Relacije

Naj bo A neka množica. Podmnožici $R \subseteq A \times A$ rečemo *relacija* na množici A. Če je $(x, y) \in R$, pišemo xRy.

$$R(x) = \{y \in A : xRy\}$$
$$R^{-1}(y) = \{x \in A : yRx\}$$

Definicijsko območje:

$$D_R = \{x \in A : R(x) \neq 0\}$$

Zaloga vrednosti:

$$Z_R = \{y \in A : R^{-1}(y) \neq 0\}$$

Graf relacije $R \subseteq A^2$ je slika na kateri vsakemu elementu iz A pripada svoja točka za vask par $(x, y) \in R$ pa naredimo puščico iz $x \to y$.

Operacije na relacijah

Komplement

$$\overline{R} = A^2 - R$$

Inverz

$$xR^{-1}y \Leftrightarrow yRy$$

Kompozitum

$$x(R \circ T)y \Leftrightarrow \exists z \in A : xTz \wedge zRy$$

Lastnosti relacij

R je *refleksinva* $\Leftrightarrow \forall x \in A : xRx$
R je *irefleksinva* $\Leftrightarrow \forall x \in A : \neg(xRx)$
R je *simetrična* $\Leftrightarrow \forall x, y \in A : xRy \Rightarrow yRx$
R je *asimetrična* $\Leftrightarrow \forall x, y \in A : xRy \Rightarrow \neg(yRx)$
R je *antisimetrična* $\Leftrightarrow \forall x, y \in A : xRy \Rightarrow \neg(yRx) \vee x = y$
R je *tranzitivna* $\Leftrightarrow \forall x, y, z \in A : xRy \wedge yRz \Rightarrow xRz$
R je *sovisna* $\Leftrightarrow \forall x, y \in A : xRy \vee yRx \vee x = y$
R je *strogosovisna* $\Leftrightarrow \forall x, y \in A : xRy \vee yRx$
R je *enolična* $\Leftrightarrow \forall x, y, z \in A : xRy \wedge xRz \Rightarrow y = z$

Ekvivalenčne relacije

Relacija je ekvivalenčna, če je *refleksivna*, *simetrična* in *tranzitivna*.

Ekvivalenčni razred

Naj bo R ekvivalenčna relacija. $R(a)$ je ekvivalenčni razred elementa a.

$$a \in A : R(a) = \{b \in A : aRb\}$$

Množica ekvivalenčnih razredov glede na R:

$$A_{/R} = \{R(a) : a \in A\}$$

Relacije urejenosti

Vsaki *tranzitivni* relaciji rečemo relacija urejenosti. Naj bo R tranzitivno:

- R je **delna urejenost**, če je *refleksivna* in *antisimetrična*
- R je **linearna urejenost**, če je *antisimetrična* in *strogo sovisna* (in zato tudi refleksivna)
- R je **stroga delna urejenost**, če je *asimetrilna* (in zato irefleksivna)
- R je **stroga linearna urejenost**, če je *asimetrilna* in *sovisna*
- R je **dobra urejenost**, če je *linearna urejenost* in ima vasaka podmnožica svoj *minimum*

Naj bo R relacija urejenosti na A in $X \subseteq A$:

- Element $a \in A$ je **zgornja meja** za X, če velja $\forall x \in X : xRa$.
- Element $a \in A$ je **spodnja meja** za X, če velja $\forall x \in X : aRx$.
- Zgornja meja $a \in X$ je **natančna zgornja meja**/supremum, če za vsako zgornjo mejo b množice X velja $a = b \vee aRb$.
- Spodnja meja $a \in X$ je **natančna spodnja meja**/infimum, če za vsako spodnjo mejo b množice X velja $a = b \vee bRa$.
- **maksimum** je taka *natančna zgornja meja*, ki je vsebovana v množici X.
- **minimum** je taka *natančna spodnja meja*, ki je vsebovana v množici X.

Funkcije

Enolični relaciji R na A rečemo tudi funkcija.

$$R : D_R \to A$$

Relacija $R \subseteq A^2$ je:

- **injektivna** $\Leftrightarrow \forall x, y, z \in A : xRy \wedge zRy \Rightarrow x = z$
- **surjektivna** $\Leftrightarrow Z_R = A$
- **bijektivna** $\Leftrightarrow$ injektivna in surjektivna

Funkcija R ima inverz $\Leftrightarrow$ ko je R *injektivna*

Moč množic

Množici A, B sta eneko močni (ekvipotentni, imata isto kardinalnost), če obstaja bijektivna preslikava iz A v B. Pišemo $|A| = |B|$.
Množica A je *neskončna* $\Leftrightarrow \exists B \subset A : |A| = |B|$

$$|A| \leq |B| \Leftrightarrow \exists f : A \to B, \text{ ki je injektivna}$$
$$|A| \leq |B| \Leftrightarrow \exists f : B \to A, \text{ ki je surjektivna}$$

Teorija števil

$$a|b \Leftrightarrow \exists k : b = ka$$

Deleitelji števila a:

$$D(a) = \{m \in \mathbb{Z} : m|a\}$$

$$D^+(a) = \{m \in \mathbb{N} : m|a\}$$

Večkratniki števila a:

$$V(a) = \{b \in \mathbb{Z} : a|b\} = \{ka : k \in \mathbb{Z}\}$$

Največji skupni delitelj

$$\gcd(a, b) = \max(D^+(a) \cap D^+(b))$$

Najmanjši skupni večkratniki

$$\text{lcm}(a, b) = \min(V^+(a) \cup V^+(b))$$

Če za $a, b \in \mathbb{Z} - \{0\}$ velja $\gcd(a, b) = 1$, sta si a in b **tuji števili**.

$$\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$$

$$a, b, c \in \mathbb{Z} - \{0\} : \gcd(a, b) = 1 \wedge a|bc \Rightarrow a|c$$

$$a, b, c \in \mathbb{Z} - \{0\} : c|a \wedge c|b \Rightarrow \gcd\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\gcd(a, b)}{c}$$

$$\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$$

Praštevila

Če sta edina pozitivna delitelja naravnega števila $n \geq 2$ 1 in n, je n **praštevilo**. Množica preštevil:

$$\mathbb{P} = \{2, 3, 5, 7, 11, ...\}$$

Razcep na prafaktorje

Vsak $n \geq 2$ lahko zapišemo kot produkt praštevil $p_1, ..., p_m$:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_m^{\alpha_m}$$

Linearne diofantske enačbe

Diofantska enačba $ax + by = c$ ima rešitev $\Leftrightarrow gcd(a, b)|c$.
Če ima eno rešitev $(x_0, y_0) \in \mathbb{Z}^2$ ima neskončno množico rešitev:

$$\{(x_k, y_k) : k \in \mathbb{Z}\}$$
$$x_k = x_0 - k\frac{b}{\gcd(\text{a, b})}$$
$$y_k = y_0 + k\frac{a}{\gcd(\text{a, b})}$$

Razširjen evklidov algoritem

vhod: (a, b)
$(r_0\ ,\ x_0\ ,\ y_0) = (a\ ,\ 1\ ,\ 0)$
$(r_1\ ,\ x_1\ ,\ y_1) = (b\ ,\ 0\ ,\ 1)$
$i = 1$

dokler $r_i \neq 0$:
$i = i{+}1$
$k_i = r_{i-2}//r_{i-1}$
$(r_i, x_i, y_i) = (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})$
konec zanke
vrni: $(r_{i-1}, x_{i-1}, y_{i-1})$

Naj bosta $a, b \in \mathbb{Z}$. Tedaj trojica (d, x, y), ki jo vrne razširjen evklidov algoritem z vhodnim podatkomk (a, b), zadošča:

$$ax + by = d \text{ in } d = \gcd(a, b)$$

Modularna aritmetika

Kongurenca

$$a \equiv_m b \Leftrightarrow m|(b - a)$$

$$a \equiv_m b \Leftrightarrow a \bmod m = b \bmod m$$

$$r = x \bmod m \Leftrightarrow r \equiv_m x \text{ in } r \in \{0, 1, ..., m - 1\}$$

Če je $x_1 \equiv_m y_1$ in $x_2 \equiv_m y_2$:

$$x_1 + x_2 \equiv_m y_1 + y_2$$
$$x_1 x_2 \equiv_m y_1 y_2$$
$$x_1^r \equiv_m y_1^r$$

Če je $ax \equiv_m ay$:

$$x \equiv y \left(\bmod \frac{m}{\gcd(a, m)}\right)$$

Kolobar ostankov

$$\mathbb{Z}_m = \{0, 1, ..., m - 1\}$$
$$a, b \in \mathbb{Z}_m$$

$a \bigoplus b = (a + b) \bmod m \sim a + b$
$a \bigodot b = (ab) \bmod m \sim ab$

$(\mathbb{Z}_m, +, \cdot)$ je kolobar ostankov po mod m

- Operaciji $+$ in $\cdot$ sta asociativni, distributivni in komutativni
- 0 je enota za $+$ in 1 je enota za $\cdot$
- vsak $a \in \mathbb{Z}_m$ ima nasprotni element $(-a)$

$$-a = \begin{cases} m - a; a \neq 0 \\ 0; a = 0 \end{cases}$$

Naj bo $a \in \mathbb{Z}_m$. Če obstaja $b \in \mathbb{Z}_m$, za katerega je $ab = 1$ v $\mathbb{Z}_m$ potem je a *obrnljiv* in b njegov *inverz* (v $\mathbb{Z}_m$).
Množico vseh obrnlivih elementov v $\mathbb{Z}_m$ označimo $\mathbb{Z}_m^*$.

$$a \in \mathbb{Z}_m^* \Leftrightarrow a \text{ je tuj } m$$

Inverz od a je tisti $x \in \mathbb{Z}_m$, ki (skupaj z nekim y) reši diofantsko enačbo $ax + (-m)y = 1$
Vsak element $\mathbb{Z}_m^*$ ima natanko en inverz. Označimo ga z a^{-1}.

Euljerjeva funkcija

Euljerjeva funkcija nam pove koliko je obrnlivih elementov v $\mathbb{Z}_m$.

$$\varphi(m) = \begin{cases} |\{a \in \mathbb{Z}_m - \{0\} : \gcd(a, m) = 1\}|; m \geq 2 \\ 1; m = 1 \end{cases}$$

$$\varphi(p^k) = (p - 1)p^{k-1} = p^k \left(1 - \frac{1}{p}\right); p \in \mathbb{P}$$

Za $n \in \mathbb{N}$ s paraštevilskim razcepom $n = p_1^{\alpha_1} \cdot ... \cdot p_m^{\alpha_m}$ velja:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot ... \cdot \varphi(p_m^{\alpha_m}) = n \prod_{p_k \in \mathbb{P}} \left(1 - \frac{1}{p_k}\right)$$

Euljerjev izrek:

$$\gcd(a, m) = 1 \Leftrightarrow a^{\varphi(m)} \equiv_m 1; a \in \mathbb{Z}_m^*$$

$$a, m \in \mathbb{N} \wedge \gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$$
$$a^{\varphi(m)} = 1 \text{ v } \mathbb{Z}_m^*$$

Mali Frematov izrek: če je $m \in \mathbb{P}$ ($\varphi(m) = m - 1$) in $\gcd(a, m) = 1$, potem:

$$a^{m-1} \equiv_m 1$$

RSA

A želi varno prejeti sporočilo od B.

- A izbere praštevili p in q
- A izračuna $n = pq$ in $\varphi = \varphi(n) = (p - 1)(q - 1)$
- A izbere $e \in \mathbb{Z}_\varphi^*$, ki je tuje φ
- A izračuna $d = e^{-1}$ (reši diofantsko enačbo $ex - \varphi y = 1$ za $x = d$ in y)
- A javno objavi (n, e) in si naskrivaj zapomni d
- B sestavi sporočilo m
- B izračuna $m' = m^e \bmod n$
- B pošlje m'
- A izračuna $m'' = m'^d \bmod n$

Izkaže se, da je m'' enak m

Permutacije

Permutacija množice Ω je bijektivna preslikava $\pi : \Omega \to \Omega$
$\mathrm{Sym}(\Omega)$ je množica vseh permutacij na Ω.

$$|\mathrm{Sym}(\Omega)| = |\Omega|!$$

$$S_n = \mathrm{Sym}(\Omega); \Omega = \{1, 2, ..., n\}$$

Ciklična struktura

Multimnožica določin ciklov.

- **negibne točke**: cilki dolžine 1
- **transpozicije**: cilki dolžine 2
- **k-cikli**: cilki dolžine k

Ciklična premutacija je taka premutacija kjer je največ en cikel dolžine več kot 1. (ostali pa so dolžine 1)

Produkt permutacij

$$(\pi \cdot \varphi)(\omega) = (\varphi \circ \pi)(\omega) = \varphi(\pi(\omega))$$
$$\pi(\omega) = \omega^\pi$$
$$(\pi \cdot \varphi)(\omega) = \omega^{(\pi \cdot \varphi)} = (\omega^\pi)^\varphi = \omega^{\pi\varphi}$$

Nosilec
Naj bo $\pi \in \mathrm{Sym}(\Omega)$.

$$\mathrm{supp}(\pi) = \{\omega \in \Omega : \omega^\pi \neq \omega\}$$

$$\omega \in \mathrm{supp}(\pi) \Leftrightarrow \omega^\pi \in \mathrm{supp}(\pi)$$

$\pi, \varphi \in \mathrm{Sym}(\Omega)$ sta **disjunktni** permutaciji, če

$$\mathrm{supp}(\pi) \cap \mathrm{supp}(\varphi) = \emptyset$$

Če sta permutaciji $\pi, \varphi \in \mathrm{Sym}(\Omega)$ disjunktni, **komutirata** $(\pi \cdot \varphi = \varphi \cdot \pi)$.

Red permutacije

Red permutacije $\alpha \in S_n$ je najmanjše število k, da je

$$\alpha^k = \mathrm{id}$$

Inverzije

$\varphi \in S_n$, par števil i, j $(1 \leq i < j \leq n)$ je v *inverzu* v permutaciji φ, če se v spodnji vrstici zapisa parmutacije φ s tabelo pojavita v "napačnem" vrstnem redu: večje število je zapisano bolj levo od manjšega.
Število inverzi permutacije φ označimo z $\mathrm{inv}(\varphi)$.

Denimo, da je φ permutacija in τ transpozicija, potem velja:

$$\mathrm{inv}(\varphi) \not\equiv_2 \mathrm{inv}(\varphi \cdot \tau)$$

Permutacija $\varphi \in S_n$ je soda $\Leftrightarrow \mathrm{inv}(\varphi)$ sodo.
Permutacija $\varphi \in S_n$ je liha $\Leftrightarrow \mathrm{inv}(\varphi)$ liho.

Vsako permutacijo lahko zapišemo kot produkt transpozicij.

$$\pi = (13927)(4658) = (13)(19)(12)(17)(46)(45)(48)$$

$$(1\ 2\ 3\ ...\ n) = (1\ 2)(1\ 3)...(1\ n)$$

Permutacija je **soda**, če je n lih.
Permutacija je **liha**, če je n sod.