Diskretne strukture

Trinajstiou sklop izročkov

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

9. januar 2021

Izrek o deljenju in deljivost celih števil

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 ($k = \lfloor \frac{n}{m} \rfloor$), r pa je **ostanek** pri deljenju števila n z m.
- Naj bosta $m, n \in \mathbb{Z}$. Pravimo, da m **deli** n, kar pišemo z $m|n$, če je rešljiva enačba $n = m \cdot x$.
- Če sta m in n različna od 0, potem lahko definiramo
$$\gcd(m, n) = \max\{d \in \mathbb{Z} \,;\, d|m \text{ in } d|n\},$$
in ga imenujemo **največji skupni delitelj** števil m in n, ter
$$\operatorname{lcm}(m, n) = \min\{v \in \mathbb{Z} \,;\, m|v \text{ in } n|v \text{ in } v > 0\},$$
in ga imenujemo **najmanjši skupni večkratnik** števil m in n.
- Posebej definiramo še $\gcd(0, 0) = 0$ in $\operatorname{lcm}(0, 0) = 0$.
- Pravimo, da sta si celi števili a in b **tuji**, če je $\gcd(a, b) = 1$. Npr. 89 in 81 sta si tuji.

Trditev

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

Izrek

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

Izrek *skoraj* velja tudi za celoštevilska a in b. Paziti je potrebno le na predznake.

Razširjeni Evklidov Algoritem - REA

Poiščimo $\gcd(899, 812)$.

$$\begin{aligned}
(1): &\quad 899 = 1 \cdot 899 + 0 \cdot 812, \\
(2): &\quad 812 = 0 \cdot 899 + 1 \cdot 812, && 899 = 1 \cdot 812 - 87, \\
(3) = (1) - (2): &\quad 87 = 1 \cdot 899 - 1 \cdot 812, && 812 = 9 \cdot 87 - 29, \\
(4) = (2) - 9(3): &\quad 29 = -9 \cdot 899 + 10 \cdot 812, && 87 = 3 \cdot 29 + 0, \\
(5) = (3) - 3(4): &\quad 0 = 28 \cdot 899 - 31 \cdot 29.
\end{aligned}$$

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

- 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.

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.*

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.

Rešujemo enačbo

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

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

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. 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 $\gcd(a, b) | c$.

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

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.

- Eno rešitev LDE dobimo tako, da *predzadnjo* vrstico REA pomnožimo s kvocientom desne strani in gcd koeficientov.
- Vse druge rešitve dobimo tako, da prištejemo k-kratnik zadnje vrstice REA.

Primer

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

$$\begin{aligned}
(1): &\quad 15 = 1 \cdot 15 + 0 \cdot 6, \\
(2): &\quad 6 = 0 \cdot 15 + 1 \cdot 6, && 15 = 2 \cdot 6 + 3, \\
(3) = (1) - 2(2): &\quad 3 = 1 \cdot 15 - 2 \cdot 6, && 6 = 2 \cdot 3 + 0, \\
(4) = (2) - 2(3): &\quad 0 = -2 \cdot 15 + 5 \cdot 6.
\end{aligned}$$

Ena rešitev enačbe je $(-6, 3)$. Vse rešitve so $(-6 + 5k, -6 - 2k)$ za $k \in \mathbb{Z}$.