
5	0	0	0	0	0	0	1	1	1	1	1	1
7	0	0	0	0	0	0	1	1	1	1	1	1
9	0	0	0	0	0	0	1	1	1	1	1	1
11	0	0	0	0	0	0	0	1	1	1	1	1

1 na križišču i-te vrstice in j-tega stolpca pomeni, da lahko v dveh korakih pridemo od i do j;

0 pomeni, da ni povezave od i do j

$R^+ = R \cup R^2 \cup R^3 \cup R^4 \cup \cdots$ = tranzitivna ovojnica relacije R

= najmanjša tranzitivna relacija, ki vsebuje R

$R^+ \rightsquigarrow$ poljubno število korakov v grafu za R

$a \xrightarrow{+2} a+2 \xrightarrow{-2} a$ ali $a \xrightarrow{-2} a-2 \xrightarrow{+2} a$ $\rightsquigarrow$ zanke

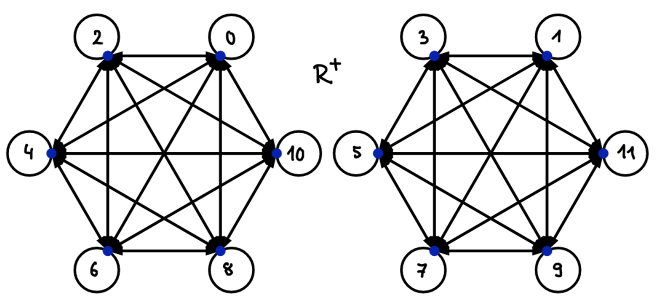
$a \xrightarrow{+4} a+4 \xrightarrow{-2} a+2$ ali $a \xrightarrow{-4} a-4 \xrightarrow{+2} a-2$ ali

$a \longrightarrow a-2 \longrightarrow a+4$ ali $a \longrightarrow a+2 \longrightarrow a-4$ ali ... $\rightsquigarrow$ 2 naprej/nazaj

$a \xrightarrow{+2} a+2 \xrightarrow{+2} a+4$ ali $a \xrightarrow{-2} a-2 \xrightarrow{-2} a-4$ $\rightsquigarrow$ 4 naprej/nazaj

$a \xrightarrow{+2} a+2 \xrightarrow{+4} a+6$ ali $a \xrightarrow{-2} a-2 \xrightarrow{-4} a-4$ ali ... $\rightsquigarrow$ 6 naprej/nazaj

$a \longrightarrow a+4 \longrightarrow a+8$ ali $a \longrightarrow a-4 \longrightarrow a-8$ $\rightsquigarrow$ 8 naprej/nazaj



(b) Katere izmed relacij so refleksivne, simetrične, tranzitivne?

Ker je $|x-y| = |y-x|$, je R simetrična. Ker je R simetrična, sta tudi R^2 in R^+ simetrični. Ker je R simetrična, je R^2 refleksivna. Ker je R^2 refleksivna, je tudi R^+ refleksivna. R^+ je tranzitivna, ker je tranzitivna ovojnica.

R ni refleksivna, ker $\neg 1R1$. R ni tranzitivna, ker je $0R4$ in $4R8$ in $\neg 0R8$. R^2 ni tranzitivna, ker je $0R^28$ in $8R^210$ in $\neg 0R^210$.

(c) Določi ekvivalenčne razrede tistih od relacij R, R^2 in R^+, ki so ekvivalenčne.

Ekvivalenčna je R^+, ker je refleksivna, simetrična in tranzitivna. $[0] = \{0,2,4,6,8,10\}$, $[1] = \{1,3,5,7,9,11\}$.

3. Naj bo B_n množica naravnih števil od 0 do $2^n - 1$. Ta števila predstavimo v dvojiškem zapisu; število $b \in B_n$ zapišemo kot $b = \mathsf{b}_n \cdots \mathsf{b}_2\mathsf{b}_1$, kjer so števke b_i enake 0 ali 1. Na B_n definiramo relacijo $\preceq$ z

$$a \preceq b \quad \Leftrightarrow \quad \forall i\, (\mathsf{a}_i \leq \mathsf{b}_i).$$

(a) Ali velja: $2 \preceq 3$, $5 \preceq 8$, $4 \preceq 5$?

(b) Prepričaj se, da je $\preceq$ relacija delne urejenosti.

(c) Skiciraj Hassejev diagram te delne urejenosti v primeru $n = 3$.

(d) Ali je $\preceq$ relacija linearne urejenosti? Za kateri n oziroma zakaj ne? Kako to sledi iz Hassejevega diagrama?

(e) Preveri, da velja implikacija: Če $a \preceq b$, potem $a \leq b$.

(a) Ali velja: $2 \preceq 3$, $5 \preceq 8$, $4 \preceq 5$?

$B_1 = \{0_2, 1_2\}$ $\quad B_2 = \{00_2, 01_2, 10_2, 11_2\}$ $\quad B_3 = \{\overset{0}{000_2}, \overset{1}{001_2}, \overset{2}{010_2}, \overset{3}{011_2}, \overset{4}{100_2}, \overset{5}{101_2}, \overset{6}{110_2}, \overset{7}{111_2}\}$ $\quad \dots$

$2 = 10_2$, $3 = 11_2$, $5 = 101_2$, $8 = 1000_2$, $4 = 100_2$

$2 \preceq 3$?
$10_2 \preceq 11_2$?
$1 \leq 1$ in $0 \leq 1$ ✓
$2 \preceq 3$

$5 \preceq 8$?
$0101_2 \preceq 1000_2$?
$0 \leq 1$ in $1 \leq 0$ in $0 \leq 1$ in $1 \leq 0$ //
$\neg\, 5 \preceq 8$

$4 \preceq 5$?
$100_2 \preceq 101_2$?
$1 \leq 1$ in $0 \leq 0$ in $1 \leq 1$ ✓
$4 \preceq 5$

(b) Prepričaj se, da je $\preceq$ relacija delne urejenosti.

- $\preceq$ refleksivna ?

$\forall a: a \preceq a$?

$\forall a\, (\forall i: \underbrace{a_i \leq a_i}_{1})$?

$\forall a\, \forall i: 1$ ✓

je refleksivna

- $\preceq$ antisimetrična ?

$\forall a \forall b\, (a \preceq b \wedge b \preceq a \Rightarrow a = b)$?

$\forall a \forall b\, (\forall i: a_i \leq b_i \wedge \forall j: b_j \leq a_j \Rightarrow a = b)$?

$\forall a \forall b\, (\forall i: a_i \leq b_i \wedge \forall i: b_i \leq a_i \Rightarrow a = b)$?

$\forall a \forall b\, (\forall i\, (a_i \leq b_i \wedge b_i \leq a_i) \Rightarrow a = b)$?

$\forall a \forall b\, (\forall i\, (a_i = b_i) \Rightarrow a = b)$ ✓

vse števke so enake $\Rightarrow$ števili sta enaki

je antisimetrična

- $\preceq$ tranzitivna ?

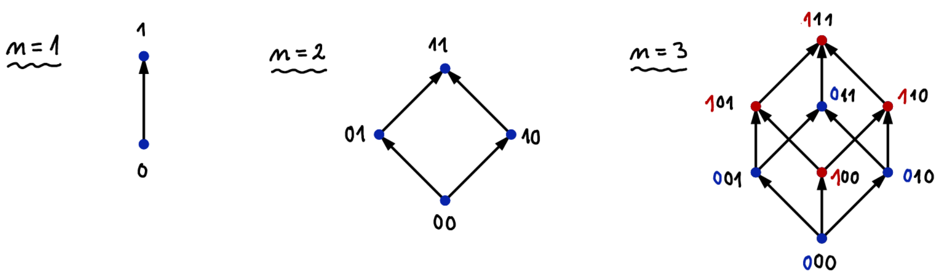
$\forall a \forall b \forall c\, (a \preceq b \wedge b \preceq c \Rightarrow a \preceq c)$?

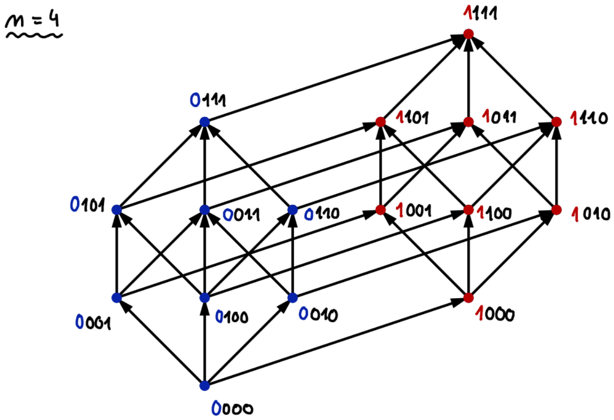
$\forall a \forall b \forall c\, (\forall i: a_i \leq b_i \wedge \forall i: b_i \leq c_i \Rightarrow \forall i: a_i \leq c_i)$?

Naj bodo $a, b, c \in B_n$ poljubni in naj velja $\forall i: a_i \leq b_i \wedge \forall i: b_i \leq c_i \sim 1$. Potem je $\forall i\, (a_i \leq b_i \wedge b_i \leq c_i) \sim 1$. Iz $(a_i \leq b_i \wedge b_i \leq c_i)$ sledi $a_i \leq c_i$, ker je $\leq$ tranzitivna. Torej je $\forall i: a_i \leq c_i \sim 1$. ∎

je tranzitivna

(c) Skiciraj Hassejev diagram te delne urejenosti v primeru $n = 3$.



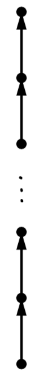


(d) Ali je $\preceq$ relacija linearne urejenosti? Za kateri n oziroma zakaj ne? Kako to sledi iz Hassejevega diagrama?

Za $n = 1$ je linearna urejenost. Za $n > 1$ ni linearna urejenost, ker nista poljubna dva elementa B_n primerljiva.

Npr. za $x = 1\underbrace{0000\ldots0}_{n-1}$ in $y = 01\underbrace{00\cdots0}_{n-2}$ ne velja niti $x \preceq y$ niti $y \preceq x$.

Če bi bila linearna urejenost, potem bi bil pripadajoči Hassejev diagram brez razvejišč:



Relacija R na A je linearna urejenost, če je R delna urejenost in za vse $x, y \in A$ velja $xRy \vee yRx$.

(e) Preveri, da velja implikacija: Če $a \preceq b$, potem $a \leq b$.

$a = a_n a_{n-1} \cdots a_{1(2)} \Rightarrow a = \sum_{i=1}^{n} a_i \cdot 2^{i-1}$

dvojiški zapis

Naj bo $a \preceq b$. Potem je $\forall i: a_i \leq b_i$, zato je

$$a = \sum_{i=1}^{n} a_i \cdot 2^{i-1} \leq \sum_{i=1}^{n} b_i \cdot 2^{i-1} = b.$$

4. Na množici števil $\mathbb{N} \setminus \{0\}$ definiramo relacijo R:

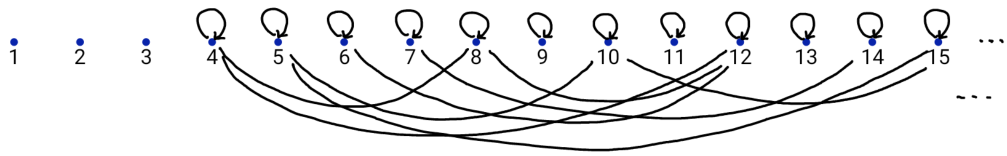
$$aRb \quad \Leftrightarrow \quad \gcd(a,b) > 3.$$

   (a) Pokaži, da je $R \subseteq R^2$.
   (b) Ali je relacija R refleksivna, simetrična ali tranzitivna?
   (c) Ali je relacija R^2 refleksivna, simetrična ali tranzitivna?

(a) Pokaži, da je $R \subseteq R^2$.

Za $a > 3$ je $\gcd(a,a) = a > 3$, zato je aRa.

Za $a = 1,2,3$ je $\neg aRa$. Za $a = 1,2,3$ in vse $b \in \mathbb{N} \setminus \{0\}$ je $\gcd(a,b) \leq a \leq 3$, torej $\neg aRb$. Ker je $\gcd(a,b) = \gcd(b,a)$, velja tudi $\neg bRa$. Torej so $a = 1,2,3$ izolirane točke (v grafu relacije R ni nobenih povezav v ali iz $a = 1,2,3$).



Naj bo $(a,b) \in R$. Potem je aRb in $a > 3$. Ker je $a > 3$, je aRa. Ker je aRa in aRb, je aR^2b oziroma $(a,b) \in R^2$.
Torej je $R \subseteq R^2$.

(b) Ali je relacija R refleksivna, simetrična ali tranzitivna?

- R ni refleksivna, ker $\neg 1R1$.
- R je simetrična, ker je $aRb \Leftrightarrow \gcd(a,b) > 3 \Leftrightarrow \gcd(b,a) > 3 \Leftrightarrow bRa$.
- R ni tranzitivna, ker je $4R20 \land 20R5 \land \neg 4R5$.

(c) Ali je relacija R^2 refleksivna, simetrična ali tranzitivna?

- R^2 ni refleksivna, ker $\neg 1R^21$.
- R^2 je simetrična, ker je R simetrična.
- R^2 je tranzitivna: 1, 2 in 3 niso del nobene poti dolžine 2, za vse $a, c \geq 4$ pa velja aR^2c, ker je $aRac$ in $acRc$.
  Torej je $\forall a \forall b \forall c : (aR^2b \land bR^2c \Rightarrow aRc^2) \sim 1$, ker je leva stran implikacije napačna (če je kateri od a, b, c manjši od 4) ali pa je desna stran pravilna (če so vsi večji od 4).

5. V množici celih števil $\mathbb{Z}$ je dana relacija

$$xRy \quad \Leftrightarrow \quad 7 \text{ deli } x^2 - y^2.$$

(a) Dokaži, da je relacija R ekvivalenčna.

(b) Določi ekvivalenčni razred $[1]_R$ števila 1.

(c) Določi moč faktorske množice $\mathbb{Z}/R$.

(a) Dokaži, da je relacija R ekvivalenčna.

$\boxed{a \text{ deli } b \Leftrightarrow b = a \cdot k \text{ za nek } k \in \mathbb{Z}}$

$a \mid b$ = a deli b

$a / b = \frac{a}{b}$

- R refleksivna?

  $\forall x : xRx$?

  $\forall x : 7 \text{ deli } x^2 - x^2$?

  $\forall x : 7 \text{ deli } 0$ ✓

  $0 = 7 \cdot 0$

- R simetrična?

  $\forall x \forall y : (xRy \Rightarrow yRx)$?

  $\forall x \forall y : (7 \text{ deli } x^2 - y^2 \Rightarrow 7 \text{ deli } y^2 - x^2)$ ✓

  če 7 deli $x^2 - y^2$, je $x^2 - y^2 = 7k$ za nek $k \in \mathbb{Z}$,
  zato je $y^2 - x^2 = -7k = 7(-k) = 7l$ za nek $l \in \mathbb{Z}$
  in torej 7 deli $y^2 - x^2$ ■

- R tranzitivna?

  $\forall x \forall y \forall z \, (xRy \wedge yRz \Rightarrow xRz)$?

  $\forall x \forall y \forall z \, (7 \text{ deli } x^2 - y^2 \text{ in } y^2 - z^2 \Rightarrow 7 \text{ deli } x^2 - z^2)$ ✓

  če 7 deli $x^2 - y^2$ in $y^2 - z^2$, potem deli tudi vsoto $x^2 - y^2 + y^2 - z^2 = x^2 - z^2$ ■

$\boxed{a \mid x \wedge a \mid y \Rightarrow a \mid \alpha x + \beta y \text{ za vse } \alpha, \beta \in \mathbb{Z}}$

Če a deli dve števili, deli tudi poljubno celo linearno kombinacijo teh dveh števil

Ker je R refleksivna, simetrična in tranzitivna, je ekvivalenčna.

(b) Določi ekvivalenčni razred $[1]_R$ števila 1.

$$[1] = \{x \in \mathbb{Z} \, ; \, xR1\} = \{x \in \mathbb{Z} \, ; \, 7 \text{ deli } x^2 - 1\} = \{1, -1, 6, -6, 8, -8, 13, -13, 15, -15, 20, -20, \ldots\}$$

+7 +7 +7 +7

(c) Določi moč faktorske množice $\mathbb{Z}/R$.

množica ekvivalenčnih razredov

$$[0] = \{x \in \mathbb{Z} \, ; \, xR0\} = \{x \in \mathbb{Z} \, ; \, 7 \text{ deli } x^2\} = \{0, 7, -7, 14, -14, 21, -21, \ldots\}$$

+7 +7 +7

$$[2] = \{x \in \mathbb{Z} \, ; \, xR2\} = \{x \in \mathbb{Z} \, ; \, 7 \text{ deli } x^2 - 4\} = \{2, -2, 5, -5, 9, -9, 12, -12, 16, -16, 19, -19, \ldots\}$$

+7 +7 +7 +7

$$[3] = \{x \in \mathbb{Z} \, ; \, xR3\} = \{x \in \mathbb{Z} \, ; \, 7 \text{ deli } x^2 - 9\} = \{x \in \mathbb{Z} \, ; \, 7 \text{ deli } x^2 - 2\} = \{3, -3, 4, -4, 10, -10, 11, -11, \ldots\}$$

+7 +7

$$[0] \cup [1] \cup [2] \cup [3] = \mathbb{Z} \Rightarrow \mathbb{Z}/R = \{[0], [1], [2], [3]\} \Rightarrow \underline{\underline{|\mathbb{Z}/R| = 4}}$$

Imamo 4 različne ekvivalenčne razrede.

Krajše:

...	[3]	[1]	[0]	[1]	[2]	[3]	[3]	[2]	[1]	[0]	[1] ...
n	−2	−1	0	1	2	3	4	5	6	7	8
n^2	4	1	0	1	4	9	16	25	36	49	64
$n^2 \% 7$	2	1	0	1	4	2	2	4	1	0	1

ta vzorec se ponavlja

6. Na množici $\mathbb{N} \setminus \{0\}$ je dana relacija:

$$aRb \quad \Leftrightarrow \quad a \text{ deli } b^2.$$

(a) Dokaži, da je relacija R refleksivna.

(b) Ali je R tranzitivna? Dokaži ali pa poišči protiprimer!

(c) Dokaži implikacijo: Če obstaja $k \in \mathbb{N}$, da a deli b^{2^k}, potem velja aR^*b.

(a) Dokaži, da je relacija R refleksivna.

$\forall a \in \mathbb{N}\setminus\{0\}: a \text{ deli } a^2 \Rightarrow \forall a: aRa \Rightarrow R$ je refleksivna

(b) Ali je R tranzitivna? Dokaži ali pa poišči protiprimer!

$\forall a \forall b \forall c: (a \text{ deli } b^2 \wedge b \text{ deli } c^2 \Rightarrow a \text{ deli } c^2)$?

$16 \text{ deli } 4^2 \wedge 4 \text{ deli } 2^2 \wedge \neg\, 16 \text{ deli } 2^2 \longrightarrow a = 16, b = 4, c = 2$ je protiprimer

ni tranzitivna

(c) Dokaži implikacijo: Če obstaja $k \in \mathbb{N}$, da a deli b^{2^k}, potem velja aR^*b.

$\exists k: a \text{ deli } b^{2^k} \Rightarrow aR^*b$

$\boxed{R^* = id \cup R \cup R^2 \cup R^3 \cup R^4 \cup \cdots}$

$aR^*b \Leftrightarrow a = b$ ali aRb ali aR^2b ali ...

$aR^*b \Leftrightarrow a = b$ ali aRb ali pa $\exists c_1, \dots, c_k$, da je $aRc_1Rc_2R\cdots Rc_kRb$

pogojni sklep

Predpostavimo, da za nek k a deli b^{2^k}.

Če je slučajno $a = b$, potem je aR^0b in je aR^*b.

- Če je $k = 0$, potem a deli $b^1 = b$, zato a deli b^2 in je aRb. Torej spet aR^*b.
- Če je $k = 1$, potem a deli b^2, zato je spet aRb in aR^*b.

analiza primerov

- Če pa je $k > 1$, potem

$$a \text{ deli } b^{2^k} = (b^{2^{k-1}})^2,\; b^{2^{k-1}} \text{ deli } \underbrace{(b^{2^{k-2}})^2}_{=b^{2^{k-1}}},\; b^{2^{k-2}} \text{ deli } \underbrace{(b^{2^{k-3}})^2}_{=b^{2^{k-2}}}, \dots,\; b^2 \text{ deli } b^2,$$

zato je $aR\,b^{2^{k-1}},\; b^{2^{k-1}}R\,b^{2^{k-2}},\; b^{2^{k-2}}R\,b^{2^{k-3}}, \dots,\; b^2Rb$, torej je aR^kb in je aR^*b.

Iz predpostavke, da a deli b^{2^k}, torej sledi, da je aR^*b.