4 Elementarna teorija brojeva

Skup cijelih brojeva:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Definicija. Neka su a, $b \in \mathbb{Z}$. Kažemo da cijeli broj a dijeli cijeli broj b i pišemo $a \mid b$ ako postoji cijeli broj k takav da je $b = a \cdot k$. Simbolima to zapisujemo ovako: za a, $b \in \mathbb{Z}$

$$a \mid b \overset{def}{\Leftrightarrow} (\exists k \in \mathbb{Z})(b = a \cdot k).$$

Svojstva dijeljenja

(i) $(\forall a \in \mathbb{Z})(a \mid a)$ (refleksivnost)

(ii) $(\forall a, b, c \in \mathbb{Z})(a \mid b \wedge b \mid c \Rightarrow a \mid c)$ (tranzitivnost)

Je li $\mid$ na $\mathbb{Z}$ relacija ekvivalencije? Ne, jer nije simetrična, tj.

$$(\exists a, b \in \mathbb{Z})(a \mid b \wedge b \nmid a),$$

na primjer $2 \mid 4$, ali $4 \nmid 2$.

(iii) $(\forall a, b \in \mathbb{Z})(a \mid b \wedge b \mid a \Rightarrow a = b \vee a = -b)$

(iv) $(\forall a, b, c \in \mathbb{Z})(a \mid b \wedge a \mid c \Rightarrow a \mid b + c)$

(v) $(\forall a, a', b, b' \in \mathbb{Z})(a \mid b \wedge a' \mid b' \Rightarrow aa' \mid bb')$

(vi) $(\forall a, b \in \mathbb{Z})(a \mid b \Rightarrow (\forall c \in \mathbb{Z})(a \mid b \cdot c))$.

Dokažite ta svojstva.

Teorem. (o dijeljenju s ostatkom) Neka su a, $b \in \mathbb{Z}$ i $b > 0$. Tada postoje jedinstveni q, $r \in \mathbb{Z}$ takvi da je

$$a = b \cdot q + r$$

$$0 \leq r < b.$$

Definicija. Neka su a, $b \in \mathbb{Z}$. *Najveća zajednička mjera* brojeva a i b je najveći broj koji dijeli a i b. Oznaka: $M(a, b)$.

Definicija. Za brojeve a, $b \in \mathbb{Z}$ kažemo da su *relativno prosti* ako je $M(a, b) = 1$.

Najveća zajednička mjera (n.z.m.) uvijek postoji. Nalazimo je Euklidovim algoritmom.

Primjer. Izračunajmo $M(420, 195)$ Euklidovim algoritmom.

Zadatak 1. Neka su a, $b \in \mathbb{Z}$ i neka je d najmanji pozitivni broj oblika $ax + by$, gdje su x, $y \in \mathbb{Z}$. Dokažite da je $d = M(a, b)$.

Karakterizacija najveće zajedničke mjere. Neka su a, $b \in \mathbb{Z}$. Prirodan broj d je najveća zajednička mjera brojeva a i b ako i samo ako vrijedi: $d \mid a$, $d \mid b$ i svaki cijeli broj d' koji dijeli a i b dijeli nužno i d. Simbolima: $d = M(a, b)$ ako i samo ako

- $d \mid a \wedge d \mid b$ (d je zajednička mjera od a i b)
- $(\forall d' \in \mathbb{Z})(d' \mid a \wedge d' \mid b \Rightarrow d' \mid d)$ (d je djeljiv svakom zajedničkom mjerom od a i b)
- $d \in \mathbb{N}$ (radi jedinstvenosti).

Zadatak 2. Izračunajte najveću zajedničku mjeru brojeva $2^{2004} - 1$ i $2^{2002} - 1$.

Zadatak 3. Dokažite sljedeće tvrdnje:

(a) $M(a, b) = M(-a, b) = M(a, -b) = M(-a, -b)$

(b) $M(a, b) = M(a, a + b)$

(c) $M(a, b) = M(a, a - b)$

(d) $M(na, nb) = n \cdot M(a, b)$.

Zadatak 4. Dokažite da su za svaki prirodni broj n brojevi $28n + 10$ i $8n + 3$ relativno prosti.

Definicija. Neka je n prirodan broj. Definiramo relaciju *kongruencija modulo* n na skupu $\mathbb{Z}$ sa

$$a \equiv b \,(\mathrm{mod}\ n) \overset{def}{\Leftrightarrow} n \mid a - b.$$

Zadatak 5. Dokažite da je relacija $\equiv (\mathrm{mod}\ n)$ relacija ekvivalencije i odredite njene klase ekvivalencije.

Zadatak 6. Dokažite da iz

$$a_1 \equiv b_1 \,(\mathrm{mod}\ n)$$
$$a_2 \equiv b_2 \,(\mathrm{mod}\ n)$$

slijedi

$$a_1 + a_2 \equiv b_1 + b_2 \,(\mathrm{mod}\ n)$$
$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \,(\mathrm{mod}\ n).$$

Zadatak 7. Dokažite da je zbroj kubova triju uzastopnih cijelih brojeva djeljiv s 9.

Zadatak 8. Dokažite da nijedan član niza

$$a_n = 4^n + \frac{5 + (-1)^n}{2}$$

nije kvadrat prirodnog broja.

Zadatak 9. Neka su a, b, $c \in \mathbb{Z}$ takvi da je

$$a^n + nb + c \equiv 0 \,(\mathrm{mod}\ m)$$

za $n = 1, 2, 3$. Dokažite da je b^2 višekratnik od m.

Zadatak 10. Dokažite da je $mn(m^6 - n^6)$ djeljivo s 21 za sve $n, m \in \mathbb{N}$.

DZ Dokažite da je za sve $n \in \mathbb{N}$ broj $n^3 - n$ djeljiv s 3, a broj $n^5 - n$ djeljiv s 5.

Prosti brojevi

Definicija. Prirodan broj $p \neq 1$ je *prost* ako nema drugih djelitelja u skupu $\mathbb{N}$ osim broja 1 i samog sebe.

Dokažimo sljedeće tvrdnje.

♢ Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva.

♢ Prostih brojeva ima beskonačno mnogo. (Euklidov dokaz.)

Propozicija. Ako je broj n složen, onda postoji njegov djelitelj koji je $\leq \sqrt{n}$.

Zadatak 11. Dokažite:

(a) Ako su p i $8p - 1$ prosti brojevi, onda je $8p + 1$ složen broj.

(b) Ako su p i $8p^2 + 1$ prosti brojevi, onda je $8p^2 - 1$ prost broj.

Uputa: promatrajte djeljivost tih brojeva s 3.

Zadatak 12. Za koje proste brojeve p, q, r vrijedi jednakost $p^q = r - 1$?

Zadatak 13. Dokažite da ostatak pri dijeljenju prostorg broja s 30 ne može biti složen broj.

Zadatak 14. Dokažite da postoji beskonačno mnogo prostih brojeva oblika $4m + 3$, gdje je $m \in \mathbb{N}_0$.

Eulerova funkcija

Definicija. *Eulerova funkcija* $\phi\colon \mathbb{N} \to \mathbb{N}$ definirana je sa: $\phi(n)$ je broj brojeva između 1 i n koji su relativno prosti s n, tj.

$$\phi(n) := \operatorname{card}\{k \in \{1, 2, \ldots, n\} \mid M(k, n) = 1\}.$$

Primjer. Vrijednost Eulerove funkcije za $n = 1, 2, \ldots, 9$.

Teorem. Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ rastav broja n na proste faktore. Tada vrijedi

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

to jest

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Teorem. Eulerova funkcija je *multiplikativna*, tj. za sve relativno proste m, $n \in \mathbb{N}$ vrijedi

$$\phi(mn) = \phi(m)\phi(n).$$

Zadatak 16. Riješite jednadžbu $\phi(7^x) = 294$.

Zadatak 17. Riješite jednadžbu $\phi(x) = 100$.

Teorem. (Eulerov teorem) Ako je $M(a, n) = 1$, onda je

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Korolar. (Mali Fermatov teorem) Ako je p prost i $p \nmid a$, onda je

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

Zadatak 18. Odredite ostatak pri dijeljenju broja $1^{30} + 2^{30} + \ldots 10^{30}$ brojem 11.

Zadatak 19. Dokažite da je za svaki prost broj p i svaki prirodan broj k suma

$$1 + 1^{k(p-1)} + 2^{k(p-1)} + \ldots + p^{k(p-1)}$$

djeljiva s p.

Zadatak 20. Dokažite da je za svaki prirodan broj n koji nije djeljiv s 4 zbroj

$$1^n + 2^n + 3^n + 4^n$$

djeljiv s 5.

Zadatak 21. Odredite ostatak pri dijeljenju broja

$$7^{1998^{1997}} - 3^{1998^{1997}}$$

brojem 10.

Zadatak 22. Dokažite da je broj $2222^{5555} + 5555^{2222}$ djeljiv sa 7.

Zadatak 23. Odredite ostatak pri dijeljenju broja $140^{67} + 153^{51}$ brojem 17.

Zadatak 24. Dokažite da $7 \mid 3^{2n+1} + 2^{n+2}$ za svaki $n \in \mathbb{N}$.

Zadatak 25. Odredite ostatak pri dijeljenju $3^{105} + 4^{105}$ brojem 13.

Zadatak 26. Odredite ostatak pri dijeljenju 2006^{2007} s 13.

Zadatak 27. Dokažite da je $n(2n+1)(7n+1)$ djeljiv sa 6 za svaki $n \in \mathbb{Z}$.

Zadatak 28. Dokažite da za svaki prost broj p vrijedi

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$