Algoritmi u teoriji brojeva

Cindrić, Filip

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Sveučilišni prijediplomski studij Matematika

Algoritmi u teoriji brojeva

Završni rad

Mentor:
prof. dr. sc. Ivan Matić

Student:
Filip Cindrić

Osijek, 2024.

Sadržaj

1 | Uvod

Teorija brojeva najraširenija je grana teorijske matematike koja ima mnoštvo svojih primjena. Kroz godine doživjela je razvoj do neslućenih razina te ju možemo vezati i uz druge grane matematike. Vrlo važno je napomenuti kako se njena materija može približiti i ljudima s vrlo malo matematičkog predznanja. Mnogi su matematičari zaslužni za razvoj teorije brojeva, a kao najznačajnije izdvajamo Euklida, jednog od najvećih grčkih matematičara Starog vijeka te Karla Friedricha Gaussa kojeg nazivamo ocem moderne teorije brojeva.
Unutar ovoga rada detaljnije ćemo obraditi teme:

- Euklidov algoritam
- Legendreov simbol
- Jacobijev simbol
- Gaussov kvadratni zakon reciprociteta.

Vidjevši teme koje ćemo obraditi, možemo reći kako ćemo fokus imati na djeljivosti i kvadratnim ostacima.
U prvom dijelu rada definirat ćemo i objasniti djeljivost te što nam predstavlja Euklidov algoritam, vidjeti princip njegova djelovanja te proučiti konkretan primjer.
U drugom dijelu rada proučavat ćemo zakonitosti kvadratnih ostataka. Naglasak stavljamo na proučavanje Legendreova simbola te njegova primjera, objasniti Jacobijev simbol te uz pomoć primjera pokazati njegovo djelovanje. Na poslijetku, proučavat ćemo Gaussov kvadratni zakon reciprociteta. Definirat ćemo ga, analizirati te kao i prethodne dijelove, uz pomoć primjera, lakše razumjeti.

2 | Djeljivost

Jedan od najjednostavnijih, ali i najvažnijih pojmova u teoriji brojeva je pojam djeljivosti. Kako bismo razmjeli daljnje metode u radu bitno je razumjeti ovaj pojam pa krenimo s njim u razmatranje.

Definicija 1 (vidjeti [3, str. 4]). *Uzmimo da su $t \neq 0$ i u cijeli brojevi. Kažemo da je u djeljiv s t, odnosno da t dijeli u, ako postoji cijeli broj x takav da je $u = tx$. Zapisat ćemo to kao $t \mid u$. Ako u nije djeljiv s t, onda pišemo $t \nmid u$.*
Ako $t \mid u$, onda još kažemo da je t djelitelj od u, te da je u višekratnik od t.

Primjer 1. *Kako je $4 = 2 \cdot 2$, očito $2 \mid 4$. Također $2 \mid -6$ jer je $-6 = -3 \cdot 2$.*
No, $2 \nmid 7$.

Teorem 1. *Idući teorem naziva se Teorem o dijeljenju s ostatkom. (vidjeti [3, str. 4]) Ako su odabrani proizvoljan prirodan broj t i cijeli broj u postoje jedinstveni cijeli brojevi q i r takvi da je $u = qt + r$, $0 \leq r < t$.*

Dokaz. Promotrimo skup $\{u - tm : m \in \mathbb{N}\}$. Najmanji nenegativni član ovog skupa označimo s r. Tada je po definiciji $0 \leq r < t$ i postoji $q \in \mathbb{Z}$ takav da je $u - qt = r$, tj. $u = qt + r$.
Jedinstvenost od q i r dokazujemo na sljedeći način. Pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete. Pokažimo najprije da je $r_1 = r$. Pretpostavimo da je npr. $r < r_1$. Tada je $0 < r_1 - r < t$, dok je s druge strane $r_1 - r = t(q - q_1) \geq t$. Prema tome je $r_1 = r$, pa je stoga i $q_1 = q$. □

Definicija 2 (vidjeti [1, str. 12]). *Uzimimo u i z cijele brojeve. Cijeli broj t koji dijeli oba broja u i z naziva se **zajednički djelitelj** brojeva u i z.*
*Ukoliko je barem jedan od brojeva u i z različit od nule, tada taj broj ima konačno mnogo djelitelja. U tom slučaju postoji i konačno mnogo zajedničkih djelitelja brojeva u i z. Najvećeg od njih (a taj je uvijek pozitivan) označavamo s (u, z). Broj (u, z) nazivamo **najveći zajednički djelitelj** brojeva u i z.*
*Slično se definira i **najveći zajednički djelitelj** cijelih brojeva $u_1, u_2, ..., u_n$ (od kojih je barem jedan različit od nule) koji se označava s $(u_1, u_2, ..., u_n)$.*

Definicija 3 (vidjeti [3, str. 56]). *Cijeli brojevi t i u su relativno prosti ako vrijedi $(t, u) = 1$.*
Cijeli brojevi $t_1, t_2, ..., t_n$ su relativno prosti ako vrijedi $(t_1, t_2, ..., t_n) = 1$, a u parovima su relativno prosti ako vrijedi $(t_i, t_j) = 1$ za sve $1 \leq i, j \leq n, i \neq j$.

Primjer 2. *i*) $(40, 13) = 1$. *Brojevi* 40 *i* 13 *su relativno prosti brojevi.*

ii) $(40, 30) = 10$. *Brojevi* 40 *i* 30 *nisu relativno prosti brojevi.*

iii) $(40, 13, 7) = 1$. *Brojevi* 40, 13 *i* 7 *su u parovima relativno prosti brojevi.*

iv) $(40, 30, 4) = 2$ *nisu u parovima relativno prosti brojevi.*

Kada smo se uveli u svijet djeljivosti, prelazimo na konkretan algoritam.

2.1 Euklidov algoritam

Teorem 2 (vidjeti [1, str. 14]). *Ovaj teorem naziva se Euklidov algoritam. Neka su u i $z > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom Teorema o dijeljenju s ostatkom dobiven niz jednakosti*

$$u = zq_1 + r_1, 0 < r_1 < z,$$

$$z = r_1q_2 + r_2, 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2,$$

$$\dots$$

$$r_{j-2} = r_{j-1}q_j + r_j, 0 < r_j < r_{j-1},$$

$$r_{j-1} = r_jq_{j+1}.$$

Tada je (u,z) jednak r_j, posljednjem ostatku različitom od nule. Vrijednosti od x_0 i y_0 u izrazu $(u,z) = ux_0 + zy_0$ mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od u i z.

Dokaz. Pozivajući na jednakost $(u,z) = (u, z+ux)$, imamo

$$(u,z) = (u - zq_1, z) = (r_1, z) = (r_1, z - r_1q_2) = (r_1, r_2) = (r_1 - r_2q_3, r_2) = (r_3, r_2).$$

Nastavljajući proces, dobit ćemo: $(u,z) = (r_{j-1}, r_j) = (r_j, 0) = r_j$.
Indukcijom dokazujemo da je svaki r_i linearna kombinacija u i z. To je točno za r_1 i r_2, pa pretpostavimo da vrijedi i za r_{i-1} i r_{i-2}. Po pretpostavci indukcije dobivamo da je i linearna kombinacija od u i z. □

Primjer 3. *Izračunajmo $d = (252, 198)$ te prikažimo d kao linearnu kombinaciju brojeva* 252 *i* 198.
S d označimo posljednji ostatak različit od nule u Euklidovu algoritmu.

$$252 = 191 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2 + 0$$

$$\Rightarrow d = 18.$$

Dakle, $(252, 198) = 18$. *Nadalje, imamo:*

$$18 = 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 4 \cdot 54 - 1 \cdot 198 = 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198$$

$$= 4 \cdot 252 - 5 \cdot 198.$$

Euklidov algoritam je drevni algoritam za kojega se smatra da su ga koristili indijski i kineski matematičari u 5. stoljeću. On predstavlja efikasan način za određivanje najvećeg zajedničkog djelitelja dva cijela broja.
Uočimo kako iz prve jednakosti algoritma možemo zapisati $r_1 = u - q_1 t$. Uvrštavanjem u idući redak dobivamo $r_2 = (1 + q_1 q_2)t - q_2 u$. Ako bi nastavili uvrštavati u slijedeće jednakosti, dolazimo do zaključka kako postoje cijeli brojevi x i y za koje vrijedi:

$$tx + uy = r_n = (t, u).$$

Prethodnu jednakost nazivamo **Bezoutov identitet**.

Rješenja jednadžbe $ux + zy = (u, z)$ dobivamo na slijedeći način: ako je

$$r_{-1} = u, r_0 = z; r_i = r_{i-2} - q_i r_{i-1};$$
$$x_{-1} = 1, x_0 = 0; x_i = x_{i-2} - q_i x_{i-1};$$
$$y_{-1} = 0, y_0 = 1; y_i = y_{i-2} - q_i y_{i-1};$$

onda je

$$ux_i + zy_i = r_i, i = -1, 0, 1, ..., j + 1.$$

Formula je točna za $i = -1$ i $i = 0$, pa tvrdnja trivijalno slijedi indukcijom (obje strane formule zadovoljavaju rekurzivnu relaciju). Posebno, vrijedi:

$$ux_j + zy_j = (u, z).$$

Primjer 4. *Izračunajte x i y iz jednadžbe* $252x + 198y = (252, 198)$.
$x, y = ?$
Prema Primjeru 3 znamo da je $(252, 198) = 18$.

$$(252, 198) = 18 = 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) = 54 \cdot 4 - 198 =$$
$$= (252 - 198) \cdot 4 - 198 = 252 \cdot 4 - 198 \cdot 5$$
$$(252, 198) = 252x + 198y$$
$$\Rightarrow x = 4, y = -5$$

Teorem 3 (vidjeti [3, str. 7]). *Uzmimo t i u cijele brojeve. Najmanji prirodan broj m za kojeg postoji cjelobrojno rješenje jednadžbe $tx + uy = m$ je (t, u). Jednadžba $tx + uy = m$ ima cjelobrojno rješenje ako i samo ako (t, u) dijeli m.*

Dokaz. Kako $(t, u) \mid t$ i $(t, u) \mid u$, za sve $x, y \in \mathbb{Z}$ mora vrijediti i $(t, u) \mid tx + uy$. Prema tome, ako jednadžba $tx + uy = m$ ima cjelobrojno rješenje, tada $(t, u) \mid m$. Ukoliko je m prirodan broj manji od (t, u) tada m nije djeljiv s (t, u) pa promatrana jednadžba nema rješenja za takav broj m.
U razmatranjima prije teorema pokazali smo da postoji cjelobrojno rješenje jednadžbe $tx + uy = (t, u)$. Neka je $m \in \mathbb{N}$ takav da $(t, u) \mid m$. Tada postoji $d \in \mathbb{N}$ za koji vrijedi $m = (t, u) \cdot d$. Direktno slijedi

$$tdx + udy = d \cdot (t, u) = m$$

pa je dx, dy traženo cjelobrojno rješenje. □

Prethodni teorem pokazuje kako jednadžba $tx + uy = 1$ ima cjelobrojno rješenje ako i samo ako su brojevi t i u relativno prosti.
Svaki algoritam ima određenu brzinu. Prirodno je pitati se koliko je Euklidov algoritam brz, odnosno koliko koraka mu je potrebno za izvršenje. Naravno, postoje situacije u kojima je algoritam jako efikasan, ali postoje i situacije gdje je potrebno više koraka za njegovo izvršavanje. Sljedeći rezultat dat će nam ogradu na broj mogućih koraka Euklidova algoritma.

Propozicija 2.1 (vidjeti [3, str. 8]). *Neka su t i u prirodni brojevi, pri čemu je $u \geq t$. Za broj koraka Euklidova algoritma vrijedi da je manji ili jednak $5 \cdot (\lfloor \log t \rfloor + 1)$, gdje smo s $\log t$ označili dekadski logaritam prirodnog broja t.*

Dokaz. Najprije ćemo dokazati kako je broj znamenki broja t jednak upravo $\lfloor \log t \rfloor + 1$. Označimo broj znamenaka broja t (u dekadskom zapisu) s n. Tada očito vrijedi

$$10^{n-1} \leq a \leq 10^n.$$

Logaritmiranjem prethodnog izraza te korištenjem činjenice da je log rastuća funkcija dobivamo

$$n - 1 \leq \log a < n,$$

odakle direktno slijedi $n = \lfloor \log t \rfloor + 1$.
Pretpostavimo da smo primjenom Euklidova algoritma dobili sljedeći niz jednakosti:

$$\begin{aligned} u &= q_{n-1}t + r_{n-1} \\ t &= q_{n-2}r_{n-1} + r_{n-2} \\ &\vdots \\ r_3 &= q_1 r_2 + r_1 \\ r_2 &= q_0 r_1, \end{aligned}$$

dakle imamo n koraka provedbi algoritma te smo, označili dobivane ostatke redom s $t = r_n > r_{n-1} > \ldots > r_1$.
Kako je $q_i \geq 1$ za sve i, dobivamo $r_{i+1} \geq r_i + r_{i-1}$. Osim toga, $r_1 \geq 1$ i $r_2 \geq 2$. Iz toga dobivamo

$$\begin{aligned} r_3 &\geq r_2 + r_1 \geq 3, \\ r_4 &\geq r_3 + r_2 \geq 5, \\ r_5 &\geq r_4 + r_3 \geq 8. \end{aligned}$$

Možemo zaključiti da je $r_i \geq F_i$, gdje je F_i i-ti Fibonaccijev broj. Dakle, $a \geq F_n$ i broj znamenki od t veći je ili jednak broju znamenki od F_n.
Da bismo ocijenili broj znamenki Fibonaccijeva broja koristimo Binetovu formulu

$$F_n = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}),$$

jedna od čijih posljedica je i nejednakost $F_n \geq (\frac{1-\sqrt{5}}{2})^{n+1}$. Odatle je $\log F_n \geq (n-1)\log(\frac{1+\sqrt{5}}{2})$. Kako je $\log(\frac{1+\sqrt{5}}{2}) > \frac{1}{5}$, slijedi $\log F_n > \frac{n-1}{5}$ te je broj znamenki od F_n barem $\frac{n}{5}$. Prema tome, broj koraka algoritma manji je ili jednak od broja znamenki broja t uvećanog 5 puta, odnosno $\lfloor \log t \rfloor + 1 \geq \frac{n}{5}$. □

3 | Kvadratni ostaci

Dio teorije brojeva koje nazivamo kvadratni ostatci bavi se pitanjem postoji li kvadratni korijen modulo n cijeloga broja a te ukoliko on postoji, kako ga odrediti.
Da bi lakše razumjeli pojmove koje ćemo koristiti u ovom poglavlju, definirajmo prvo kongruenciju i ostale potrebne pojmove.
Važno je naglasiti kako je teoriju kongruencija te oznaku za kongruenciju koju i danas koristimo uveo Carl Friedrich Gauss, jedan od najvećih matematičara svih vremena.

Definicija 4 (vidjeti [3, str. 19]). *Ako cijeli broj $m \neq 0$ dijeli razliku $t - u$, gdje su t, u također cijeli brojevi, onda kažemo da je t kongruentan u modulo m i pišemo $t \equiv u \pmod{m}$. U protivnom, kažemo da t nije kongruentan u modulo m i pišemo $t \not\equiv u \pmod{m}$.*

Primjer 5.

$$12 \equiv 2 \pmod{10}$$
$$12 \equiv -8 \pmod{10}$$
$$12 \equiv 2 \pmod{5}$$
$$12 \equiv 0 \pmod{3}$$
$$12 \not\equiv 1 \pmod{3}$$

Propozicija 3.1 (vidjeti [3, str. 19]). *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz. Treba provjeriti refleksivnost, simetričnost i tranzitivnost.

i) Iz $m \mid 0$ slijedi $t \equiv t \pmod{m}$.

ii) Ako je $t \equiv u \pmod{m}$, onda postoji $k \in \mathbb{Z}$ takav da $t - u = mk$. Sada je $u - t = m \cdot (-k)$, pa je $u \equiv t \pmod{m}$.

iii) Iz $t \equiv u \pmod{m}$ i $u \equiv z \pmod{m}$ slijedi da postoje $k, l \in \mathbb{Z}$ takvi da je $t - u = mk$ i $z - u = ml$. Zbrajanjem dobivamo $t - z = m(k + l)$, što povlači $t \equiv z \pmod{m}$.

□

Potpuni i reducirani sustav ostataka

Definicija 5 (vidjeti [3, str. 20]). *Uzmimo prirodan broj n koji je veći od 1. Skup $S = \{t_1, t_2, ..., t_n\}$ nazivamo* ***potpuni sustav ostataka modulo*** *n ako za svaki cijeli broj u postoji jedinstveni $t_i \in S$ za koji vrijedi $u \equiv t_i \pmod{n}$.*

Napomena 1. *Uočimo kako svaki potpuni sustav ostataka modulo n ima točno n elemenata. Također, svaki n-člani skup koji se sastoji od cijelih brojeva međusobno nekongruentnih modulo n predstavlja jedan potpun sustav ostataka modulo n.*

Skup $\{0, 1, 2, ..., n-1\}$ je najčešće korišten potpuni sustav ostataka modulo n. Navedimo nekoliko primjera.

Primjer 6. *Primjeri potpunih sustava ostataka modulo 5:*

i) $\{0, 1, 2, 3, 4\}$

ii) $\{1, 2, 3, 4, 5\}$

iii) $\{-2, -1, 0, 1, 2\}$

iv) $\{-10, -8, -4, 13, 39\}$.

Definicija 6 (vidjeti [3, str. 23]). *Uzmimo n prirodan broj veći od 1. Skup $S = \{t_1, t_2, ..., t_k\}$ nazivamo* ***reducirani sustav ostataka modulo*** *n ako za svaki cijeli broj u koji je relativno prost s n postoji jedinstveni $t_i \in S$ za koji vrijedi $u \equiv t_i \pmod{n}$.*

Primjer 7. *Skupovi $\{1, 2, 3, 4\}$ i $\{-2, -6, 6, 7\}$ su reducirani sustavi ostataka modulo 5.*

3.1 Legendreov simbol

Definicija 7 (vidjeti [1, str. 24]). *Neka je* $(t, m) = 1$. *Ako kongruencija* $x^2 \equiv t \pmod{m}$ *ima rješenja, onda kažemo da je* t *kvadratni ostatak modulo* m. *U protivnom kažemo da je* t *kvadratni neostatak modulo* m.

Primjer 8. *Kvadratni ostatci modulo* 5 *su* 1 *i* 4, *a neostatci su* 2 *i* 3.

Primjer 9. *Izračunajmo kvadratne ostatke i kvadratne neostatke modulo* 7.

$$\begin{aligned} 1^2 &\equiv 1 \pmod 7, \\ 2^2 &\equiv 4 \pmod 7, \\ 3^2 &\equiv 2 \pmod 7, \\ 4^2 &\equiv 2 \pmod 7, \\ 5^2 &\equiv 4 \pmod 7, \\ 6^2 &\equiv 1 \pmod 7. \end{aligned}$$

Reducirani sustav ostataka modulo 7 *iznosi* $\{1, 2, 3, 4, 5, 6\}$.
Vidimo kako su $1, 2, 4$ *kvadratni ostatci modulo* 7, *a* $3, 5, 6$ *su kvadratni neostatci modulo* 7.

Teorem 4 (vidjeti [1, str. 23]). *Uzmimo prost broj* p *koji je neparan. Reducirani sustav ostataka modulo* p *sastoji se od* $\frac{p-1}{2}$ *kvadratnih ostataka i* $\frac{p-1}{2}$ *kvadratnih neostataka.*

Dokaz. Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od brojeva

$$-\frac{p-1}{2}, ..., -1, 1, ..., \frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2, 2^2, ..., (\frac{p-1}{2})^2$. Još treba pokazati da je ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentno modulo p. Pa pretpostavimo da je $k^2 \equiv l^2 \pmod p$, gdje je $1 \leq k < l \leq \frac{p-1}{2}$. Tada je $(l-k)(l+k) \equiv 0 \pmod p$, pa je $l - k \equiv 0 \pmod p$ ili $l + k \equiv 0 \pmod p$, što je u suprotnosti s pretpostavkama na k i l, jer je $0 < l - k < p$ i $0 < l + k < p$. □

Definicija 8 (vidjeti [3, str. 41]). *Uzmimo neparan prost broj* p *i cijeli broj* t. ***Legendreov simbol*** $\left(\frac{t}{p}\right)$ *definiran je s*

$$\left(\frac{t}{p}\right) = \begin{cases} 1, & \text{ako je } t \text{ kvadratni ostatak modulo } p, \\ 0, & \text{ako je } p \mid t, \\ -1, & \text{ako je } t \text{ kvadratni neostatak modulo } p. \end{cases}.$$

Ako pogledamo posljednji primjer i definiciju Legendreova simbola, dobit ćemo sljedeće rezultate:

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = 1,$$
$$\left(\frac{3}{7}\right) = \left(\frac{6}{7}\right) = -1,$$
$$\left(\frac{21}{7}\right) = 0.$$

Primjetimo da vrijedi i $(\frac{1}{p}) = 1$ te $(\frac{t^2}{p}) = 1$, ako p ne dijeli t i $(\frac{t^2}{p}) = 0$, ako p dijeli t. U slučaju da su t i p relativno prosti brojevi i p neparan prost, vrijedi $t^{p-1} \equiv 1 \pmod{p}$. Euler je iskoristio tu relaciju kako bi dobio formulu koju ćemo iskazati u sljedećem teoremu.

Teorem 5 (vidjeti [3, str. 42]). *Eulerov kriterij kaže: ako je p neparan prost broj, tada vrijedi $\left(\frac{t}{p}\right) \equiv t^{\frac{p-1}{2}} \pmod{p}$. Tada je t kvadratni ostatak modulo p ako i samo ako je $t^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Dokaz. Ako je $\left(\frac{t}{p}\right) = 0$, onda $p \mid t$, pa je tvrdnja zadovoljena. Ako je $\left(\frac{t}{p}\right) = 1$, onda postoji $x_0 \in \mathbb{Z}$ takav da je $x_0^2 \equiv t \pmod{p}$. Sada je iz Malog Fermatovog teorema $t^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{t}{p}\right) \pmod{p}$. Neka je $\left(\frac{t}{p}\right) = -1$. Za svaki $i \in \{1, ..., p-1\}$ odaberimo $j \in \{1, ..., p-1\}$ tako da vrijedi $i \cdot j \equiv t \pmod{p}$ (to vrijedi po teoremu koji tvrdi ako je $\{x_1, ..., x_m\}$ potpun sustav ostataka modulo m, te $(t, m) = 1$, tada je $\{tx_1, ..., tx_m\}$ također potpun sustav ostataka modulo m). Uočimo da je $i \neq j$, budući da je kongruencija $x^2 \equiv t \pmod{p}$ nema rješenja. Dakle, skup $\{1, ..., p-1\}$ se raspada na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv t \pmod{p}$. Množenjem ovih $\frac{p-1}{2}$ kongruencija, te koristeći Wilsonov teorem koji kaže da ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$, dobivamo

$$t^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}.$$

□

Napomena 2. *Posljedica prethodnog teorema tvrdi da, ukoliko je $t \equiv u \pmod{p}$, vrijedi i $\left(\frac{t}{p}\right) = \left(\frac{u}{p}\right)$.*

Propozicija 3.2 (vidjeti [3, str. 42]). *Ako je p neparan prost broj, tada su točno polovica brojeva $1, 2, ..., p-1$ kvadratni ostaci modulo p.*

Dokaz. U dokazu prethodnog teorema vidjeli smo kako su $1^2, 2^2, ..., (\frac{p-1}{2})^2$ kvadratni ostatci modulo p. Pokažimo da je svaki kvadratni ostatak modulo p kongruentan modulo p nekom od brojeva iz prethodnog niza.
Ako je neki $1 \leq t \leq p-1$ kvadratni ostatak modulo p, tada postoji x takav da je $x^2 \equiv t \pmod{p}$. Možemo uzeti da je $1 \leq x \leq p-1$ jer rješenja tražimo u reduciranom sustavu ostataka modulo p.

Ako je $x \leq \frac{p-1}{2}$, tada se x^2 nalazi u prethodnom nizu. Ako je $\frac{p-1}{2} < x$, tada je $x^2 \equiv (p-x)^2 \pmod{p}$ te zbog $p - x < \frac{p-1}{2}$ slijedi da je x^2 kongruentno nekom od brojeva $1^2, 2^2, ..., (\frac{p-3}{2})^2$ modulo p.
Time smo dokazali da u nizu $1, 2, ..., p-1$ postoji točno $\frac{p-1}{2}$ kvadratnih ostataka modulo p koji čine oni članovi koji su kongruentni s $1^2, 2^2, ..., (\frac{p-1}{2})^2$ modulo p. □

U nastavku ćemo pokazati još neka vrlo korisna svojstva Legendreovih simbola.

Propozicija 3.3 (vidjeti [3, str. 43]). *Za svaka dva cijela broja t_1 i t_2 te neparan prost broj p vrijedi*

$$\left(\frac{t_1 t_2}{p}\right) = \left(\frac{t_1}{p}\right)\left(\frac{t_2}{p}\right).$$

Dokaz. Korištenjem Eulerova kriterija dobivamo

$$\left(\frac{t_1}{p}\right)\left(\frac{t_2}{p}\right) \equiv (t_1)^{\frac{p-1}{2}}(t_2)^{\frac{p-1}{2}} \equiv (t_1 t_2)^{\frac{p-1}{2}} \equiv \left(\frac{t_1 t_2}{p}\right) \pmod{p}$$

pa, kako je Legendreov simbol jednak $0, 1$, ili -1, slijedi jednakost. □

Propozicija 3.4 (vidjeti [3, str. 43]). *Za neparan prost broj p vrijedi*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ako je } p \equiv 1 \pmod 4, \\ -1, & \text{ako je } p \equiv 3 \pmod 4. \end{cases}$$

Drugim riječima, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Dokaz. Prema Eulerovu kriteriju je $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.
Ako je $p \equiv 1 \pmod 4$, tada je broj $\frac{p-1}{2}$ paran pa je $\left(\frac{-1}{p}\right) = 1$.
Ako je $p \equiv 3 \pmod 4$, tada je broj $\frac{p-1}{2}$ neparan pa je $\left(\frac{-1}{p}\right) = -1$. □

3.2 Kvadratni zakon reciprociteta

U prethodnom potpoglavlju iskazali smo nekoliko rezultata pomoću kojih određujemo Legendreov simbol, no eksplicitno računanje je i dalje komplicirano. Kvadratni zakon reciprociteta je najveći korak prema pojednostavljenju tog postupka. On se smatra ključnim teoremom u teoriji brojeva kada se proučavaju kvadratne diofantske jednadžbe. Sve zasluge za ovaj rezultat idu Gaussu. Zanimljiv je podatak kako je do 2000. godine konstruirano mnogo različitih dokaza, čak 196.
Kako bi izveli dokaz kvadratnog zakona reciprociteta koji se temelji na množenju elemenata koji posjeduju multiplikativni inverz modulo produkt dva različita prosta broja, iskažimo prvo jedan tehnički rezultat:

Lema 1. *Neka su p i q međusobno različiti prosti brojevi. Tada je*

$$\prod_{1\leq x\leq \frac{pq-1}{2}} x \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$$

i

$$\prod_{1\leq x\leq \frac{pq-1}{2}} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

Dokaz. Promotrimo invertibilne elemente modulo pq,. To su elementi koji nisu djeljivi niti s p niti s q. Skup invertibilnih elemenata x koji se nalaze u $\{1, 2, ..., , \frac{pq-1}{2}\}$, promatran modulo p sastoji se od $\frac{q-1}{2}$ nizova $1, 2, ..., p-1$ te niza $1, 2, ..., \frac{p-1}{2}$, gdje još treba isključiti niz $q, 2q, ..., \frac{p-1}{2}q$ koji se sastoji od višekratnika broja q. Na taj način dobivamo

$$\prod_{1\leq x\leq \frac{pq-1}{2}} x \equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \diagup q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \equiv$$

$$\equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$$

jer se $\left(\frac{p-1}{2}\right)!$ pokrati, $(p-1)! \equiv -1 \pmod{p}$, prema Wilsonovu teoremu te $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$, prema Eulerovu kriteriju.
Na isti način dobivamo i

$$\prod_{1\leq x\leq \frac{pq-1}{2}} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q},$$

čime je lema dokazana. □

Kada smo iskazali i dokazali rezultat koji nam je potreban, iskažimo i glavnu tvrdnju:

Teorem 6 (vidjeti [1, str. 24]). *Ovaj teorem nazivamo Gaussov kvadratni zakon reciprociteta, Ako su p i q različiti neparni prosti brojevi, onda vrijedi*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Možemo to reći i na ovaj način. Ako su p i q oba oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}, x^2 \equiv q \pmod{p}$ ima rješenja, a druga nema. Ako je barem jedan od brojeva p i q oblika $4k+1$, onda ili obje ove kongruencije imaju rješenja ili niti jedna nema rješenja.

Dokaz. Neka je $S = \{(x,y) : x,y \in \mathbb{Z}, 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}$. Skup S ima $\frac{p-1}{2}\cdot\frac{q-1}{2}$ članova. Podijelimo S na dva disjunktna podskupa S_1 i S_2 prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$. Skup S_1 je, dakle, skup svih parova (x,y) takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $1 \leq y \leq \frac{qx}{p}$. Takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$. Slično se S_2 sastoji od svih parova (x,y) takvih da je $1 \leq y \leq \frac{q-1}{2}$ i $1 \leq x \leq \frac{py}{q}$, a takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$. Prema tome je $\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor = \frac{p-1}{2}\cdot\frac{q-1}{2}$, pa je po teoremu (koji tvrdi ako je p neparan prost broj i $(a,2p)=1$, onda je $\left(\frac{a}{p}\right) = (-1)^t$, gdje je $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor$. Također vrijedi: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, tj. broj 2 je kvadratni ostatak modulo p ako i samo ako je p oblika $8k+1$ ili $8k-1$.)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

□

Pogledajmo jedan primjer:

Primjer 10. *Izračunajmo* $\left(\frac{-42}{61}\right)$.

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right),$$

$$\left(\frac{-1}{60}\right) = (-1)^{\frac{60}{2}} = 1,$$

$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1,$$

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1,$$

$$\Rightarrow \left(\frac{-42}{61}\right) = 1\cdot(-1)\cdot 1\cdot(-1) = 1.$$

3.3 Jacobijev simbol

Jacobijev simbol generalizira Legendreov simbol. Stoga krenimo s definicijom:

Definicija 9 (vidjeti [3, str. 47]). *Uzmimo P koji je neparan broj iz skupa prirodnih brojeva te ga zapišimo u obliku $P = p_1 p_2 \cdots p_n$, gdje su $p_1, p_2, ..., p_n$ prosti brojevi, koji su nužno neparni. Jacobijev simbol $\left(\frac{a}{P}\right)$ definiran je s*
$\left(\frac{t}{P}\right) = \left(\frac{t}{p_1}\right)\left(\frac{t}{p_2}\right)\cdots\left(\frac{t}{p_n}\right)$, *gdje je $\left(\frac{t}{p_i}\right)$ Legendreov simbol.*

Napomena 3. *Ako je P prost, tada se Jacobijev i Legendreov simbol podudaraju. Ako t i P nisu relativno prosti, tada je $\left(\frac{t}{P}\right) = 0$, inače je jednako 1 ili -1.*

Napomena 4. *Primjetimo da $\left(\frac{t}{P}\right) = 1$ ne povlači da je t kvadratni ostatak modulo P. Na primjer, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, ali kongruencija $x^2 \equiv 2 \pmod{15}$ nema rješenja. Da bi t bio kvadratni ostatak modulo P nužno je i dovoljno da svi $\left(\frac{t}{p_i}\right)$ budu jednaki 1.*

Pogledajmo svojstva Jacobijeva simbola. Ona se dobivaju analogno svojstvima Legendreova simbola:

Propozicija 3.5 (vidjeti [3, str. 47]). *Neka su t i u cijeli brojevi te P_1 i P_2 neparni prirodni brojevi. Tada vrijedi:*

i) $\left(\frac{t}{P_1 P_2}\right) = \left(\frac{t}{P_1}\right)\left(\frac{t}{P_2}\right)$,

ii) $\left(\frac{tu}{P_1}\right) = \left(\frac{t}{P_1}\right)\left(\frac{u}{P_1}\right)$,

iii) ako je $t \equiv u \pmod{P_1}$, *tada vrijedi* $\left(\frac{a}{P_1}\right) = \left(\frac{b}{P_1}\right)$,

iv) ako je $(t, P_1) = 1$, *tada vrijedi* $\left(\frac{t^2}{P_1}\right) = \left(\frac{t}{P_1^2}\right) = 1$,

v) $\left(\frac{-1}{P_1}\right) = (-1)^{\frac{P_1-1}{2}}$, $\left(\frac{2}{P_1}\right) = (-1)^{\frac{P_1-1}{8}}$,

vi) ako je $(P_1, P_2) = 1$, *tada vrijedi* $\left(\frac{P_1}{P_2}\right)\left(\frac{P_2}{P_1}\right) = (-1)^{\frac{P_1-1}{2}\cdot\frac{P_2-1}{2}}$.

Primjer 11. *Izračunajmo* $\left(\frac{105}{317}\right)$.

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1.$$

Sada kada smo se upoznali razna svojstva, riješimo još jedan primjer:

Primjer 12. *Izračunajte:*

a) $\left(\frac{24}{31}\right)$,

b) $\left(\frac{-20}{61}\right)$.

Rješenje:

a) $\left(\frac{24}{31}\right) = \left(\frac{4}{31}\right)\cdot\left(\frac{6}{31}\right) = \left(\frac{2}{31}\right)^2\cdot\left(\frac{6}{31}\right) = 1\cdot\left(\frac{2}{31}\right)\cdot\left(\frac{3}{31}\right) = (-1)^{\frac{31^2-1}{8}}\cdot\left(\frac{3}{31}\right) = 1\cdot\left(\frac{3}{31}\right) = \left(\frac{3}{31}\right) = \left(\frac{31}{3}\right)(-1)^{\frac{31-1}{2}\cdot\frac{3-1}{2}} = -\left(\frac{1}{3}\right) = -1,$

b) $\left(\frac{-20}{61}\right) = \left(\frac{-1}{61}\right)\cdot\left(\frac{20}{61}\right) = (-1)^{\frac{61-1}{2}}\cdot\left(\frac{4}{61}\right)\cdot\left(\frac{5}{61}\right) = 1\cdot\left(\frac{2}{61}\right)^2\cdot\left(\frac{5}{61}\right) = \left(\frac{5}{61}\right) = \left(\frac{61}{5}\right)\cdot(-1)^{\frac{61-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{61}{5}\right) = 1.$

S obzirom da je tema završnoga rada Algoritmi u teoriji brojeva, napišimo za kraj algoritam koji računa Jacobijev simbol: [vidjeti [1, str. 25]]

Algoritam 1 Algoritam za računanje Jacobijeva simbola

```
t = t (mod m); a = 1
while (t ≠ 0) do
while (t paran) do
t = t/2
if (m ≡ 3,5 (mod 8)) then a = −a
(t, m) = (m, t)
if (t ≡ m ≡ 3 (mod 4)) then a = −a
t = t (mod m)
if (m = 1) then return a
else return 0
```

Literatura

[1] A. Dujella, Algoritmi u teoriji brojeva, PMF, Matematički odjel, Sveučilište u Zagrebu, Zagreb, 2021.
dostupno na: https://web.math.pmf.unizg.hr/~duje/algortb/algortb.pdf

[2] A. Dujella, Uvod u teoriju brojeva (skripta), PMF, Matematički odjel, Sveučilište u Zagrebu, Zagreb, 2009.

[3] I. Matić, Uvod u teoriju brojeva, Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku, Osijek, 2015.

Sažetak

Teorija brojeva, kao jedna od grana matematike, proučava svojstva cijelih brojeva pomoću raznih algoritama. U ovom završnom radu, objasnit ćemo neke algoritme koji se koriste u teoriji brojeva. U prvom dijelu proučavamo djeljivost, odnosno reći ćemo nešto više o Euklidovu algoritmu. U drugom dijelu rada proučavat ćemo kvadratne ostatke. Bazirat ćemo se na Legendreov i Jacobijev simbolu te ćemo na kraju objasniti Gaussov zakon reciprociteta.

Ključne riječi

Euklidov algoritam, Legendreov simbol, Jacobijev simbol, Gaussov kvadratni zakon reciprociteta.

Algorithms of Number Theory

Summary

Number Theory, as one of the branches of mathematics, studies the properties of integers using various algorithms. In this final work we are going to explain some of algorithms used in Number Theory. In the first part, we will say something more about divisibility, especially Euclid's algorithm. Second part of final exam studies Legendre's symbol, Jacobi's symbol and Law of Quadratic Reciprocity.

Keywords

Euclid's algorithm, Legendre's symbol, Jacobi's symbol, Law of Quadratic Reciprocity.

Životopis

Moje ime je Filip Cindrić. Rođen sam 09.03.1997. godine u Novoj Gradiški.
U razdoblju od 2004. do 2012. godine pohađao sam Osnovnu školu "Antun Mihanović" Nova Kapela - Batrina. Nakon toga upisujem Opću gimnaziju u Novoj Gradiški. Istu sam završio 2016. godine te nakon toga upisujem Sveučilišni prijediplomski studij Matematike na Odjelu za matematiku Sveučilišta Josipa Jurja Strossmayera u Osijeku, sada Fakultet primijenjene matematike i informatike.
Tijekom studiranja sam redovno nastupao na Sveučilišnim sportskim natjecanjima te sam 2019. godine osvojio prvo mjesto u futsalu nastupajući za momčad tadašnjeg Odjela za matematiku. Aktivno volontiram s djecom i mladima pružajući im podršku u učenju matematike i informatike.