Diskretne strukture

Izročki, teorija števil

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

5. december 2022

Izrek (o deljenju)

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

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

Dokaz.

Obstoj števil k, r**:** Naj bo k največje celo število, da velja $km \leq n < (k+1)m$. Število $r := n - km$ zadošča $0 \leq r < m$. Velja $n = km + r$.

Enoličnost števil k, r**:** Če sta k' in r' še dve števili, ki zadoščata pogojem izreka, potem je

$$n = k'm + r' = km + r.$$

Od tod sledi

$$(k' - k)m = r - r'.$$

Velja $-m < r - r' < m$ in zato $|r - r'| < m$. Če je $(k' - k)m \neq 0$, potem je $|(k' - k)m| \geq m$. To pa je protislovje z $|r - r'| < m$. Sledi, da je $(k' - k)m = 0$. Od tod pa še $k' = k$ in $r' = r$. □

k je *kvocient* števil n in m ($k = \lfloor \frac{n}{m} \rfloor$), r pa je *ostanek* pri deljenju števila n z m.

Nekaj nujnih definicij

Naj bosta $m, n \in \mathbb{Z}$. Pravimo, da m *deli* n oz. je n *deljiv* z m, kar pišemo z $m|n$, če je rešljiva enačba $n = m \cdot x$.

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

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

in ga imenujemo *največji skupni delitelj* števil m in n, ter

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

in ga imenujemo *najmanjši skupni večkratnik* števil m in n.

Posebej definiramo še $\gcd(a, 0) = a$ in $\operatorname{lcm}(a, 0) = 0$ za vse $a \geq 0$.

Pravimo, da sta si celi števili a in b *tuji*, če je $\gcd(a, b) = 1$. Npr. 89 in 81 sta si tuji.

Motivacija: Radi bi poiskali največji skupni delitelj števil $m, n \in \mathbb{Z}$, hkrati pa še števili s, t, da velja

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

To se da narediti s pomočjo *razširjenega Evklidovega algoritma (REA)*, ki si ga bomo ogledali na naslednjem primeru.

Primer

Poiščimo $\gcd(899, 812)$.

$$\begin{aligned}
(I): &\quad 899 = 1 \cdot 899 + 0 \cdot 812, \\
(II): &\quad 812 = 0 \cdot 899 + 1 \cdot 812, && 899 = 1 \cdot 812 + 87, \\
(III) = (I) + (-1) \cdot (II): &\quad 87 = 1 \cdot 899 - 1 \cdot 812, && 812 = 9 \cdot 87 + 29, \\
(IV) = (II) + (-9) \cdot (III): &\quad 29 = -9 \cdot 899 + 10 \cdot 812, && 87 = 3 \cdot 29 + 0, \\
(V) = (III) + (-3) \cdot (IV): &\quad 0 = 28 \cdot 899 - 31 \cdot 29. \; 812
\end{aligned}$$

gcd je zadnji od 0 različen ostanek. V našem primeru je to 29. Vemo:

- 29 deli vse leve 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.

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.

Uporabimo REA za dokaz naslednje zelo pomembne trditve v teoriji števil.

Trditev

Naj velja $a|(b \cdot c)$ in $\gcd(a, b) = 1$. Potem je $a|c$.

Dokaz.

Iz $a|(b \cdot c)$ sledi, da obstaja $k \in \mathbb{Z}$, ki zadošča

$$bc = ka. \tag{1}$$

Ker je $\gcd(a, b) = 1$, po REA obstaja $s, t \in \mathbb{Z}$, da velja

$$1 = sa + tb. \tag{2}$$

Pomnožimo (2) s c:

$$c = 1 \cdot c = (sa + tb) \cdot c = sac + tbc.$$

Izraz bc nadomestimo v skladu z (1) in izpostavimo a: $c = a(sc + tk)$. Torej $a|c$. □

Z uporabo zadnje trditve lahko dokažemo zanimiv izrek, ki povezuje a, b z $\gcd(a, b), \operatorname{lcm}(a, b)$.

Izrek

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

Dokaz.

Označimo $d = \gcd(a, b)$. Dokazati moramo, da je $\operatorname{lcm}(a, b)$ enak $\frac{a \cdot b}{d}$, ki ga označimo z v. Torej moramo videti, da je $a|v$, $b|v$ in je $v \leq v'$ za poljuben večkratnik v' števil a in b.

Obstajata $a_1, b_1 \in \mathbb{Z}$, da je $a = da_1$, $b = db_1$ in $\gcd(a_1, b_1) = 1$. Torej je $v = da_1b_1 = ab_1 = ba_1$. Zato $a|v$ in $b|v$.

Naj bo sedaj v' nek drug večkratnik števil a in b. Potem je $v' = a\ell_1 = b\ell_2$ za neka $\ell_1, \ell_2 \in \mathbb{Z}$. Naprej

$$v' = a\ell_1 = da_1\ell_1 = db_1\ell_2 \quad \Rightarrow \quad a_1\ell_1 = b_1\ell_2.$$

Ker je $\gcd(a_1, b_1) = 1$, z uporabo trditve od zgoraj velja $b_1|\ell_1$ in zato pri prikladno izbranem ℓ' velja $\ell_1 = \ell' b_1$. Torej je $v' = a\ell_1 = ab_1\ell' = v\ell'$. Torej je $v \geq v'$, kar smo morali dokazati. □

Motivacija: Skupina otrok je v slaščičarni jedla torte in kremne rezine. Koliko tort in koliko kremnih rezin so pojedli, če je račun znašal 98,25 EUR, torta stane 5,25 EUR, kremšnita pa 6,75 EUR. Vemo tudi, da so pojedli več tort kot kremnih rezin.

Rešujemo enačbo

$$5.25 \cdot x + 6.75 \cdot y = 98.25.$$

Množimo enačbo s 100 in dobimo enačbo

$$525 \cdot x + 675 \cdot y = 9825.$$

Delimo enačbo s 75 in dobimo enačbo

$$9 \cdot x + 7 \cdot y = 131.$$

Iščemo *naravni števili* x in y, ki rešita enačbo.

Linearna diofantska enačba z dvema neznankama (LDE) 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. Pravimo, da sta a in b *koeficienta* enačbe, c pa njena *desna stran*.

Izrek

Linearna diofantska enačba

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

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

Dokaz.

Dokaz implikacije ($\Rightarrow$)**:** Naj bo $ax + by = c$ rešljiva. Potem za neka $x_0, y_0 \in \mathbb{Z}$ velja

$$ax_0 + by_0 = \gcd(a, b)k_1x_0 + \gcd(a, b)k_2y_0 = \gcd(a, b)(k_1x_0 + k_2y_0) = c,$$

kjer je $a = \gcd(a, b)k_1$ in $b = \gcd(a, b)k_2$ za neka $k_1, k_2 \in \mathbb{Z}$. Torej je $\gcd(a, b)|c$.

Dokaz implikacije ($\Leftarrow$)**:** Po REA obstajata $x_0, y_0 \in \mathbb{Z}$, da velja

$$ax_0 + by_0 = \gcd(a, b).$$

Pomnožimo zadnjo enačbo s celim številom $\frac{c}{\gcd(a, b)}$ in dobimo

$$a \cdot (x_0 \frac{c}{\gcd(a, b)}) + b \cdot (y_0 \frac{c}{\gcd(a, b)}) = c.$$

Motivacija: Radi bi poiskali vse rešitve LDE. Vse rešitve opiše naslednji izrek.

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.

Dokaz.

Dokažimo najprej, da vsak par (x_k, y_k) res reši $ax + by = c$. Velja:

$$ax_k + by_k = a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) = (ax_0 + by_0) + \frac{akb}{d} - \frac{bak}{d}$$
$$= ax_0 + by_0 = c.$$

Naj bo sedaj $(x', y') \in \mathbb{Z}^2$ poljuben par, ki reši $ax + by = c$. Velja:

$$ax_0 + by_0 = c = ax' + by'.$$

Dokaz.

Od tod sledi

$$a(x_0 - x') = b(y' - y_0).$$

Če je $a = \gcd(a, b)k_1$ in $b = \gcd(a, b)k_2$ za neka $k_1, k_2 \in \mathbb{Z}$ z $\gcd(k_1, k_2) = 1$, potem sledi

$$k_1(x_0 - x') = k_2(y' - y_0).$$

Torej je $k_1 | (y' - y_0)$, $k_2 | (x_0 - x')$ in

$$x' = x_0 - \frac{y' - y_0}{k_1} \frac{b}{\gcd(a, b)}, \quad y' = y_0 + \frac{x_0 - x'}{k_2} \frac{a}{\gcd(a, b)}.$$

Ker je

$$\frac{y' - y_0}{k_1} = \frac{x_0 - x'}{k_2},$$

sta x', y' ravno x_k, y_k za $k = -\dfrac{y' - y_0}{k_1}$. □

- Eno rešitev LDE dobimo tako, da *predzadnjo* vrstico REA pomnožimo s kvocientom desne strani in gcd koeficientov.
- Vse druge rešitve dobimo z uporabo zadnjega izreka.

Primer

Poišči rešitve (linearne) diofantske enačbe $6x + 15y = 9$.

$$\begin{aligned}
(I): &\quad 15 = 1 \cdot 15 + 0 \cdot 6, \\
(II): &\quad 6 = 0 \cdot 15 + 1 \cdot 6, && 15 = 2 \cdot 6 + 3, \\
(III) = (I) - 2(I): &\quad 3 = 1 \cdot 15 - 2 \cdot 6, && 6 = 2 \cdot 3 + 0, \\
(IV) = (II) - 2(III): &\quad 0 = -2 \cdot 15 + 5 \cdot 6.
\end{aligned}$$

Pomnožimo predzadnjo vrstico REA z $\frac{9}{3} = 3$. *Dobimo*

$$9 = 3 \cdot 15 - 6 \cdot 6.$$

Ena rešitev enačbe je $(x_0, y_0) = (-6, 3)$. *Vse rešitve so*

$$(x_k, y_k) = (-6 + 5k, 3 - 2k),$$

kjer je $k \in \mathbb{Z}$.