Diskretne strukture

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

22. december 2023

Izrek o deljenju

Izrek (o deljenju)

Naj bosta $m, n \in \mathbb{Z}$ in $m > 0$. Obstajata enolično določeni celi števili k in r, pri čemer je

$$n = k \cdot m + r \quad \text{in velja} \quad 0 \leq r < m.$$

k je *kvocient* števil n in m
r je *ostanek* pri deljenju števila n z m.

Deljivost celih števil

Naj bosta $m, n \in \mathbb{Z}$. Pravimo, da m *deli* n,

$$m|n,$$

če je rešljiva enačba $n = m \cdot x$.

Če sta m in n različna od 0, potem lahko definiramo

$$\mathrm{gcd}(m,n) = \max\{d \in \mathbb{Z}\ ;\ d|m \text{ in } d|n\}$$

največji skupni delitelj števil m in n

$$\mathrm{lcm}(m,n) = \min\{v \in \mathbb{Z}\ ;\ m|v \text{ in } n|v \text{ in } v > 0\}$$

najmanjši skupni večkratnik števil m in n

Razširjeni Evklidov Algoritem - REA

Zgled: Poišči $\mathrm{gcd}(899, 812)$.

Razširjeni Evklidov Algoritem - REA

Izrek (REA)

Naj bosta m in n celi števili in $d = \mathrm{gcd}(m, n)$. Potem obstajata $s, t \in \mathbb{Z}$, za katera je

$$\mathrm{gcd}(m, n) \; = \; d \; = \; s \cdot m + t \cdot n$$

Tako d kot koeficienta s in t preberemo iz predzadnje vrstice REA.

Tuja števila

Pravimo, da sta si celi števili a in b *tuji*, če je $\mathrm{gcd}(a, b) = 1$.
V tem primeru pišemo $a \perp b$.

Zgled: $89 \perp 81$

Trditev

Naj velja $a|(b \cdot c)$ in $a \perp b$. Potem $a|c$.

Izrek

Naj bosta $a, b \in \mathbb{N}$. Potem je $\mathrm{gcd}(a, b) \cdot \mathrm{lcm}(a, b) = a \cdot b$.

Linearne diofantske enačbe

Naloga: Skupina otrok je v slaščičarni jedla torte in kremne rezine. Koliko tort in koliko kremnih rezin so pojedli, če je račun znašal 104,80 EUR, torta stane 7,20 EUR, kremšnita pa 5,60 EUR.
Vemo tudi, da so pojedli manj tort kot kremnih rezin.

Linearna diofantske enačbe

Linearna diofantska enačba z dvema neznankama je enačba oblike

$$a \cdot x + b \cdot y = c,$$

kjer so znani $a, b, c \in \mathbb{Z}$, iščemo pa celoštevilsko rešitev x, y.
a in b sta *koeficienta* enačbe, c standardno imenujemo *desna stran*.

Diofantske enačbe

Zgled: Poišči rešitve (linearne) diofantske enačbe $6x + 15y = 7$.

Izrek

Linearna diofantska enačba

$$a \cdot x + b \cdot y = c$$

je rešljiva natanko tedaj, ko $\gcd(a, b) | c$*.*

Če $\gcd(a, b)$ *ne deli desne strani* c*, potem taka diofantska enačba nima rešitev.*

Diofantske enačbe

Izrek

Naj par x_0, y_0 *reši LDE* $a \cdot x + b \cdot y = c$*, in naj bo* $d = \gcd(a, b)$*. Potem so*

$$\begin{aligned} x_k = & \quad x_0 + k \cdot \frac{b}{d} \\ y_k = & \quad y_0 - k \cdot \frac{a}{d}, \end{aligned}$$

kjer je k *poljubno celo število, vse rešitve te diofantske enačbe.*

Kaj so permutacije

Naj bo A poljubna množica. *Permutacija* na A je vsaka bijektivna preslikava $f : A \to A$.

Permutacija reda n je permutacija v $\{1, 2, \dots, n\}$. Množico vseh permutacij reda n imenujemo *simetrična grupa reda n* in jo označimo z S_n.

Zgled:

- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ je permutacija reda 3.
- $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ je permutacija reda 4.
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}$ je permutacija reda 6.

Produkt permutacij

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi * \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

$$\psi * \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

Inverzna permutacija

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 7 & 6 & 5 \end{pmatrix} \qquad \psi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 3 & 2 & 7 & 1 \end{pmatrix}$$

$$\pi * \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 7 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

Grupa S_n

Trditev

Naj bodo $\pi, \psi, \sigma \in S_n$. Velja

- $\pi * \psi \in S_n$
- $\pi^{-1} \in S_n$
- $\pi * (\psi * \sigma) = (\pi * \psi) * \sigma$
- $(\pi * \psi)^{-1} = \psi^{-1} * \pi^{-1}$
- $\pi * \pi^{-1} = \pi^{-1} * \pi = \mathrm{id}$
- $\pi * \mathrm{id} = \mathrm{id} * \pi = \pi$

Zapis permutacije z disjunktnimi cikli

Permutacijo lahko zapišemo tudi *z disjunktnimi cikli* in ne v obliki *tabelice*.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi * \psi = (1234)(57) * (176)(2534) =$$

$$\psi * \pi = (176)(2534) * (1234)(57) =$$

Ciklična struktura permutacije

Ciklična struktura permutacije je število ciklov posameznih dolžin v zapisu permutacije z disjunktnimi cikli.

Ciklična struktura permutacije π je
Ciklična struktura permutacije ψ je

1-ciklu pravimo tudi *fiksna točka* permutacije,
2-ciklu pa *transpozicija*.

Potenciranje permutacij

Za potenciranje permutacij je ugodnejši zapis permutacije *z disjunktnimi cikli* kot pa zapis v obliki *tabelice*.

$$\pi =$$

Kako izračunati $\pi^2, \pi^3, \pi^4, \ldots$?

$\pi^2 =$

$\pi^3 =$

$\vdots$

Potenciranje ciklov

Potencirajmo 5- in 6-cikel, $\alpha = (12345)$, $\beta = (123456)$.

Potenciranje ciklov

Trditev

Naj bo α permutacija, sestavljena iz samo enega cikla dolžine n. Permutacija α^k je sestavljena iz $\gcd(n,k)$ disjunktnih ciklov, ki so vsi iste dolžine $\frac{n}{\gcd(n,k)}$.

Posledica

Naj bo α permutacija, sestavljena iz samo enega cikla dolžine n. Potem je $\alpha^n = \mathrm{id}$ in $\alpha^{-1} = \alpha^{n-1}$ in je n najmanjše naravno število (> 0) s to lastnostjo.

Potenciranje permutacij

Izrek

Naj bo

$$\pi = \alpha_1 * \alpha_2 * \cdots * \alpha_m,$$

kjer so α_i, $i = 1, \ldots, m$, cikli v zapisu permutacije α z disjunktnimi cikli. Potem je

$$\pi^k = {\alpha_1}^k * {\alpha_2}^k * \cdots * {\alpha_m}^k.$$

Zapis permutacije s transpozicijami

Trditev

Vsako permutacijo lahko zapišemo kot produkt transpozicij.

Komentar: Ker že *zapis cikla* ni enoličen, tudi zapis kot produkt transpozicij ni enolično določen.

Parnost permutacij

Izrek (o parnosti permutacij)

Denimo, da lahko permutacijo π zapišemo kot produkt m transpozicij, pa tudi kot produkt (morda drugih) n transpozicij. Potem je

$$m \equiv n \pmod 2.$$

Parnost permutacij

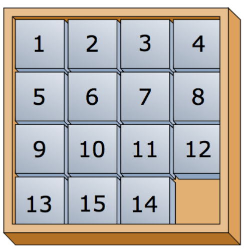
Permutacija je *soda*, če jo lahko zapišemo kot produkt sodo mnogo transpozicij, permutacija je *liha*, če jo lahko zapišemo kot produkt liho mnogo transpozicij.

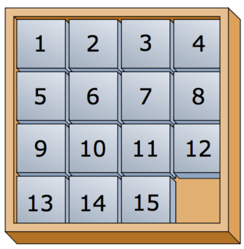
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix}$$

Pravimo, da sta (v permutaciji π) števili 1 in 2 v *inverziji*, ker sta v spodnji vrstici tabelice v *napačnem* vrstnem redu: 1 je manjše kot 2, toda 2 je zapisana pred 1.

Igra 15

Igro 15 igramo na kvadratni igralni površini, na kateri je 15 ploščic s številskimi oznakami in eno *prazno polje*.





Naš cilj je, da s premikanjem ploščic dosežemo *ciljno konfiguracijo*, v kateri so številke po poljih urejene po velikosti.

V tem primeru pravimo, da smo igro *uspešno zaključili.*

Kakšna je zveza s permutacijami? Kaj je ena poteza?

Linearna enačba

Trditev

Naj bodo α, β, γ znane permutacije iz S_n in π neznana permutacija. Enačba

$$\alpha * \pi * \beta = \gamma$$

je v S_n enolično rešljiva.

Potenčna enačba

Kaj lahko poveš o rešljivosti kvadratne enačbe

$$\alpha * \pi^2 * \beta = \gamma$$

$\pi^2 = (1\,2)(3\,4\,5\,6\,7)$

$\pi^2 = (1\,2)(3\,4)(5\,6\,7\,8\,9)$

$\pi^2 = (1\,2)(3\,4\,5\,6)(7\,8\,9\,10\,11)$

$\pi^3 = (1\,2)(3\,4)(5\,6\,7\,8\,9)$

$\pi^3 = (1\,2)(3\,4\,5\,6)(7\,8\,9\,10\,11)$

Red permutacije

Red permutacije π je najmanjše naravno število $k \geq 1$, za katerega je

$$\pi^k = \mathrm{id}.$$

Trditev

Red permutacije π je najmanjši skupni večkratnik dolžin ciklov v zapisu permutacije π z disjunktnimi cikli.