Uvod u teoriju brojeva

Borka Jadrijević

PREDAVANJA i VJEŽBE: ponedjeljak, 8 – 10
srijeda, 8 – 10

KONZULTACIJE: srijeda, 10:00 – 11:00
četvrtak, 10:00 – 11:00

Sadržaj:

1. **Djeljivost**
2. **Kongruencije**
3. **Kvadratni ostaci**
4. **Kvadratne forme**
5. **Aritmetičke funkcije**
6. **Diofantske aproksimacije**
7. **Diofantske jednadžbe**
8. **Kvadratna polja**

Literatura:

- http://www.fesb.hr/~borka/UTB.htm;
- Andrej Dujella, *Uvod u teoriju brojeva,* skripta (PMF-MO), http://web.math.hr/~duje/utb/utblink.pdf;
- D. Veljan, *Kombinatorna i diskretna matematika*,

Algoritam, Zagreb, 2001

Obveze:

- predavanja ($\geq 70\%$)
- vježbe ($\geq 70\%$)

Provjere znanja:

- *dva kolokvija:*

- oba pozitivna
- zadaci ($\geq 45\%$) i teoretska pitanja ($\geq 45\%$)

- *ispit:*

- pismeni i usmeni.

0. Uvod

Aritmetika (računstvo) je grana matematike koja se bavi brojevima.

Danas je češći naziv za aritmetiku **teorija brojeva.**

Teorija brojeva (klasična) se bavi ponajprije prirodnim brojevima, te cijelim i racionalnim brojevima.

Skup prirodnih brojeva označavamo sa

$$\mathbb{N} = \{1, 2, 3, ..., n, ...\}.$$

Neka svojstva skupa $\mathbb{N}$ koja ćemo koristiti:

- Na skupu $\mathbb{N}$ su definirane operacije zbrajanja i množenja koje zadovoljavaju svojstva komutativnosti, asocijativnosti i distributivnosti;
- Na skupu $\mathbb{N}$ imamo uređaj takav da za svaka dva različita elementa $m, n \in \mathbb{N}$ vrijedi ili $m < n$ ili $n < m$;
- Svaki neprazan podskup skupa $\mathbb{N}$ ima najmanji element i vrijedi princip matematičke indukcije;

1. Djeljivost

Definicija 1.1 Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da a *dijeli* b, odnosno da je b *djeljiv* s a ako postoji cijeli broj x takav da je $b = ax$.

To zapisujemo sa $a \,|b$. Broj a nazivamo *djelitelj* broja b, a broj b *višekratnik* broja a.

Ako b nije djeljiv s a onda pišemo $a \nmid b$. Oznaku $a^k \,||b$ ćemo koristiti kada $a^k \,|b$ i $a^{k+1} \nmid b$.

Zadatak 1.1 Pokažite da relacija "dijeliti" na skupu $\mathbb{Z}$ ima sljedeća svojstva:

- za svaki cijeli broj a, $a \neq 0$, vrijedi $a \,|a$;
- za svaka dva cijela broja a i b vrijedi: ako $a \,|b$ i $b \,|a$ onda je $a = \pm b$. Ako su $a, b \in \mathbb{N}$, onda je $a = b$;
- za svaka tri cijela broja a,b, c vrijedi: ako $a \,|b$ i $b \,|c$ onda $a \,|c$.

Zadatak 1.2 Ako su $a, b, c \in \mathbb{Z}$, onda iz $a \,|b$ i $a \,|c$ slijedi $a \,|(nb + mc)$ za bilo koja dva cijela broja m i n.

Teorem 1.1 (o dijeljenju s ostatkom) Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

Dokaz:

Definicija 1.2 . Broj $d \in \mathbb{Z}$ nazivamo *zajedničiki djelitelj* od a i b ako $d \,|a$ i $d \,|b$.

Ako je barem jedan od brojeva a i b različit od nule, onda postoji konačno mnogo zajedničikih djelitelja od a i b i najveći među njima nazivamo *najveći zajednički djelitelj* od a i b i označavamo sa

$$\gcd(a, b)$$

Uočimo: $\gcd(a, b) \geq 1$.

Na sličan način definiramo najveći zajednički djelitelj za bilo koji konačan skup cijelih brojeva $a_1, a_2, ..., a_n$, a označavamo ga sa $\gcd(a_1, a_2, ..., a_n)$.

Teorem 1.2 Neka su $a, b \in \mathbb{Z}$ i barem jedan od brojeva a i b je različit od nule. Neka je

$$S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je

$$\gcd(a, b) = \min S.$$

Dokaz:

Uočimo: Ako se cijeli broj d može prikazati u obliku

$$d = ax + by,$$

onda je $\gcd(a, b)$ djelitelj od d. Posebno, ako je $ax + by = 1$, onda je $\gcd(a, b) = 1$.

Definicija 1.3 Kažemo da su cijeli brojevi a i b *relativno prosti*, ako je $\gcd(a, b) = 1$.

Za cijele brojeve $a_1, a_2, ..., a_n$ kažemo da su *relativno prosti* ako je $\gcd(a_1, a_2, ..., a_n) = 1$, a da su *u parovima relativno prosti* ako je $\gcd(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.

Propozicija 1.1 Neka su $a, b, m \in \mathbb{Z}$. Ako je $\gcd(a, m) = \gcd(b, m) = 1$, onda je $\gcd(ab, m) = 1$.

Dokaz:

Propozicija 1.2 Neka su $a, b \in \mathbb{Z}$, tada je

$$\gcd(a, b) = \gcd(a, b + ax)$$

za svaki $x \in \mathbb{Z}$.

Dokaz:

Teorem 1.3 (Euklidov algoritam) Neka su dani $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema 1.1 dobiven niz jednakosti

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \qquad (*) \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1} \\
r_{k-1} &= r_k q_{k+1}.
\end{aligned}$$

Tada je $\gcd(a, b) = r_k$, tj. $\gcd(a, b)$ jednako je posljednjem ostatku različitom od 0. Brojevi $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$\gcd(a, b) = r_k = ax_0 + by_0, \qquad (**)$$

mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od a i b.

Dokaz:

Napomena:

- U Euklidovom algoritmu smo pretpostavili da je $b > 0$ što nije bitno ograničenje jer je $\gcd(a, b) = \gcd(|a|, |b|)$;

- Ako su $a, b \in \mathbb{N}$ i $a < b$, onda u prvom koraku imamo $a = b \cdot 0 + a$, pa a i b zamijene mjesta;

- Primijetimo da je (konačan) niz ostataka u (*) $r_0 = b$, $r_1, r_2, ..., r_k$ strogo padajući niz;
- Primijetimo da je

$$\left\lfloor \frac{a}{b} \right\rfloor = q_1, \qquad \left\lfloor \frac{b}{r_1} \right\rfloor = q_2, \qquad \left\lfloor \frac{r_1}{r_2} \right\rfloor = q_3 \ \ ...,$$

  gdje je $\lfloor x \rfloor$ *najveći cijeli dio* od x, tj. $\lfloor x \rfloor = q$, gdje je q najveći cijeli broj $\leq x$.

- Brojevi $x_0, y_0 \in \mathbb{Z}$ u (**) nisu jednoznačno određeni, jer je npr.

$$\gcd(a, b) = ax_0 + by_0 = (x_0 + b)\, a + (y_0 - a)\, b,$$

Primjer 1.1 Odredimo $d = \gcd(252, 198)$ i prikažimo d kao linearnu kombinaciju brojeva 252 i 198.

Rješenja jednadžbe $\gcd(a,b) = ax + by$, mogu se dobiti iz (*) na sljedeći način: Ako je

$$\begin{aligned} r_{-1} &= a, \quad r_0 = b, \quad r_i = r_{i-2} - q_i r_{i-1} \\ x_{-1} &= 1, \quad x_0 = 0, \quad x_i = x_{i-2} - q_i x_{i-1} \\ y_{-1} &= 0, \quad y_0 = 1, \quad y_i = y_{i-2} - q_i y_{i-1} \end{aligned}$$

onda je

$$ax_i + by_i = r_i, \quad \text{za } i = -1, 0, 1, ..., r+1.$$

Formula je točna za $i = -1$ i $i = 0$, pa tvrdnju dobivamo indukcijom (sami). Posebno je

$$ax_k + by_k = r_k.$$

Primjer 1.2 Odredimo $d = \gcd(3587, 1819)$ i prikažimo d kao linearnu kombinaciju brojeva 3587 i 1819.

Zadatak 1.4 Odredite cijele brojeve x i y (ako postoje) takve da je

a) $71x + 50y = 1$, b) $93x + 81y = 3$ c) $93x + 81y = 5$.

Jednadžbu oblika

$$ax + by = d, \tag{1}$$

gdje su a, b, d zadani cijeli brojevi kojoj tražimo cjelobrojna rješenja x i y je primjer *diofantske jednadžbe*.

Zadatak 1.5 Neka su $a, b, d \in \mathbb{Z}$ zadani cijeli brojevi. Diofantska jednadžba (1) ima rješenje onda i samo onda ako $\gcd(a, b) \,|d$.

Propozicija 1.3 Za broj koraka k u Euklidovom algoritamu vrijedi $k < 2 \log_2 b$.

Dokaz:

Zadatak 1.3 Uz oznake od prije, dokažite da za $i = 0, 1, ..., r + 1$ vrijedi

$$x_{i-1}y_i - x_i y_{i-1} = (-1)^i,$$

te $\gcd(x_i, y_i) = 1$.

Propozicija 1.4 Uz oznake od prije, vrijedi

$$|x_k| \leq \frac{b}{2g} \quad \text{i} \quad |y_k| \leq \frac{b}{2g},$$

gdje je $\gcd(a, b) = g$.

Uočimo: Svaki prirodan broj $a > 1$ ima uvijek dva djelitelja 1 i a i njih nazivamo *trivijalni djelitelji*.

Definicija 1.4

- Za prirodan broj $p > 1$ kažemo da je *prost broj* (ili *prim broj*) ako nema niti jednog djelitlja d takvog da je $1 < d < p$, tj. ako ima samo trivijalne djelitelje;
- Prirodan broj $a > 1$ koji nije prost nazivamo *složen broj*.

Primjer 1.3 Prvi prosti brojevi su: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

Ako želimo naći sve proste projeve $\leq a$, koristimo jednostavni postupak kojeg nazivamo **Eratostenovo sito:**

- Ispišemo, po redu, sve prirodne brojeve od 1 do a;
- Križamo 1;
- Zaokružimo 2 (prost) i križamo sve prave višekratnike od 2;
- Prvi preostali 3 (prost) zaokružimo i križamo sve prave višekratnike od 3 (koji nisu već prekriženi);
- Prvi preostali 5 (prost) zaokružimo i križamo sve prave višekratnike od 5 (koji nisu već prekriženi);
- ....

- Algoritam završava u konačno koraka, a zaokruženi brojevi su prosti.

Zadatak 1.4 Nađimo sve proste brojeve ≤ 60 pomoću Eratostenovog sita.

1	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

Teorem 1.4 Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).

Dokaz:

Iz Teorema 1.4 slijedi: Za svaki prirodan broja n postoji prikaz u obliku

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}, \tag{2}$$

gdje su $p_1, p_2, ..., p_k$ svi različiti prosti brojevi i $\alpha_1, ..., \alpha_k \in \mathbb{N}$. Broj $\alpha_i \in \mathbb{N}$ nazivamo *kratnošću* prostog broja p_i, a prikaz (2) *kanonski rastav* broja n na proste faktore.

Propozicija 1.5 Ako je p prost broj i $p \,|ab$, onda $p \,|a$ ili $p \,|b$. Općenitije, ako $p \,|a_1 a_2 ... a_k$, onda postoji barem jedan a_i takav da $p \,|a_i$.

Dokaz:

Teorem 1.5 (Osnovni teorem aritmetike) Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Dakle, iz Teorema 1.4 i Teorema 1.5 slijedi da postoji jedinstven zapis (rastav) prirodnog broja $n > 1$ oblika

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k},$$

gdje su $p_1 < p_2 < ... < p_k$ svi prosti faktori od n i $\alpha_1, ..., \alpha_k \in \mathbb{N}$. Često pišemo

$$n = \prod_{p-prost} p^{\alpha(p)},$$

gdje je $\alpha\,(p) \geq 0$ i $\alpha\,(p) = 0$ za gotovo sve proste brojeve.

Ako je $n = 1$, onda su svi $\alpha\,(p) = 0$.

Neka su $a, b, c \in \mathbb{N}$,

$$a = \prod_p p^{\alpha(p)}, \quad b = \prod_p p^{\beta(p)}, \quad c = \prod_p p^{\gamma(p)}.$$

Ako je

$$ab = c,$$

tada je po Teoremu 1.5

$$\alpha(p) + \beta(p) = \gamma(p) \quad \text{za sve } p.$$

Dakle, ako

$$a \mid c,$$

tada je

$$\alpha(p) \leq \gamma(p) \quad \text{za sve } p.$$

Obrnuto, ako je

$$\alpha(p) \leq \gamma(p) \quad \text{za sve } p,$$

definiramo prirodan broj $b = \prod_p p^{\beta(p)}$, gdje je $\beta(p) = \gamma(p) - \alpha(p)$ za sve p. Tada je

$$ab = c, \text{ tj. } a \mid c.$$

Zaključujemo:

$$a \mid c \quad \Leftrightarrow \quad \alpha(p) \leq \gamma(p) \quad \text{za sve } p. \tag{3}$$

Posljedica od (3):

$$\gcd(a,b) = \prod_p p^{\min\{\alpha(p),\beta(p)\}} \tag{4}$$

Definicija 1.5 Ako su cijeli brojevi a i b različiti od 0, onda najmanji prirodan c broj takav da $a \,|c$ i $b \,|c$ nazivamo *najmanji zajednički višekratnik* od a i b i označavamo sa $\operatorname{lcm}(a,b)$.

Na sličan način definiramo najveći zajednički višekratnik za bilo koji konačan skup cijelih brojeva a_1, $a_2, ..., a_n$, a označavamo ga sa $\operatorname{lcm}(a_1, a_2, ..., a_n)$.

Iz (3) slijedi:

$$\operatorname{lcm}(a,b) = \prod_p p^{\max\{\alpha(p),\beta(p)\}} \tag{5}$$

Propozicija 1.6 Neka su a i b cijeli brojevi, tada je

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|.$$

Dokaz:

Zadatak 1.5 Odredite

a) $\operatorname{lcm}(482, 1687)$ b) $\operatorname{lcm}(1400, 2420)$.

Definicija 1.6

- Kažemo da je prirodan broj a *(potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$;
- Kažemo da je prirodan broj a *kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a;

Uočimo: Neka je $a = \prod_p p^{\alpha(p)} \in \mathbb{N}$. Iz Teorema 1.5 slijedi:

- a potpun kvadrat $\Leftrightarrow \alpha(p)$ paran za sve p;
- a kvadratno slobodan $\Leftrightarrow \alpha(p) = 0$ ili $\alpha(p) = 1$ za sve p;
- ako je p prost, onda je: $p^k \| a \Leftrightarrow k = \alpha(p)$.

Zadatak 1.6 Nađite prirodan broj n sa svojstvom da je $\frac{n}{2}$ kvadrat, $\frac{n}{3}$ kub, a $\frac{n}{5}$ peta potencija nekog prirodnog broja.

Zadatak 1.7 Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Uočimo: U Primjeru 1.3 (Eratostenovo sito) algoritam je gotov već nakon križanja višekratnika od 7 jer je $\sqrt{60} < 11$.

Teorem 1.6 (Euklid) Skup svih prostih brojeva je beskonačan.

Dokaz:

Primjer 1.4 Dokažimo da prostih brojeva oblika $4k+3$ ima beskonačno mnogo.

Primjer 1.5 Dokažimo da za svaki realan broj $y \geq 2$ vrijedi

$$\sum_{p \leq y} \frac{1}{p} > \ln \ln y - 1.$$

Iz ovoga direktno slijedi da red $\sum_{p-prost} \frac{1}{p}$ divergira, što je još jedan dokaz da prostih brojeva ma beskonačno mnogo.

Napomena: Ako za $x \in \mathbb{R}$ sa $\pi(x)$ označimo broj prostih brojeva koji su $\leq x$, onda je[1]

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{(Prime Number Theorem -PNT).}$$

Ovo je prvi naslutio Gauss, a dokazali su neovisno Hadamar i de la Vallée Poussin 1896.

[1] Neka su $f, g : S \to \mathbb{R}$, $S \subseteq \mathbb{R}$. Pišemo:

$$f(x) \sim g(x) \text{ ako je } \lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

Još bolja aproksimacija je

$$\pi(x) \sim li(x),$$

gdje je

$$li(x) = \int_2^x \frac{dt}{\ln t} \quad \textit{- logaritamsko-integralna funkcija.}$$

Primjer 1.6 Dokažimo da za svaki prirodan broj n postoji n uzastopnih složenih brojeva.

Primjer 1.7 Dokažimo da ne postoji polinom $f(x)$ stupnja ≥ 1 s cjelobrojnim koeficijentima, takav da je $f(n)$ prost za svaki prirodan broj n.

Problem: Odrediti polinome $f(x)$ stupnja ≥ 1 s cjelobrojnim koeficijentima, takave da je $f(n)$ prost za beskonačno prirodnih brojeva n.

- Zna se da to vrijedi za polinome oblika $f(x) = ax + b$, $\gcd(a, b) = 1$ (Dirihletov teorem o prostim brojevima u aritmetičkom nizu);

- Za polinom $f(x) = x^2 + 1$ je to još otvoreno pitanje;

- Slutnja: to vrijedi za ireducibilne polinome f za koje ne postoji prirodan broj $d > 1$ takav da $d \,|\, f\,(n)$ za svaki $n \in \mathbb{N}$.

Primjer 1.7 Neka je broj $2^k + 1$ prost. Dokažimo da je tada $k = 0$ ili $k = 2^n$ za neki $n \in \mathbb{N}$.

Napomena: Brojevi oblika

$$f_n = 2^{2^n} + 1, \quad n \in \mathbb{N} \cup \{0\}$$

nazivaju se *Fermatovi brojevi*.

Fermat je mislio da su svi ovi brojevi prosti. Međutim.

$$f_0 = 3, \quad f_1 = 5, \quad f_2 = 17, \quad f_3 = 257, \quad f_4 = 65537$$

su prosti, ali je složen

$$f_5 = 2^{2^5} + 1 = 2^{32} + 1.$$

Slutnja: Samo je konačno mnogo Fermatovih brojeva prosto.

Zadatak 1.8 Dokažite da za $m \neq n$ vrijedi

$$\gcd\,(f_m, f_n) = 1.$$

Pokažite da ova činjenica povlači da prostih brojeva ima beskonačno mnogo.

Primjer 1.9 Neka je broj $2^n - 1$ prost. Dokažimo da je tada i n prost broj.

Napomena: Brojevi oblika

$$M_p = 2^p - 1, \quad p \text{ prost},$$

nazivaju se *Mersennovi brojevi*.

Neki Mersennovi brojevi su prosti, kao npr. $M_7 = 127$, a neki su složeni, kao npr. $M_{11} = 2047 = 23 \cdot 89$.

Slutnja: Beskonačno mnogo Mersennovi brojeva je prosto.

Napomena: Do danas je nađeno ukupno 47 Mersennovih prostih brojeva. Najveći među njima je našao Smith (2008.), a dobiven je za $p = 43112609$, ima $12\,978\,189$ znamenaka i to je ujedno najveći do sada pronađeni prost broj.