Diskretne strukture

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

8. januar 2016

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

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

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 obstaja tak $k \in \mathbb{Z}$, da je $n = k \cdot m$.

Če sta m in n različna 0, potem lahko definiramo

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

največji skupni delitelj števil m in n

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

najmanjši skupni večkratnik števil m in n

Razširjeni Evklidov Algoritem - REA

Zgled: Poišči $\gcd(899, 812)$.

Razširjeni Evklidov Algoritem - REA

Trdimo:

- 29 deli vse desne strani enačb.
  Posebej, 29 deli tudi 812 in 899.
- 29 je celoštevilska linearna kombinacija števil 812 in 899.
- Če število d deli 899 in 812, potem deli tudi vsako njuno celoštevilsko linearno kombinacijo. Zato deli tudi 29.
- 29 je največji skupni delitelj števil 899 in 812.

Razširjeni Evklidov Algoritem - REA

Izrek (REA)

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

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

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 $\gcd(a, b) = 1$.
V tem primeru pišemo $a \perp b$.

Zgled: $899 \perp 813$

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

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

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 39,30 EUR, torta stane 2,70 EUR, kremšnita pa 2,10 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

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

$$x_k = x_0 + k \cdot \frac{b}{d}$$

$$y_k = y_0 - k \cdot \frac{a}{d},$$

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 $\dfrac{n}{\gcd(n,k)}$.

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

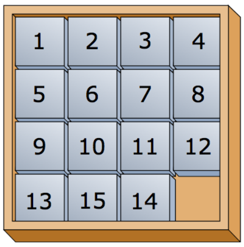
Permutacija je *soda*, če jo lahko zapišemo kot produkt sodo mnogo transpozicij, permutacija je *liha*, če jo lahko zapišemo kot produkt liho mnogo transpozicij.

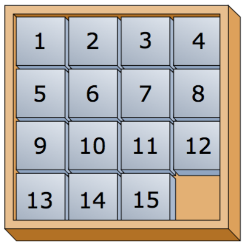
$$\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{smallmatrix}\right)$$

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.

Kvadratna enačba

Kaj lahko poveš o rešljivosti kvadratne enačbe

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

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.

Linearna rekurzivna enačba

Linearna rekurzivna enačba (s konstantnimi koeficienti) je enačba oblike

$$c_d a_{n+d} + c_{d-1} a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = f(n) \quad (\text{za } n \geq 0)$$

kjer so $c_d, c_{d-1}, \ldots, c_1, c_0$ dana števila , $f(n)$ pa predpisano zaporedje.

Pravimo, da je LRE *homogena*, če je $f(n) = 0$ za vse $n \geq 0$. Sicer je LRE *nehomogena*.

Privzeli bomo, da sta koeficienta c_d in c_0 različna od 0, v tem primeru pravimo, da je LRE *stopnje d*.

Karakteristični polinom

Karakteristični polinom LRE

$$a_{n+d} + c_{d-1} a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = f(n)$$

je polinom

$$Q(x) = x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0$$

Trditev

Če je λ ničla karakterističnega polinoma, potem je $a_n = \lambda^n$ rešitev homogene LRE

$$a_{n+d} + c_{d-1} a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = 0$$

Zajčki in besede brez *bb*

Karakteristični polinom lineranih rekurzivnih enačb

$$z_{n+2} - z_{n+1} - z_n = 0 \qquad \text{in} \qquad b_{n+2} - b_{n+1} - b_n = 0$$

je enak

$$Q(x) = x^2 - x - 1,$$

njegovi ničli sta

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \qquad \text{in} \qquad \lambda_2 = \frac{1-\sqrt{5}}{2}$$

Zato sta *geometrijski* zaporedji

$$(\lambda_1^n)_{n\in\mathbb{N}} \qquad \text{in} \qquad (\lambda_2^n)_{n\in\mathbb{N}}$$

rešitvi omenjene LRE.
Toda, ne eno ne drugo zaporedje ni rešitev zastavljene naloge!!!!

Splošna rešitev homogene enačbe

Trditev
Če sta a'_n in a''_n rešitvi homogene LRE

$$a_{n+d} + c_{d-1}a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = 0,$$

potem je pri poljubnih realnih številih α in β tudi

$$\bar{a}_n = \alpha a'_n + \beta a''_n$$

rešitev omenjene LRE.

Ideja! Število zajčkov z_n izrazimo kot

$$z_n = \alpha\lambda_1^n + \beta\lambda_2^n,$$

pri čemer števili α, β izberemo tako, da zadostimo začetnim pogojem $z_0 = 0, z_1 = 1$.

Splošna rešitev homogene enačbe

Denimo, da je $Q(x)$ karakteristični polinom LRE stopnje d in so

$$\lambda_1, \lambda_2, \dots, \lambda_d$$

njegove različne ničle.
Potem je splošna rešitev takšne homogene LRE oblike

$$a_n = \alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n + \cdots + \alpha_d \lambda_d^n$$

in *koeficiente* $\alpha_1, \dots, \alpha_d$ lahko enolično določimo iz *d začetnih pogojev*, vrednosti začetnih členov $a_0, a_1, \dots, a_{d-1}$.
V primeru, ko ima karakteristični polinom $Q(x)$ same različne ničle, je družinica geometrijskih zaporedij

$$(\lambda_1^n)_{n\in\mathbb{N}}, \quad (\lambda_2^n)_{n\in\mathbb{N}}, \dots, (\lambda_d^n)_{n\in\mathbb{N}}$$

zadostna.
Če ima $Q(x)$ večkratne ničle, se moramo znajti malo drugače.

Splošna rešitev homogene LRE

Trditev

$$a_{n+d} + c_{d-1} a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = 0$$

Naj bodo $\lambda_1, \dots, \lambda_k$ ničle karakterističnega polinoma LRE večkratnosti (po vrsti) $m_1, \dots, m_k$, ter naj bodo $P_i(n)$, $i = 1, \dots, k$, polinomi z nedoločenimi koeficienti stopenj $m_i - 1$. Potem je

$$a_n = P_1(n)\lambda_1^n + P_2(n)\lambda_2^n + \cdots + P_k(n)\lambda_k^n$$

splošna rešitev LRE.

Fibonaccijeva števila, znova

Fibonaccijeva števila $(f_n)_{n\in\mathbb{N}}$ ustrezajo homogeni LRE

$$f_{n+2} = f_{n+1} + f_n$$

in začetnima pogojema $f_0 = 0, f_1 = 1$.

Poišči splošno formulo za rešitev zgornje homogene LRE in določi koeficiente, da dobiš *zaprto formulo* za Fibonaccijeva števila f_n.

Zgledi

Reši naslednji homogeni LRE:

- $a_{n+2} - 3a_{n+1} - 4a_n = 0, \quad a_0 = 1, a_1 = 9$
- $a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 0, \quad a_0 = 3, a_1 = 6, a_2 = 13$

Nehomogene enačbe

Trditev

Splošno rešitev LRE

$$a_{n+d} + c_{d-1}a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = f(n)$$

iščemo v obliki $a_n = q_n + h_n$, ker je q_n posebna rešitev nehomogene LRE, in h_n splošna rešitev homogene LRE.

Pri tem

1. bomo s q_n poskrbeli za *desno stran* in
2. z izbiro h_n poskrbimo za začetne pogoje (če jih imamo).

Nehomogene enačbe, nastavek

Rešujemo nehomogeno LRE, pri čemer je desna stran $f(n) = p(n)\alpha^n$

$$a_{n+d} + c_{d-1}a_{n+d-1} + \cdots + c_1 a_{n+1} + c_0 a_n = p(n)\alpha^n$$

kjer je $p(n)$ polinom stopnje r.

Če je α *s-kratna ničla* karakterističnega polinoma LRE $Q(x)$, potem posebno rešitev q_n zgornje nehomogene LRE pridelamo z uporabo nastavka

$$q_n = n^s P(n)\alpha^n,$$

kjer je $P(n)$ polinom stopnje r z nedoločenimi koeficienti.

Zgledi

Reši naslednji nehomogeni LRE:

- $a_{n+2} - 3a_{n+1} - 4a_n = 24, \quad a_0 = -3, a_1 = 5$
- $a_{n+2} - 2a_{n+1} + a_n = 12n + 2, \quad a_0 = 3, a_1 = 4$