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[1] postoji q tako da je $b = aq + r$ onda se r zove **ostatkom** cjelobrojnog djeljenja i $0 \leq r \leq |b|$
  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:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

[1] 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.

$$
\begin{aligned}
210 &= 2 \cdot 76 = 56 \\
76 &= 1 \cdot 58 + 18 \\
58 &= 3 \cdot 18 + 4 \\
18 &= 4 \cdot 4 + 2 \\
4 &= 2 \cdot \underline{2} + 0
\end{aligned}
$$

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:

$$
\begin{aligned}
2 &:= 2, 4, \mathbf{6}, 8, 10, \mathbf{12}, 14, 16, \mathbf{18}, ... \\
3 &:= 3, \mathbf{6}, 9, \mathbf{12}, 15, \mathbf{18}, ...
\end{aligned}
$$

- 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 $n \geq 2$ onda, LCM možemo pronaći koristeći GCD:

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

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

$$\mathrm{LCM}(1050, 735, 392) = \mathrm{LCM}(\mathrm{LCM}(1050, 735), 392) = \mathrm{LCM}(\frac{1050 \cdot 735}{\mathrm{GCD}(1050,735)}, 392)$$

$$\text{pošto je } \mathrm{GCD}(1050, 735) = ... = 105, \text{ onda}$$

$$\mathrm{LCM}(\frac{1050 \cdot 735}{105}, 392) = \mathrm{LCM}(7350, 392) = \frac{7350 \cdot 392}{\mathrm{GCD}(7350 \cdot 392)} = \frac{2881200}{98} = 29400$$

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