

# Diskretne strukture

Gašper Fijavž

Fakulteta za računalništvo in informatiko  
Univerza v Ljubljani

2. december 2022

# 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  $m$

$r$  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 ima enačba  $n = x \cdot m$  **celoštevilsko** rešitev.

Če  $m, n$  nista enaka 0, potem lahko definiramo

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

*največji skupni delitelj* števil  $m$  in  $n$

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

*najmanjši skupni večkratnik* števil  $m$  in  $n$

$\gcd$  in  $\text{lcm}$  sta *komutativni* in *asociativni* operaciji.

## Razširjeni Evklidov Algoritem - REA

*Zgled:* Poišči  $\gcd(899, 812)$ .

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)

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

*Največji skupni delitelj  $\gcd(m, n)$  števil  $m$  in  $n$  dobimo kot zadnji neničelni **ostanek** v REA. Obenem  $\gcd(m, n)$  zapišemo tudi kot celoštevilsko linearno kombinacijo števil  $m$  in  $n$ .*

## 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:*  $89 \perp 81$

*Velja tudi:*  $5 \perp 7$ ,  $7 \perp 37$ ,  $37 \perp 101$ ,  $101 \perp 214$

$$\begin{array}{rclcl} (-4) \cdot 5 & + & 3 \cdot 7 & = & 1 \\ 16 \cdot 7 & + & (-3) \cdot 37 & = & 1 \\ (-30) \cdot 37 & + & 11 \cdot 101 & = & 1 \\ 89 \cdot 101 & + & (-42) \cdot 214 & = & 1 \end{array}$$

# Tuja števila

## Trditev

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

## Izrek

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

## 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 32,75€, kremna rezina stane 6,75€, torta pa 5,25€.

Vemo tudi, da so pojedli več tort kot kremnih rezin.



## Diofantske enačbe

Enačba je *diofantska*, če ima celoštevilske podatke in iščemo celoštevilske rešitve.

*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  $\gcd(a, b) \mid c$ .*

*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

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

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

kjer je  $t$  poljubno celo število, vse rešitve te diofantske enačbe.

# Diofantske enačbe

## Izrek

*Linearna diofantska enačba*

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \dots + a_n \cdot x_n = c$$

*je rešljiva natanko takrat, ko*

$$\gcd(a_1, a_2, \dots, a_n) \mid c.$$

# Praštevila

Naravno število  $n \geq 1$  je *praštevilo*, če ima natanko dva pozitivna delitelja.

Sicer je 1 ali pa *sestavljeno število*.

Praštevila do 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Par praštevil oblike  $(p, p + 2)$  imenujemo *praštevilska dvojčka*.

# Praštevila

## Trditev

- ▶  $p$  praštevilo in  $a \in \mathbb{Z}$ . Potem  $p|a$  ali  $p \perp a$ .
- ▶  $p$  praštevilo,  $a, b \in \mathbb{Z}$ . Če  $p|(a \cdot b)$ , potem  $p|a$  ali  $p|b$ .
- ▶ vsako naravno število  $n \geq 2$  je deljivo s katerim od praštevil.

Praštevil je neskončno mnogo

Izrek (Evklid)

*Obstaja neskončno mnogo praštevil.*

## Enolični razcep

### Izrek

*Vsako naravno število  $n \geq 2$  lahko zapišemo kot produkt praštevil.*

*Zapis je enoličen, če se ne oziramo na vrstni red faktorjev.*



## Eulerjeva funkcija $\varphi$

*Eulerjeva funkcija*  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  je definirana takole:

$$\varphi(n) = |\{k \in \mathbb{N} ; 1 \leq k \leq n \text{ in } k \perp n\}|$$

$\varphi(n)$  je število števil med 1 in  $n$ , ki so tuja  $n$ .

*Zgled:*

$$\varphi(4) = 2$$

1,2,3,4

$$\varphi(5) = 4$$

1,2,3,4,5

$$\varphi(6) = 2$$

1,2,3,4,5,6

## Kako računamo Eulerjevo funkcijo

### Trditev

Če je  $p$  praštevilo, je  $\varphi(p) = p - 1$ .

### Trditev

Če je  $p$  praštevilo, je  $\varphi(p^n) = p^n - p^{n-1}$ .

### Trditev

Če  $a, b \in \mathbb{N}$  in  $a \perp b$ , potem je  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ .

## Kako računamo Eulerjevo funkcijo

### Izrek

Naj bo  $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ , kjer so  $p_1, p_2, \dots, p_m$  različna praštevila. Potem je

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

# Kongruence

Naj bo  $a \in \mathbb{Z}$  in  $m \in \mathbb{N}$ ,  $m \geq 2$ .

$a \bmod m$

je ostanek  $a$ -ja pri deljenju z  $m$ .

Definirajmo relacijo, *kongruenco po modulu  $m$* , z naslednjim opisom:

$$a \equiv b \pmod{m} \text{ ntk. } m \mid (a - b) \text{ ntk. } a \bmod m = b \bmod m$$

## Lastnosti kongruenc

1. kongruenca po modulu  $m$  je ekvivalenčna relacija v  $\mathbb{Z}$
2. Če  $a \equiv b \pmod{m}$ , potem

$$a \pm c \equiv b \pm c \pmod{m}$$

$$a \cdot c \equiv b \cdot c \pmod{m}$$

$$a^n \equiv b^n \pmod{m}$$

3. Če  $a \equiv b \pmod{m}$  in  $c \equiv d \pmod{m}$ , potem

$$a \pm c \equiv b \pm d \pmod{m}$$

$$a \cdot c \equiv b \cdot d \pmod{m}$$

4. Če  $a \cdot c \equiv b \cdot c \pmod{m}$  in  $c \perp m$ , potem  $a \equiv b \pmod{m}$

# Zgledi

*Zgledi:*

- ▶ Izračunaj ostanek pri deljenju števila  $3^{120}$  s 13.
- ▶ Izračunaj zadnjo cifro števila  $9^{8^{7^6}}$ .
- ▶ Izračunaj ostanek pri deljenju števila  $9^{8^{7^6}}$  z 11.

## Rezultati

### Izrek (Eulerjev)

Naj bo  $a \in \mathbb{Z}$ ,  $m \geq 2 \in \mathbb{N}$  in  $a \perp m$ . Potem je

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

### Izrek (mali Fermatov)

Če je  $p$  praštevilo in  $a \perp p$ , potem je

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Za vse  $a \in \mathbb{Z}$  pa velja

$$a^p \equiv a \pmod{p}.$$

# RSA kriptosistem

## Trditev

*Naj bosta  $p$  in  $q$  različni praštevili. Potem je*

$$a \equiv b \pmod{p} \quad \text{in} \quad a \equiv b \pmod{q}$$

*natanko tedaj, ko je*

$$a \equiv b \pmod{pq}.$$

## Trditev

*Naj bosta  $p$  in  $q$  različni praštevili. Potem za poljubni naravni števili  $a$  in  $k$  velja*

$$a^{k \cdot \varphi(pq) + 1} \equiv a^{k \cdot (p-1)(q-1) + 1} \equiv a \pmod{pq}$$



# RSA kriptosistem

RSA kriptosistem deluje na principu *javnih* in *privatnih ključev*.

Pogovarjajmo se o dveh uporabnikih *Ančki* in *Borutu*. Vsak izmed njiju ima svoj *privatni ključ*  $P_A$ ,  $P_B$ , ki ga hrani na skrivnem mestu, svoj *javni ključ*  $J_A$ ,  $J_B$  da na vpogled vsem.

## RSA kriptosistem

Komunikacija med Ančko in Borutom:

- ▶ Ančka bi rada Borutu posredovala sporočilo  $x$ :

$$x, J_B(x) \xrightarrow{!} J_B(x), P_B(J_B(x)) = x$$

- ▶ Ančka bi rada Borutu posredovala sporočilo  $x$  in Borut bi rad bil prepričan, da mu je sporočilo res posredovala Ančka:

$$x, P_A(x), J_B(P_A(x)) \xrightarrow{!}$$

$$\xrightarrow{!} J_B(P_A(x)), P_B(J_B(P_A(x))) = P_A(x), J_A(P_A(x)) = x$$

Veljati mora:

1.  $P_A$  in  $J_A$  kot tudi  $P_B$  in  $J_B$  sta *inverzni preslikavi*.
2. Če poznamo  $J_A$  iz tega ne moremo (vsaj ne enostavno) izračunati  $P_A$ .

