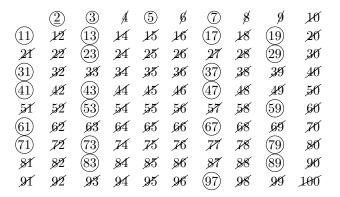
# Osnove teorije brojeva

## 1 Djeljivost

- Ako postoji  $q = \frac{b}{a}$  gdje je q cijeli broj  $(q \in \mathbb{Z})$ , onda je b cjelobrojno djeljiv sa a
- Za a se kaže da je **djelilac** od b i zapisuje se  $a \mid b$  za b se kaže da je **sadržilac** od a
- Ako b nije cjelobrojno djeljiv sa a, zapisuje se  $a \nmid b$
- Ako postoji  $q \cdot a = b \wedge q \in \mathbb{Z}$ , za q se kaže da je **komplementarni djelilac**
- Akko<sup>1</sup> postoji q tako da je b = aq + r onda se r zove **ostatkom** cjelobrojnog djeljenja i  $0 \le r \le |b|$  Ostatak djeljenja b sa a se zapisuje mod(b, a)

#### 2 Prosti brojevi

- Svi prirodni brojevi p > 1, koji su djeljivi sa 1 i sa samim sobom, zovu se **prosti brojevi**. Oni koji imaju još djelilaca su **složeni** brojevi.
- Prosti brojevi imaju posebnu primjenu u kriptografiji. Pronalazak prostih brojeva od 1 do n se može obaviti koristeći algoritam **Eratostenovo sito**:
  - 1. Napisati brojeve od 2 do n
  - 2. Zaokružiti najmanji neprekriženi broj, te prekrižiti sve brojeve koje je moguće cjelobrojno podijeliti odabranim brojem
  - 3. Ponoviti prethodni korak sve dok svi brojevi u tablici nisu zaokruženi ili prekriženi npr. Pronaći sve proste brojeve od 1 do 100:



 $<sup>^1 {\</sup>rm akko}$ — ako i samo ako

### 3 Najveći zajednički djelilac (GCD)

- Ako je  $\mathcal{D}$  skup svih zajedničkih djelilaca brojeva  $a_1, a_2, a_3, ..., a_n$  onda je najveći od njih, **najveći zajednički djelilac** ili GCD greatest common divisor
- Ako je  $GCD(a_1, a_2, a_3, ..., a_n)=1$  onda su oni **uzajamno prosti**
- Za GCD vrijedi GCD $(a_1,a_2,a_3,...,a_n)$ =GCD $(GCD(a_1,a_2,...,a_{n-1}),a_n)$  za  $n\geq 2$
- Za pronalazak GCD-a se koristi **Euklidov algoritam** koji glasi: GCD(a,b) = GCD(b,mod(a,b)) gdje vrijedi mod(a,b) < b i GCD(a,0) = a

Primjer: Pronaći najveći zajednički djelilac 210 i 76.

$$210 = 2 \cdot 76 = 56$$

$$76 = 1 \cdot 58 + 18$$

$$58 = 3 \cdot 18 + 4$$

$$18 = 4 \cdot 4 + 2$$

$$4 = 2 \cdot 2 + 0$$

Tako je 2 najveći zajednički djelilac brojeva 210 i 76.

# 4 Najmanji zajednički sadržilac (LCM)

• Ako imamo dva broja 2 i 3, onda su njihovi sadržioci:

$$2 := 2, 4, 6, 8, 10, 12, 14, 16, 18, \dots$$
  
 $3 := 3, 6, 9, 12, 15, 18, \dots$ 

- U ovom primjeru, 6, 12, 18, ... su sadržioci brojeva 2 i 3 te je **najmanji zajednički sadržilac** (LCM least common multiplier) je najmanji od njih, tj. 6
- Tačnije, s obzirom da je  $GCD(a_1, a_2, a_3, ..., a_n) = GCD(GCD(a_1, a_2, ..., a_{n-1}), a_n)$  za  $n \ge 2$  onda, LCM možemo pronaći koristeći GCD:

$$LCM(a, b) = \frac{|a \cdot b|}{GCD(a, b)}$$

Primjer: Pronaći najmanji zajednički sadržilac brojeva 1050, 735, 392.

$$\begin{split} \text{LCM}(1050, 735, 392) &= \text{LCM}(\text{LCM}(1050, 735), 392) = \text{LCM}(\frac{1050 \cdot 735}{\text{GCD}(1050, 735)}, 392) \\ &\text{pošto je GCD}(1050, 735) = ... = 105, \text{ onda} \\ &\text{LCM}(\frac{1050 \cdot 735}{105}, 392) = \text{LCM}(7350, 392) = \frac{7350 \cdot 392}{\text{GCD}(7350 \cdot 392)} = \frac{2881200}{98} = 29400 \end{split}$$

# 5 Ponavljanje

- 1. Pronaći sve proste brojeve između 20 i 50?
- 2. Koristeći Euklidov algoritam pronaći najveći zajednički djelilac u sljedećim slučajevima:
  - (a) 45 i 100
  - (b) 26 i 234
  - (c) 180, 225 i 270
  - (d) 7469 i 2464
  - (e) 2947 i 3997
- 3. Pronaći najmanji zajednički sadržilac:
  - (a) 30 i 40
  - (b) 20 i 30
  - (c) 35, 42, 50