RELACIJE (NAPREJ)

EKVIVALENČNA RELACIJA

Def.: $R \subseteq A \times A$ je ekvivalenčna relacija (enakovrednost) če je R refleksivna, simetrična in tranzitivna.

Zgledi:

1) $p \| q$ p je vzporedna q na množici premic v ravnini.
2) a »ima enako barvo oči kot« b … v množici ljudi.
3) $f: A \rightarrow B$ R relacija v A
   $xRy \Leftrightarrow f(x)=f(y)$
4) izberemo $m \in N$, $m>1$
   a »a isti ostanek pri deljenju z m kot« b v Z.

Def.: R ekvivalenčna v A, $x \in A$

$R[x] = \{y \in A;\ yRx\} \leftarrow$ ekvivalenčni razred elementa x

$A/R = \{R[x];\ x \in A\} \leftarrow$ faktorska (kvocientna) množica množice A po relaciji R.

Trditev.: $R \subseteq A \times A$ ekvivalenčna:

$R[x] = R[y] \Leftrightarrow xRy.$

Dokaz: $(\Rightarrow)$

$x \in R[x] \Rightarrow x \in R[y] \Rightarrow xRy$

refleksivnost
predpostavka
def. ekv. Razreda
tranzitivnost

$(\Leftarrow)$ Pokažimo najprej, da $R[x] \subseteq R[y]$

Izberimo poljuben $z \in R[x]$. To pomeni, da je zRx in xRy. $\Rightarrow z \in R[y]$.
Od tod sledi, da $R[x] \subseteq R[y]$. *Doma do konca. Pokaži še, da $R[y] \subseteq R[x]$.*

Izrek: $R \subseteq A \times A$ ekvivalenčna relacija. Potem je A/R razbitje množice A.

Dokaz:

1) Ekvivalenčni razredi niso prazni. Res. $R[x] \ni x$.
2) $\forall a \in A$ obstaja ekvivalenčni razred, ki vsebuje a. Res. $a \in R[a]$.
3) $R[x] = R[y] \vee R[x] \cap R[y] = \emptyset$.
   $(\sim R[x] \cap R[y] \neq \emptyset \Rightarrow R[x] = R[y])$

Recimo, da $z \in R[x] \cap R[y]$. To pomeni: zRx in zRy.
Ker R simetrična: xRz in zRy.
Ker je R tranzitivna: xRy. Zato $R[x] = R[y]$.

Zgledi: (faktorskih množic)

1) {{navpične premice},{vodoravne premice},{45° premice},…} $\cong$ {smeri v ravnini} $\cong [-\pi/2, \pi/2]$

2) {{modrooki},{rjavooki},{zelenooki},...} ≅ {modra,rjava,zelena,rdeča,...}
4) ostanki pri deljenju s 5. Možni ostanki so 0,1,2,3,4
{{...,-5,0,5,10,15,...}
{...,-4,1,6,11,16,...},
{...,-8,-3,2,7,12,17,...},
{...,-7,-2,3,8,13,...},
{...,-6,-1,4,9,14,19,...}}
{R[0],R[1],R[2],R[3],R[19]} (R[19] == R[4]) ≅ {0,1,2,3,4}

Zgledi: Relacije, ki niso ekvivalenčne.

1)	»ima bankovec z isto vrednostjo v denarnici kot«			v {ljudje}	
	NI TRANZITIVNA:	10,50	50,200	20,200	
2)	»ima isti praštevilski delitelj kot«			v {2,3,...}	
	NI TRANZITIVNA:	6	10	35	
3)	»je približno enak«			v R	
	x »se razlikuje od« y »šele na peti decimalki«				
	NI TRANZITIVNA	5,00001	5,00007	5,00012	
		5,00013	5,000015	5,00018	5,00022
		prva in zadnja se že preveč razlikujeta			

KONGRUENCE

Izrek: (o deljenju), $n \in Z$, $m \in N$, $m \geq 1$
Obstajata enolično določeni celi števili k,r: $0 \leq r < m$, za kateri je $n = k*m + r$

Pišemo: r = n mod m
r je ostanek pri deljenju n-ja z m-jem
k je kvocient pri deljenju n-ja z m-jem

Zgled:
57 delimo s 13
57 = 4*13 + 5
[-57 = -4*13 + (-5)] (to nismo hotl)
-57 = -5*13 + 8

Def.: $m|n$ (beremo: m deli n), če je ostanek pri deljenju n-ja z m-jem enak 0.
⇔ n mod m = 0 ⇔ $\exists k \in Z: n = k*m$ (Pazi: $m \neq 0$)

Def.: $m \in N$, $m \geq 1$
Celi števili x in y sta kongruentni po modulu m, če $m|(x-y)$.
To se zgodi natanko tedaj, ko dasta x in y pri deljenju z m isti ostanek.
Pišemo tudi $x \equiv y \pmod m$ [x je kongruentno po modulu m]

Zgled: $57 \equiv 5 \pmod{13}$
$23 \equiv 3 \pmod{10}$
$55 \not\equiv 2 \pmod 7$

Zgled: Ure v dnevu interpretiramo kot ostanke pri deljenju z 12 (ali 24).

8.12.2004

$16+16 \equiv 8 \pmod{24}$

Zgled: ISBN 961-212-039-0 — Batagelj: DS1, L&M, naloge 1994

geografsko območje
založba
knjiga v založbi
kontrolna cifra 0,1,2,3,4,5,6,7,8,9,X (X=10)

$10*9 + 9*6 + 8*1 +$
$7*2 + 6*1 + 5*2 +$
$4*0 + 3*3 + 2*9 +$
$1*K \equiv 0 \pmod{11}$

961-90105-0-7 — Kuharica S. Vendeline, Vale-Novak

$10*9 + 9*6 + 8*1 +$
$7*9 + 6*0 + 5*1 + 4*0 + 3*5 +$
$2*0 +$
$7*K \equiv 0 \pmod{11}$

Zgled: EMŠO

7 številk	50	
rojstni datum		000…499 fantje
		500…999 punce

Domača naloga: poišči kontrolna EMŠO številka ZCRP mod 11

Trditev: Kongruenca po modulu m ($m \geq 1$) je ekvivalenčna relacija.
$Z/_{(\mathrm{mod}\ m)} = Z_m$

Zgled: m=5
$Z_5 = \{[0],[1],[2],[4],[3]\}$ ([3]==[333], [2]==[-333])

Trditev: Kongruenca po modulu m je usklajena z operacijami (+, - in *).

$[a],[b] \in Z_m$
$[a] \pm [b] = [a+b]$
$[a]*[b] = [a*b]$

Komentar: (m=5), potem
[2] + [3] = [5] (ekvivalenčni razred od 5-ice)
[-333] + [333] = [0]

[2]=[-333], [3]=[333] => [5]=[0]

[2] * [3] = [6]
[-333] * [333] = [-110889]
torej [6]=[-110889]

Naloga: Izračunaj ostanek pri deljenju števila 3^{120} s 13.
Kakšni so ostanki zaporednih potenc števila 3 pri deljenju s 13?

$3^0 \equiv 1 \pmod{13}$ v Z_{13}: $[3^0]=[1]$
$3^1 \equiv 3 \pmod{13}$ $[3^1]=[3]$
$3^2 \equiv 9 \pmod{13}$ $[3^2]=[9]$
$3^3 \equiv 1 \pmod{13}$ $[3^3]=[1]$
$[3^6]=[3^3*3^3]=[3^3]*[3^3]=[1]*[1]=[1]$
$3^6 \equiv 1 \pmod{13}$ $[3^6]=[1]$
$[3^{120}]=[(3^3)^{40}]=[3^3]^{40}=[1]^{40}=[1^{40}]=[1]$
$3^{120} \equiv 1 \pmod{13}$ $[3^{120}]=[1]$

STRUKTURE (RELACIJE) UREJENOSTI

Osnova za relacije urejenosti je tranzitivnost

Def.: $R \subseteq A \times A$

1) R delno ureja A (R je delna urejenost v A), če je:
   - refleksivna,
   - asimetrična,
   - tranzitivna
2) R linearno ureja A (R je linearna urejenost v A), če je:
   - delno ureja A,
   - sovisna

Zgledi:

1) $\subseteq$ delno ureja vsako družino množic
2) $|$ (deljivost) delno ureja $\{1,2,3,\ldots\}$
3) $\leq$ linearno ureja N, Z, Q, R

Pisava: Če relacija R delno ureja A, potem namesto R pogosto pišemo $\leq$.

$x \leq y$ ... »x je pod y«
$x < y$ ... »$x \leq y \wedge x \neq y$«
$x \geq y$ ... $y \leq x$ »x je nad y«
$x > y$ ... $y < x$
$x \leq y \leq z$ ... $x \leq y \wedge y \leq z$
$x < y < z$ ... $x < y \wedge y < z$

Def.: A delno urejena z $\leq$. $x,y \in A$
$x <\!\!\bullet\, y \Leftrightarrow x < y \wedge \forall z \in A (x \leq z \leq y \Rightarrow z = x \vee z = y)$
x je neposredni predhodnik y-ona $\vee$
x je neposredni naslednik x-a

Komentar: $R, \leq \rightarrow$ $<\!\!\bullet$ je prazna
$Z, \leq$ $x <\!\!\bullet\, y \Leftrightarrow y = x+1$

Trditev: A delno ureja z $\leq$.

1) Relacija $<$ je irefleksivna, asimetrična in tranzitivna
2) Relacija $<\!\!\bullet$ je irefleksivna, asimetrična in intranzitivna

Dokaz:

1) irefleksivnost √, asimetrična √, tranzitivnost √
2) intranzitivnost √