Primitivni korijeni

Milković, Marija

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marija Milković

PRIMITIVNI KORIJENI

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, veljača, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj rad posvećujem svojoj obitelji i zaručniku koji su bili uz mene kroz cijeli studij i pružali mi neizmjernu podršku. Posebne zahvale mentorici izv. prof. dr. sc. Zrinki Franušić na svoj pomoći i savjetima pri pisanju diplomskog rada.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Teorija brojeva je grana matematike koja se bavi proučavanjem svojstava prirodnih brojeva. Modularna aritmetika je grana teorije brojeva čiji je jedan od temeljnih pojmova primitivni korijen. Euler je uveo pojam primitivnog korijena 1773. godine i našao primitivne korijene za prirodne brojeve n, $n \in \{1, 2, \ldots, 41\}$. Gauss je preciznije definirao pojam i pokazao da postoji primitivni korijen modulo p za svaki prosti broj p.

U prvom poglavlju najprije se bavimo pojmom reda nekog broja. Taj pojam utemeljen je na Eulerovom teoremu koji kaže da je $a^{\varphi(n)} \equiv 1 \pmod{n}$, pri čemu su $a \in \mathbb{Z}$ i $n \in \mathbb{N}$ relativno prosti brojevi, a $\varphi(n)$ je Eulerova funkcija čija je vrijednost jednaka broju elemenata skupa $\{1, 2, \ldots, n\}$ koji su relativno prosti s n. *Red* od a modulo n je najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$. Ako je $d = \varphi(n)$, onda se a naziva *primitivni korijen* modulo n. Pokazuje se da ne postoji primitivni korijen modulo n za svaki prirodan broj n. Naime, primitivni korijen modulo n postoji ako i samo ako je $n = 2, 4, p^t$ ili $2p^t$, pri čemu je p prosti broj i $t \in \mathbb{N}$. Štoviše, za navedene oblike broja n postoji točno $\varphi(\varphi(n))$ nekongruentnih primitivnih korijena modulo n.

Ako je a primitivni korijen modulo n, skup $\{1 = a^0, a^1, \ldots, a^{\varphi(n)-1}\}$ čini reducirani sustav ostatak modulo n što znači da su elementi tog skupa relativno prosti s n, međusobno nekongruentni modulo n te za svaki $y \in \mathbb{Z}$ koji je relativno prost s n vrijedi da je $y \equiv a^x \pmod{n}$ za $x \in \{0, 1, \ldots, \varphi(n) - 1\}$. To svojstvo nam omogućava definiciju *indeksa* ili *diskretnog logaritma* broja y kao eksponenta $x \in \{0, 1, \ldots, \varphi(n) - 1\}$. Mnoga svojstva indeksa analogna su svojstvima logaritama pri čemu jednakosti samo treba zamijeniti kongruencijama modulo $\varphi(n)$. Nadalje, ako postoji primitivni korijen modulo n, skup Z_n^* (tj. skup svih elemenata iz $\{1, 2, \ldots, n\}$ koji su relativno prosti s n) čini multiplikativnu cikličku grupu čiji je generator upravo primitivni korijen modulo n.

U drugom poglavlju opisane su neke primjene primitivnih korijena kao što su rješavanje polinomijalnih i eksponencijalnih kongruencija, testovi prostosti te Diffie - Hellmanov protokol za razmjenu ključeva koji ima važnu ulogu u kriptografiji.

Poglavlje 1

Primitivni korijeni

1.1 Red broja

Neka je n prirodni broj. *Potpuni sustav ostataka modulo n* je svaki skup cijelih brojeva $\{x_1, \ldots, x_n\}$ za koji vrijedi da za svaki $x \in \mathbb{Z}$ postoji jedinstven $i \in \{1, \ldots, n\}$ za koji je

$$x \equiv x_i \pmod{n}.$$

Najčešće za potpuni sustav ostataka modulo n uzimamo skup $\{0, 1, \ldots, n-1\}$ – sustav najmanjih nenegativnih ostataka ili sustav apsolutno najmanjih ostataka: $\{\frac{n-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-1}{2}\}$ ako je n neparan, odnosno $\{\frac{n-2}{2}, \ldots, -1, 0, 1, \ldots, \frac{n}{2}\}$ ako je n paran.

Reducirani sustav ostataka modulo n je skup svih onih elemenata iz potpunog sustava ostataka koji su relativno prosti s n. Stoga je skup cijelih brojeva $\{r_1, \ldots, r_k\}$ reducirani sustav ostataka modulo n ako i samo ako vrijedi:

- $\text{nzd}(r_i, n) = 1$, za sve $i = 1, \ldots, k$;
- $r_i \not\equiv r_j \pmod{n}$, za sve $1 \leq i < j \leq k$;
- za svaki $y \in \mathbb{Z}$ koji je relativno prost s n postoji jedinstven $i \in \{1, \ldots, k\}$ za koji je $y \equiv r_i \pmod{n}$.

Svaki reducirani sustav ostataka modulo n je jednakobrojan.

Definicija 1.1.1. *Funkcija koja svakom prirodnom broju n pridruži broj elemenata u reduciranom sustavu ostataka modulo n naziva se* Eulerova funkcija *i označava s* $\varphi : \mathbb{N} \to \mathbb{N}$.

Često kažemo da je $\varphi(n)$ broj brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n. Otuda lako možemo zaključiti da je $\varphi(p) = p - 1$ za svaki prosti broj p. Nadalje, lako se pokazuje da je $\varphi(p^k) = p^k - p^{k-1}$, za sve $k \in \mathbb{N}$.

Može se pokazati da je Eulerova funkcija tzv. *multiplikativna funkcija* što znači da zadovoljava sljedeća dva svojstva:

- $\varphi(1) = 1$;
- $\varphi(mn) = \varphi(m)\varphi(n)$, za sve $m, n \in \mathbb{N}$ i $\text{nzd}(m, n) = 1$.

Zahvaljujući svojstvu multiplikativnosti može se pokazati sljedeća formula za računanje $\varphi(n)$.

Teorem 1.1.2. *Neka je $n > 1$ prirodan broj. Tada je*

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}), \tag{1.1}$$

gdje produkt prolazi svim prostim djeliteljima od n.

Ako je kanonski rastav broja n na proste faktore dan s

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

gdje su $p_1 < p_2 < \cdots < p_k$ prosti brojevi i $\alpha_1, \alpha_2 \ldots, \alpha_k \in \mathbb{N}$, tada se formula (1.1) zapisuje kao

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

Iz prethodnog lako možemo zaključiti da ako neparan prost broj p dijeli n, onda $p - 1$ dijeli $\varphi(n)$, što znači da je $\varphi(n)$ paran. Očito je $\varphi(n)$ paran i ako je $n > 2$ potencija broja 2. Dakle, $\varphi(n)$ je paran broj za sve prirodne brojeve $n > 2$, a $\varphi(1) = \varphi(2) = 1$.

Teorem 1.1.3. *Za svaki prirodni broj n vrijedi*

$$\sum_{d|n} \varphi(d) = n,$$

gdje suma prolazi skupom svih pozitivnih djelitelja od n.

Dokaz. Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Kako je svaki djelitelj d od n oblika $d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$, gdje su $0 \leq \beta_i \leq \alpha_i$, za $i = 1, \ldots, k$, imamo

$$\sum_{d|n} \varphi(d) = \sum_{d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}} \varphi(p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}).$$

Zbog multiplikativnosti od φ, slijedi $\varphi(p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}) = \varphi(p_1^{\beta_1}) \cdot \ldots \cdot \varphi(p_k^{\beta_k})$ pa je

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \ldots + \varphi(p_i^{\alpha_i})),$$

odnosno

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k}(1 + (p_i - 1) + (p_i^2 - p_i) + \ldots + (p_i^{\alpha_i}) - p_i^{\alpha_i - 1}) = \prod_{i=1}^{k} p_i^{\alpha_i} = n.$$

□

Teorem 1.1.4 (Eulerov teorem)**.** *Ako je* $\text{nzd}(a, n) = 1$*, onda je* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dokaz. Neka je $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. S obzirom da je $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ također reducirani sustav ostataka modulo n, zaključujemo da vrijedi

$$\prod_{j=1}^{\varphi(n)}(ar_j) \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n},$$

odnosno

$$a^{\varphi(n)} \prod_{j=1}^{\varphi(n)} r_j \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n}.$$

Budući da je $\text{nzd}(r_i, n) = 1$ za sve $i = 1, \ldots, \varphi(n)$, slijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$.

□

Korolar 1.1.5 (Mali Fermatov teorem)**.** *Neka je p prost broj. Ako* $p \nmid a$*, onda je* $a^{p-1} \equiv 1 \pmod{p}$*. Za svaki cijeli broj a vrijedi* $a^p \equiv a \pmod{p}$.

Definicija 1.1.6. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je* $a^d \equiv 1 \pmod{n}$ *zove se* red *od a modulo n. Još se kaže da a* pripada eksponentu *d modulo n.*

Primjer 1.1.1. *Pronađite red od* 2 *modulo* 7 *i red od* 3 *modulo* 7.

Rješenje. Odredimo najmanje pozitivne ostatke pri dijeljenju višekratnika od 2 brojem 7:

$$2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}.$$

Stoga je red od 2 modulo 7 jednak 3. Analogno, iz

$$3^1 \equiv 3 \pmod{7}, \quad 3^2 \equiv 2 \pmod{7}, \quad 3^3 \equiv 6 \pmod{7},$$

$$3^4 \equiv 4 \pmod{7}, \quad 3^5 \equiv 5 \pmod{7}, \quad 3^6 \equiv 1 \pmod{7}$$

zaključujemo da je 6 red od 3 modulo 7. □

Propozicija 1.1.7. *Neka je d red od a modulo n. Tada za prirodni broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d \mid k$. Posebno, $d \mid \varphi(n)$.*

Dokaz. Ako $d \mid k$, tada je $k = d \cdot l$, gdje je $l \in \mathbb{N}$. Slijedi da je

$$a^k \equiv (a^d)^l \equiv 1^l = 1 \pmod{n}.$$

Obratno, neka je $a^k \equiv 1 \pmod{n}$. Kako je $k = q \cdot d + r$, gdje je $0 \leq r < d$ i $q \in \mathbb{N}$, vrijedi

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q \cdot a^r \equiv a^r \pmod{n},$$

Budući da je d najmanji prirodan broj za koji je $a^d \equiv 1 \pmod{n}$, iz nejednakosti $0 \leq r < d$ možemo zaključiti da je $r = 0$. Dakle, $d \mid k$.

Eulerov teorem 1.1.4 povlači da $d \mid \varphi(n)$. □

Primjer 1.1.2. *Provjerite jesu li $x = 10$ i $x = 15$ rješenja od $2^x \equiv 1 \pmod{7}$ primjenom propozicije 1.1.7.*

Rješenje. Iz primjera 1.1.1 znamo da je 3 red od 2 modulo 7. S obzirom da 3 ne dijeli 10, ali dijeli 15, $x = 10$ nije rješenje od $2^x \equiv 1 \pmod{7}$, dok $x = 15$ je. □

Teorem 1.1.8. *Neka je d red od a modulo n, te $i, j \in \mathbb{N}_0$. Tada je $a^i \equiv a^j \pmod{n}$ ako i samo ako $i \equiv j \pmod{d}$.*

Dokaz. Pretpostavimo da vrijedi $i \equiv j \pmod{d}$. Tada je $i = j + k \cdot d$ za neki nenegativan cijeli broj k. Kako je $a^d \equiv 1 \pmod{n}$, dobivamo

$$a^i = a^{j+k\cdot d} = a^j(a^d)^k \equiv a^j \pmod{n}.$$

Obratno, pretpostavimo da vrijedi $a^i \equiv a^j \pmod{n}$ pri čemu je $i \geq j$ što možemo zapisati kao

$$a^i \equiv a^j \equiv a^j a^{i-j} \pmod{n}.$$

Prethodnu kongruenciju možemo kratiti s a^i jer je $\text{nzd}(a^i, n) = 1$. Stoga je $a^{i-j} \equiv 1 \pmod{n}$ pa prema propoziciji 1.1.7 slijedi da $d \mid i - j$, odnosno $i \equiv j \pmod{d}$. □

1.2 Primitivni korijeni

Prema Eulerovom teoremu 1.1.4 najveći mogući red broja a modulo n je $\varphi(n)$. Posebno nas zanimaju upravo ti brojevi.

Definicija 1.2.1. *Ako je red od a modulo n jednak $\varphi(n)$, onda se a naziva* primitivni korijen modulo n *ili kraće* primitivni korijen *od n.*

Primjer 1.2.1. *U primjeru 1.1.1 pokazali smo da je red od* 3 *modulo* 7 *jednak* $6 = \varphi(7)$. *Stoga je* 3 *primitivni korijen od* 7.

Zanimljivo je da ne postoji primitivni korijen modulo n za svaki prirodan broj n. U nastavku rada pokazat ćemo za koje brojeve postoji primitivni korijen. Na primjer, postoji primitivni korijen modulo p za svaki prosti broj p.

Primjer 1.2.2. *Pokažite da ne postoji primitivni korijen modulo* 8.

Rješenje. Kandidati za primitivne korijene su prirodni brojevi manji od 8 i relativno prosti s brojem 8, a to su: 1, 3, 5 i 7. Očito je red od 1 uvijek jednak 1 za svaki modul n. Nadalje,

$$3^2 \equiv 1 \pmod 8, \quad 5^2 \equiv 1 \pmod 8, \quad 7^2 \equiv 1 \pmod 8,$$

pa je red svakog od brojeva 3, 5 i 7 modulo 8 jednak 2, a $\varphi(8) = 4$. □

Teorem 1.2.2. *Ako su* r *i* $n > 0$ *relativno prosti prirodni brojevi i ako je* r *primitivni korijen modulo* n, *onda skup*

$$\{r^1, r^2, \ldots, r^{\varphi(n)}\}$$

čini reducirani sustav ostataka modulo n.

Dokaz. Kako bismo pokazali kako prvih $\varphi(n)$ potencija primitivnog korijena r čine reducirani sustav ostataka modulo n, dovoljno je pokazati da su one sve relativno proste s brojem n i da nikoje dvije nisu kongruentne modulo n.

- S obzirom da su r i n relativno prosti, slijedi da su r^k i n relativno prosti za svaki prirodni broj k.
- Pretpostavimo da je
$$r^i \equiv r^j \pmod n$$
za neke $i, j \in \{1, 2, \ldots, \varphi(n)\}$. Prema teoremu 1.1.8 vrijedi $i \equiv j \pmod d$, pri čemu je d red od r modulo n. S obzirom da je r primitivni korijen broja n tada je $d = \varphi(n)$, odnosno $i \equiv j \pmod{\varphi(n)}$. Kako je $1 \leq i, j \leq \varphi(n)$, slijedi $i = j$. Stoga $r^i \not\equiv r^j \pmod n$, za sve $1 \leq i < j \leq \varphi(n)$.

□

Ako za neki prirodan broj n postoji primitivni korijen modulo n, on ne mora biti jedinstven. U onom što slijedi pokazat ćemo koliko je točno primitivnih korijena modulo n u reduciranom sustavu ostataka modulo n.

Teorem 1.2.3. *Neka je* t *red od* a *modulo* n *i* u *prirodni broj. Tada je red od* a^u *modulo* n *jednak* $\dfrac{t}{\text{nzd}(t, u)}$.

Dokaz. Neka je s red od a^u modulo n. Nadalje, označimo $v = \text{nzd}(t, u)$. Stoga je $t = t_1 v$ i $u = u_1 v$ za neke prirodne brojeve t_1 i u_1 koji su relativno prosti. Želimo pokazati da je $s = t_1$. Vrijedi

$$(a^u)^{t_1} = (a^{u_1 v})^{t/v} = (a^t)^{u_1} \equiv 1 \pmod{n},$$

jer je t red od a modulo n. Prema propoziciji 1.1.7 slijedi da $s \mid t_1$. S obzirom da je

$$(a^u)^s = a^{us} \equiv 1 \pmod{n},$$

red od a dijeli us, tj. $t \mid us$. Stoga $t_1 v \mid u_1 vs$, odnosno $t_1 \mid u_1 s$. Kako je $\text{nzd}(t_1, u_1) = 1$, dobivamo da $t_1 \mid s$. Stoga smo pokazali da $t_1 \mid s$ i $s \mid t_1$. Budući da su t_1 i s prirodni brojevi, slijedi $s = t_1$. □

Prethodni teorem kaže nam koje potencije primitivnog korijena su također primitivni korijeni.

Korolar 1.2.4. *Neka je r primitivni korijen modulo n, pri čemu je n prirodan broj veći od* 1. *Tada je r^u primitivni korijen modulo n ako i samo ako* $\text{nzd}(u, \varphi(n)) = 1$.

Dokaz. Neka je d red od r^u modulo n. Red od r modulo n je $\varphi(n)$ jer je r primitivni korijen modulo n. Prema teoremu 1.2.3 je

$$d = \frac{\varphi(n)}{\text{nzd}(u, \varphi(n))}.$$

Dakle, $d = \varphi(n)$ (tj. r^u je primitivni korijen modulo n) ako i samo ako $\text{nzd}(u, \varphi(n)) = 1$. □

Teorem 1.2.5. *Ako postoji primitivni korijen modulo n, onda u reduciranom sustavu ostataka modulo n postoji točno $\varphi(\varphi(n))$ primitivnih korijena modulo n.*

Dokaz. Neka je r primitivni korijen modulo n. Prema teoremu 1.2.2 skup $\{r^1, r^2, \ldots, r^{\varphi(n)}\}$ čini reducirani sustav ostataka modulo n, a prema prethodnom korolaru 1.2.4 znamo da je r^u primitivni korijen modulo n ako i samo ako vrijedi da je $\text{nzd}(u, \varphi(n)) = 1$. U nizu $1, 2, \ldots, \varphi(n)$ točno je $\varphi(\varphi(n))$ brojeva koji su relativno prosti s $\varphi(n)$. Dakle, u skupu $\{r^1, r^2, \ldots, r^{\varphi(n)}\}$ postoji točno $\varphi(\varphi(n))$ primitivnih korijena modulo n. □

1.3 Primitivni korijeni prostih brojeva

U ovom odjeljku pokazat ćemo da postoji primitivni korijen modulo p za svaki prosti broj p. U tu svrhu najprije ćemo promatrati polinomijalne kongruencije. Ako je $f(x)$ polinom s cjelobrojnim koeficijentima, onda za cijeli broj c za koji je $f(c) \equiv 0 \pmod{n}$ kažemo da je *korijen polinoma f modulo n*. Nadalje, kažemo da polinom p ima k korijena modulo n, odnosno da konguencija $f(x) \equiv 0 \pmod{n}$ ima k rješenja, ako ima k međusobno nekongruentnih korijena (rješenja) modulo n.

Teorem 1.3.1 (Lagrangeov teorem)**.** *Neka je* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *polinom s cjelobrojnim koeficijentima stupnja n,* $n \geq 1$*. Pretpostavimo da je p prost broj te da vodeći koeficijent od f nije djeljiv s p. Tada kongurencija* $f(x) \equiv 0 \pmod{p}$ *ima najviše n rješenja modulo p.*

Dokaz. Dokazat ćemo teorem koristeći princip matematičke indukcije.

Baza: Za $n = 1$, imamo $f(x) = a_1 x + a_0$ te $p \nmid a_1$. Korijen od $f(x)$ modulo p je rješenje kongruencije $a_1 x \equiv -a_0 \pmod{p}$. S obzirom da vrijedi $\text{nzd}(a_1, p) = 1$, ova kongruencija ima točno jedno rješenje. Dakle, tvrdnja vrijedi za $n = 1$.

Pretpostavka: Neka je g proizvoljni polinom s cjelobrojnim koeficijentima stupnja $n-1$, $n \geq 1$, čiji vodeći koeficijent nije djeljiv s p. Tada kongurencija $g(x) \equiv 0 \pmod{p}$ ima najviše $n-1$ rješenja modulo p.

Korak: Neka je $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ polinom stupnja n pri čemu $p \nmid a_n$. Pretpostavimo da polinom $f(x)$ ima $n+1$ korijena modulo p i neka su to $c_0, c_1, \ldots, c_n \in \mathbb{Z}$. Dakle, $c_i \not\equiv c_j \pmod{p}$ za $i \neq j$ i $f(c_i) \equiv 0 \pmod{p}$ za $i = 0, 1, \ldots, n$. Tada je

$$f(x) - f(c_0) = a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0)$$

$$= a_n(x-c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + c_0^{n-1}) + a_{n-1}(x-c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + c_0^{n-2}) + \cdots + a_1(x-c_0),$$

odnosno

$$f(x) - f(c_0) = (x - c_0)g(x),$$

pri čemu je g polinom stupnja $n-1$ s vodećim koeficijentom a_n. S obzirom da vrijedi $f(c_k) \equiv f(c_0) \equiv 0 \pmod{p}$, imamo

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod{p},\ k = 1, \ldots, n.$$

Kako $c_k - c_0 \not\equiv 0 \pmod{p}$, dobivamo da je

$$g(c_k) \equiv 0 \pmod{p},\ k = 1, \ldots, n.$$

Stoga, polinom g stupnja $n-1$ ima n korijena modulo p što je u kontradikciji s pretpostavkom. Dakle, f ima najviše n korijena modulo p. □

Sustav reduciranih ostataka modulo n, uz operaciju množenja modulo n, čini Abelovu grupu. Tu grupu označavat ćemo s $\mathbb{Z}_n^*$. Sljedećim teoremom pokazat ćemo da je grupa $\mathbb{Z}_p^*$ ciklička jer postoji primitivni korijen modulo p koji je generator grupe (teorem 1.2.2).

Teorem 1.3.2. *Neka je p prosti broj i d pozitivni djelitelj od* $p - 1$*. Tada je broj nekongruentnih cijelih brojeva modulo p koji pripadaju eksponentu d jednak* $\varphi(d)$*.*

Dokaz. Označimo s $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d. Budući da je red (modulo p) svakog od brojeva $1, 2, \ldots, p-1$ djelitelj od $\varphi(p) = p-1$, slijedi da je

$$\sum_{d|p-1} \psi(d) = p - 1.$$

Također, prema teoremu 1.1.3 je

$$\sum_{d|p-1} \varphi(d) = p - 1.$$

Stoga je

$$\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d). \tag{1.2}$$

Ako pokažemo da je $\psi(d) \leq \varphi(d)$ za svakog pozitvnog djelitelja d od $p-1$, tada će, zbog prethodne jednakosti, slijediti da je $\psi(d) = \varphi(d)$ za sve $d \mid p-1$.

Neka je $d \in \mathbb{N}$ i $d \mid p-1$. Ako je $\psi(d) = 0$, onda je $\psi(d) < \varphi(d)$. Stoga pretpostavimo da je $\psi(d) > 0$. Nadalje, neka je a broj koji pripada eksponentu d modulo p pa je

$$x^d \equiv 1 \pmod{p}. \tag{1.3}$$

Prema Lagrangeovu teoremu 1.3.1 kongruencija (1.3) ima najviše d rješenja. Očito brojevi

$$a, a^2, a^3, \ldots, a^d$$

zadovoljavaju kongruenciju (1.3) i međusobno su nekogruentni modulo p. Dakle, kongruencija (1.3) ima točno d rješenja. Neka su $x_1, \ldots, x_d$ rješenja od (1.3) u skupu $\{1, 2, \ldots, p-1\}$. Tada je

$$a^k \equiv x_k \pmod{p} \quad \text{i} \quad x_k^d \equiv 1 \pmod{p},\ k = 1, \ldots, d.$$

Prema teoremu 1.2.3 red broja a^k, za $k \in \{1, 2, \ldots, d\}$ jednak je $\dfrac{d}{\text{nzd}(d,k)}$. To znači da a^k ima red d ako i samo ako je $\text{nzd}(d,k) = 1$, a takvih je upravo $\varphi(d)$. Odnosno, među brojevima $x_1, \ldots, x_d \in \{1, 2, \ldots, p-1\}$ ih točno $\varphi(d)$ koji pripadaju eksponentu d. Time smo pokazali da ako u skupu $\{1, 2, \ldots, p-1\}$ postoji bar jedan element koji pripada eksponentu d, onda ih ima točno $\varphi(d)$. Dakle, za svaki djelitelj d od $p-1$ je $\psi(d) \leq \varphi(d)$ pa, kao što smo već napomenuli, zbog (1.2) slijedi $\psi(d) = \varphi(d)$. □

Korolar 1.3.3. *Za svaki prosti broj p postoji primitivni korijen modulo p. Štoviše, postoji točno $\varphi(p-1)$ međusobno nekongruentnih primitivnih korijena modulo p.*

Dokaz. U oznakama iz teorema 1.3.2 je $\psi(p-1) = \varphi(p-1)$, odnosno broj elemenata skupa $\{1, 2, \ldots, p-1\}$ koji pripadaju eksponentu $p-1$, a to su upravo primitivni korijeni modulo p, jednak je $\varphi(p-1)$. □

Prema prethodnoj tvrdnji slijedi da primitivni korijen modulo prosti broj p postoji, no ostaje nam još za objasniti kako ga efektivno odrediti. Za svaki od brojeva $a \in \{2, 3 \ldots, p-1\}$ dovoljno je ispitati da

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p},$$

za sve proste djelitelje q od $p-1$. Uočimo, da ako $a \in \{2, 3 \ldots, p-1\}$ nije primitivni korijen modulo p, onda ni potencije a^n, $n \geq 2$ neće biti primitivni korijeni modulo p (što slijedi prema teoremu 1.2.3).

Primjer 1.3.1. *Odredite sve međusobno nekongruentne primitivne korijene modulo* 11.

Rješenje. 1. način: Prema korolaru 1.3.3 slijedi da imamo točno $\varphi(10) = 4$ nekongruentna primitivna korijena modulo 11. Ispitujemo kandidate za primitivne korijene modulo 11 iz skupa $\{2, 3, \ldots, 10\}$. Budući da su jedini prosti djelitelji od $p - 1 = 10$ brojevi 2 i 5, slijedi da je $a \in \{2, 3, \ldots, 10\}$ primitivni korijen modulo 11 ako i samo ako vrijedi da

$$a^{\frac{p-1}{5}} = a^2 \not\equiv 1 \pmod{11},\ a^{\frac{p-1}{2}} = a^5 \not\equiv 1 \pmod{11}.$$

Provodimo ispitivanje za $a \in \{2, 3, \ldots, 10\}$ redom

- $a = 2$:
$$2^2 = 4 \not\equiv 1 \pmod{11},\ 2^5 = 32 \equiv -1 \not\equiv 1 \pmod{11},$$
pa je $a = 2$ primitivni korijen modulo 11;

- $a = 3$:
$$3^2 = 9 \not\equiv 1 \pmod{11},\ 3^5 = 243 \equiv 1 \pmod{11},$$
pa $a = 3$ nije primitivni korijen modulo 11, a stoga nisu ni $3^2 = 9$, $3^3 \mod 11 = 5$, $3^4 \mod 11 = 4$;

- $a = 6$:
$$6^2 = 36 \not\equiv 1 \pmod{11},\ 6^5 = 7776 \equiv -1 \not\equiv 1 \pmod{11},$$
pa je $a = 6$ primitivni korijen modulo 11;

- $a = 7$:
$$7^2 = 49 \not\equiv 1 \pmod{11},\ 7^5 = 16807 \equiv -1 \not\equiv 1 \pmod{11},$$
pa je $a = 7$ primitivni korijen modulo 11;

- $a = 8$:
$$8^2 = 64 \not\equiv 1 \pmod{11},\ 8^5 = 32768 \equiv -1 \not\equiv 1 \pmod{11},$$
pa je $a = 8$ primitivni korijen modulo 11.

Tu možemo stati s pretraživanjem jer nam je poznato da postoje točno 4 nekongruentna primitivna korijena modulo 11 i to su brojevi $2, 6, 7$ i 8.

2. način: Koristimo dokaz teorema 1.3.2. Iz prethodnog znamo da je $a = 2$ primitivni korijen modulo 11, odnosno broj $a = 2$ pripada eksponentu $\varphi(11) = 10$. Svaka od potencija a^k, $k = 1, \ldots, 10$, zadovoljava kongruenciju $x^{10} \equiv 1 \pmod{11}$, no samo oni za koje je $\text{nzd}(k, 10) = 1$ imaju red 10, a to je za $k = 1, 3, 7, 9$. Dakle, svi primitivni korijeni moduli 11 su:

$$2^1 = 2,\ 2^3 = 8,\ 2^7 \mod 11 = 7,\ 2^9 \mod 11 = 6.$$

□

1.4 Egzistencija primitivnih korijena

Pokazali smo da za svaki prosti broj p postoji primitivni korijen modulo p. U ovom odsječku pronaći ćemo sve prirodne brojeve n za koje postoji primitivni korijen modulo n. Najprije ćemo pokazati da postoji primitivni korijen modulo p^2 gdje je p neparan prost broj, a zatim i općenitije da postoji primitivni korijen modulo p^k za svaki $k \in \mathbb{N}$.

Teorem 1.4.1. *Neka je p neparan prost broj te neka je r primitivni korijen modulo p. Tada je r ili $r + p$ primitivni korijen modulo p^2.*

Dokaz. S obzirom da je r primitivni korijen modulo p, znamo da je red od r modulo p jednak $\varphi(p) = p - 1$. Neka je n red od r modulo p^2. Tada vrijedi

$$r^n \equiv 1 \pmod{p^2}.$$

Jasno je da vrijedi i

$$r^n \equiv 1 \pmod{p}.$$

S obzirom da je red od r modulo p jednak $p - 1$, prema propoziciji 1.1.7, vrijedi

$$p - 1 \mid n.$$

Analogno, jer je n red od r modulo p^2 vrijedi

$$n \mid \varphi(p^2) = p(p - 1).$$

Iz prethodne dvije relacije slijedi da je $n = p - 1$ ili $n = p(p - 1)$.

Ako je $n = p(p - 1)$, tada je r primitivni korijen modulo p^2 jer je red od r modulo p^2 jednak $\varphi(p^2)$.

Ako je $n = p - 1$, tada vrijedi

$$r^{p-1} \equiv 1 \pmod{p^2}. \tag{1.4}$$

Neka je $s = r + p$. S obzirom da je $s \equiv r \pmod{p}$, s je također primitivni korijen modulo p pa je red od s modulo p^2 jednak ili $p-1$ ili $p(p-1)$. Koristeći binomni teorem slijedi

$$s^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \cdots + p^{p-1}$$

$$\equiv r^{p-1} + (p-1)p \cdot r^{p-2} \pmod{p^2}.$$

Iz (1.4) slijedi

$$s^{p-1} \equiv 1 + (p-1)p \cdot r^{p-2} \equiv 1 - pr^{p-2} \pmod{p^2}.$$

Ako vrijedi $s^{p-1} \equiv 1 \pmod{p^2}$, tada je $pr^{p-2} \equiv 0 \pmod{p^2}$. Iz toga slijedi $r^{p-2} \equiv 0 \pmod{p}$ što je nemoguće jer $p \nmid r$ zato što je r primitivni korijen od p. Stoga $p-1$ nije red od s modulo p^2 pa jedino preostaje da $p(p-1)$ bude red od s modulo p^2, odnosno da je $\varphi(p^2)$ red od s modulo p^2. Dakle, $s = r + p$ je primitivni korijen od p^2. □

Primjer 1.4.1. *Pronađite primitivni korijen modulo* 7^2.

Rješenje. Najprije odredimo najmanji primitivni korijen modulo 7. Ispitujemo redom prirodne brojeve veće od 1. Kako je

$$2^3 \equiv 1 \pmod{7},$$

slijedi da 2 nije primitivni korijen modulo 7. Nadalje,

$$3^2 \equiv 2 \pmod{7},\ 3^3 \equiv 6 \pmod{7},$$

tj. $3^d \not\equiv 1 \pmod{7}$ za sve djelitelje od $\varphi(7) = 6$ koji su manji od 6. Stoga je $r = 3$ primitivni korijen modulo 7. Iz dokaza teorema 1.4.1 slijedi da red od 3 modulo 7 može poprimiti jednu od dvije vrijednosti: $p - 1 = 6$ i $\varphi(p^2) = 7^2 - 7 = 42$. No, kako je

$$3^6 \equiv 43 \not\equiv 1 \pmod{7^2},$$

zaključujemo da je

$$3^{42} \equiv 1 \pmod{7^2}$$

pa je $r = 3$ i primitivni korijen modulo 7^2. □

Teorem 1.4.2. *Neka je p neparan prosti broj. Tada postoji primitivni korijen modulo* p^k *za svaki prirodni broj k. Štoviše, ako je r primitivni korijen modulo* p^2*, tada je r primitivni korijen modulo* p^k *za svaki prirodni broj k.*

Dokaz. Prema teoremu 1.4.1, p postoji prirodni broj r koji je primitivni korijen modulo p i modulo p^2. To znači da

$$r^{p-1} \not\equiv 1 \pmod{p^2}. \tag{1.5}$$

Koristeći princip matematičke indukcije, dokazat ćemo da

$$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}, \tag{1.6}$$

za sve prirodne brojeve k, $k \geq 2$.

Baza: Slučaj $k = 2$ slijedi iz (1.5).

Pretpostavka: Pretpostavimo da (1.6) vrijedi za neki $k \geq 2$.

Korak: S obzirom da je $\text{nzd}(r, p) = 1$, slijedi i da je $\text{nzd}(r, p^{k-1}) = 1$ pa prema Eulerovom teoremu 1.1.4 vrijedi

$$r^{(p-1)p^{k-2}} = r^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}.$$

Dakle, postoji prirodan broj d takav da

$$r^{(p-1)p^{k-2}} = 1 + dp^{k-1},$$

pri čemu $p \nmid d$ zbog pretpostavke indukcije. Potenciranjem prethodne jednakosti s p dobivamo

$$\begin{aligned} r^{(p-1)p^{k-1}} &= (1 + dp^{k-1})^p \\ &= 1 + p(dp^{k-1}) + \binom{p}{2}(dp^{k-1})^2 + \ldots + (dp^{k-1})^p \\ &\equiv 1 + dp^k \pmod{p^{k+1}}. \end{aligned}$$

S obzirom da $p \nmid d$, slijedi

$$r^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}.$$

Dakle, (1.6) vrijedi za svaki prirodni broj k, $k \geq 2$.

Neka je n red od r modulo p^k. Prema propoziciji 1.1.7 vrijedi da $n \mid \varphi(p^k) = p^k(p-1)$. S obzirom da vrijedi $r^n \equiv 1 \pmod{p^k}$, to je i $r^n \equiv 1 \pmod{p}$. Nadalje, jer je r primitivni korijen modulo p, tj. red od r modulo p je $\varphi(p) = p - 1$, slijedi da $p - 1 \mid n$ (prema propoziciji 1.1.7).

Iz $p - 1 \mid n$ i $n \mid p^{k-1}(p-1)$ slijedi da je n oblika $p^t(p-1)$, pri čemu je $t \in \mathbb{N}$ takav da $0 \leq t \leq k - 1$. Ako je $t \leq k - 2$, tada vrijedi

$$r^{p^{k-2}(p-1)} = (r^{(p-1)p^t})^{p^{k-2-t}} \equiv 1 \pmod{p^k}$$

što je u kontradikciji s (1.6). Dakle, red od r modulo p^k je $p^{k-1}(p-1) = \varphi(p^k)$ pa je r također primitivni korijen modulo p^k.

□

Primjer 1.4.2. *Prema primjeru 1.4.1 i teoremu 1.4.2 slijedi da je* 3 *primitivni korijen modulo* 7^k *za sve* $k \in \mathbb{N}$.

U nastavku ćemo ispitati postoje li primitivni korijeni modulo 2^k, $k \in \mathbb{N}$. Znamo da 2 i $2^2 = 4$ imaju primitivne korijene 1 i 3, redom. Sljedeći teorem kaže da su to ujedno i jedine potencije broja 2 za koje postoji primitivni korijen.

Teorem 1.4.3. *Neka je a neparan prirodan broj i* $k \geq 3$ *prirodan broj, tada vrijedi*

$$a^{\frac{\varphi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \pmod{2^k}. \tag{1.7}$$

Dokaz. Koristit ćemo princip matematičke indukcije. Budući da je a neparan prirodan broj, vrijedi

$$a^2 \equiv 1 \pmod{8}.$$

Baza: Neka je $k = 3$. Kako je $\varphi(2^3) = 4$, imamo

$$a^{\frac{4}{2}} = a^2 \equiv 1 \pmod{2^3}.$$

pa vrijedi (1.7) za $k = 3$.

Pretpostavka: Pretpostavimo da za neki $k \geq 3$ vrijedi

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}. \tag{1.8}$$

Korak: Iz pretpostavke slijedi da postoji prirodni broj d takav da vrijedi

$$a^{2^{k-2}} = 1 + d \cdot 2^k.$$

Kvadriranjem obje strane jednakosti dobivamo

$$a^{2^{k-1}} = 1 + d \cdot 2^{k+1} + d^2 2^{2k}$$

iz čega slijedi

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}.$$

Prema principu matematičke indukcije, tvrdnja (1.7) vrijedi za $k \in \mathbb{N}, k \geq 3$.

□

Korolar 1.4.4. *Neka je* $k \in \mathbb{N}$, $k \geq 3$. *Ne postoji primitivni korijen modulo* 2^k.

Iako prema prethodnom teoremu zaključujemo da ne postoje potencije broja 2, osim 2 i 4 koje imaju primitivni korijen uvijek postoji prirodan broj čiji je red 2^{k-2} modulo 2^4, a to je najveći mogući red manji od $\varphi(2^k) = 2^{k-1}$.

Propozicija 1.4.5. *Neka je $k \in \mathbb{N}, k \geq 3$. Tada je red od 5 modulo 2^k jednak $\frac{\varphi(2^k)}{2} = 2^{k-2}$.*

Dokaz. Prema teoremu 1.4.3 slijedi

$$5^{2^{k-2}} \equiv 1 \pmod{2^k},$$

za $k \geq 3$. Neka je r red od 5 modulo 2^k. Prema propoziciji 1.1.7, znamo da $r \mid 2^{k-2}$. Ako pokažemo da $r \nmid 2^{k-3}$, tada slijedi da je $r = 2^{k-2}$. Koristeći princip matematičke indukcije pokazujemo da je

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k},$$

za $k \geq 3$.

Baza: Za $k = 3$ očito je $5 = 1 + 2^2 \pmod 8$.

Pretpostavka: Pretpostavimo da vrijedi

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}.$$

Korak: Iz pretpostavke slijedi da postoji prirodan broj takav da vrijedi

$$5^{2^{k-3}} = (1 + 2^{k-1}) + d \cdot 2^k.$$

Kvadriranjem obje strane jednakosti, dobivamo

$$5^{2^{k-2}} = (1 + 2^{k-1})^2 + 2d(1 + 2^{k-1})2^k + (2^k \cdot d)^2.$$

iz čega slijedi

$$5^{2^{k-2}} \equiv (1 + 2^{k-1})^2 = 1 + 2^k + 2^{2k-2} \equiv 1 + 2^k \pmod{2^{k+1}}$$

Time smo pokazali da

$$5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$$

za sve $k \geq 3$, pa 5 pripada eksponentu $r = \frac{\varphi(2^k)}{2} = 2^{k-2}$ modulo 2^k. □

Teorem 1.4.6. *Neka je n prirodan broj takav da $n \neq p^k$ i $n \neq 2p^k$, pri čemu je p prosti broj i $k \in \mathbb{N}$. Tada ne postoji primitivni korijen modulo n.*

Dokaz. Neka je n prirodan broj. Prema Osnovnom teoremu aritmetike, n se može prikazati na sljedeći način

$$n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m},$$

pri čemu su $p_1, p_2, \ldots, p_m$ različiti prosti brojevi te $t_1, t_2, \ldots, t_m$ prirodni brojevi.

Pretpostavimo da je r primitivni korijen modulo n. Tada je $\text{nzd}(r,n) = 1$ i red od r modulo n jednak je $\varphi(n)$. S obzirom da je $\text{nzd}(r,n) = 1$, slijedi da je $\text{nzd}(r,p^t) = 1$ za sve $t = 1, 2, \ldots, m$. Prema Eulerovom teoremu 1.1.4, vrijedi

$$r^{\varphi(p^t)} \equiv 1 \pmod{p^t}.$$

Neka je U najmanji zajednički višekratnik od brojeva $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \ldots, \varphi(p_m^{t_m})$. Stoga $\varphi(p_i^{t_i}) \mid U$ i

$$r^U \equiv 1 \pmod{p_i^{t_i}}$$

za sve $i = 1, 2, \ldots, m$. Budući da su $p_1^{t_1}, p_2^{t_2}, \ldots, p_m^{t_m}$ u parovima relativno prosti brojevi, slijedi

$$r^U \equiv 1 \pmod{n}.$$

Iz činjenice da je red od r modulo n jednak $\varphi(n)$ i propozicije 1.1.7 zaključujemo da je

$$\varphi(n) \leq U. \tag{1.9}$$

Eulerova funkcija je multiplikativna pa je stoga

$$\varphi(n) = \varphi(p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}) = \varphi(p_1^{t_1})\varphi(p_2^{t_2}) \cdots \varphi(p_m^{t_m}).$$

Iz (1.9) sada slijedi

$$\varphi(p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}) = \varphi(p_1^{t_1})\varphi(p_2^{t_2}) \cdots \varphi(p_m^{t_m}) \leq U,$$

što znači da je produkt prirodnih brojeva manji ili jednak od njihovog najmanjeg zajedničkog višekratnika. To je jedino moguće ako su brojevi

$$\varphi(p_1^{t_1}) = p_1^{t_1-1}(p_1 - 1),\ \varphi(p_2^{t_2}) = p_2^{t_2-1}(p_2 - 1), \ldots,\ \varphi(p_m^{t_m}) = p_m^{t_m-1}(p_m - 1)$$

u parovima relativno prosti. To može biti ispunjeno samo u sljedeća dva slučaja:

- $m = 1$ i n je potencija prostog broja, tj. $n = p_1^{t_1}$;
- $m = 2$ i $n = 2p_2^{t_2}$, gdje je p_2 neparan prost broj.

No, to je u proturječju s pretpostavkom teorema $n \neq p^k$ i $n \neq 2p^k$ pa zaključujemo da ne postoji primitivni korijen modulo n. □

Promotrimo prirodne brojeve n oblika $n = 2p^t$, pri čemu je p neparan prost broj i $t \in \mathbb{N}$.

Teorem 1.4.7. *Ako je p neparan prost broj i $t \in \mathbb{N}$, tada $2p^t$ ima primitivni korijen. Štoviše, ako je r primitivni korijen modulo p^t i*

- *r neparan broj, tada je r primitivni korijen modulo* $2p^t$*;*
- *r paran broj, tada je* $r + p^t$ *primitivan korijen modulo* $2p^t$.

Dokaz. Prema teoremu 1.4.2 postoji r – primitivni korijen modulo p^t, to jest takav da je

$$r^{\varphi(p^t)} \equiv 1 \pmod{p^t}$$

pri čemu ne postoji $1 \leq k < \varphi(p^t)$ za koji je $r^k \equiv 1 \pmod{p^t}$. Zbog multiplikativnosti Eulerove funkcije (jer je $\text{nzd}(2, p^t) = 1$) je

$$\varphi(2p^t) = \varphi(2)\varphi(p^t) = \varphi(p^t),$$

pa slijedi

$$r^{\varphi(2p^t)} \equiv 1 \pmod{p^t}.$$

Razlikujemo dva slučaja: r neparan i r paran broj.

- 1. slučaj: Ako je r neparan, tada iz

  $$r^{\varphi(2p^t)} \equiv 1 \pmod{2},\ r^{\varphi(2p^t)} \equiv 1 \pmod{p^t}$$

  slijedi da je $\varphi(2p^t)$ najmanja potencija od r koja je kongruentna 1 modulo $2p^t$. (Kada bi postojala manja potencija, tada bi također bila kongruentna 1 modulo p^t što je u kontradikciji s pretpostavkom da je r primitivni korijen modulo p^t). Dakle, r je primitivni korijen modulo $2p^t$ kada je r neparan.

- 2. slučaj: Ako je r paran broj, tada je $r + p^t$ neparan broj pa je

  $$(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{2}.$$

  Nadalje, kako $r + p^t \equiv r \pmod{p^t}$ slijedi

  $$(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{p^t}$$

  i zaključujemo $(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{p^t}$ jer je $(r + p^t)^{\varphi(2p^t)}$ najmanja moguća potencija od $r + p^t$ koja je kongruentna 1 modulo $2p^t$. (Postojanje manje potencije dovodilo bi do kontradikcije s pretpostavkom da je r primitivni korijen modulo p^t). Stoga je $r + p^t$ primitivni korijen modulo $2p^t$ kada je r paran.

Pokazali smo da r primitivni korijen modulo $2p^t$ kada je r neparan te da je $r + p^t$ primitivni korijen modulo $2p^t$ kada je r paran. □

Primjer 1.4.3. *Pronađite primitivni korijen modulo* $2 \cdot 7^k$.

Rješenje. U primjeru 1.4.2 pokazali smo da je 3 primitivni korijen modulo $7^k, k \in \mathbb{N}$. S obzirom da je 3 neparan broj, prema teoremu 1.4.7 zaključujemo da je 3 primitivni korijen modulo $2 \cdot 7^k$. □

Konačno, prema teoremima 1.4.2, 1.4.6, 1.4.7 i korolaru 1.4.4 slijedi važan zaključak:

Teorem 1.4.8. *Prirodan broj $n, n > 1$ ima primitivni korijen ako i samo ako je*

$$n = 2, 4, p^t \ \ ili \ \ 2p^t,$$

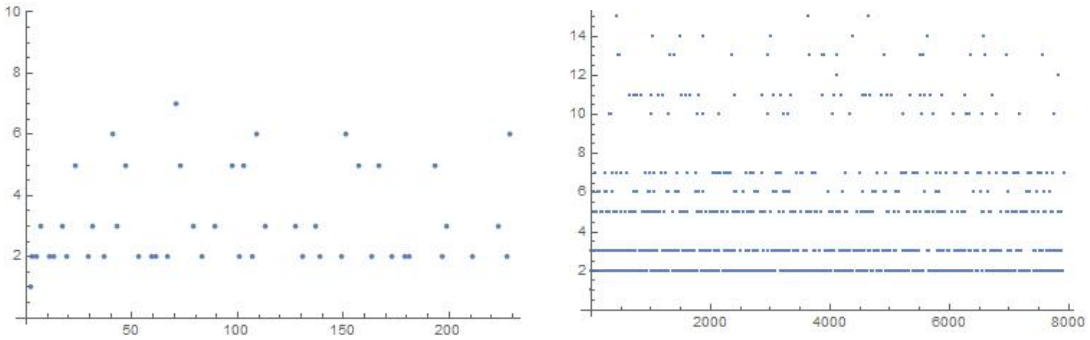
pri čemu je p prosti broj i $t \in \mathbb{N}$.

U tablici 1.1 nalaze se svi prirodni brojevi $n \leq 100$ koji imaju primitivne korijene i njihovi najmanji primitivni korijeni r, a u tablici 1.2 navodimo skupove svih primitivnih korijena modulo n za $n \leq 50$.

n	2	3	4	5	6	7	9	10	11	13	14	17	18	19	22	23	25
r	1	2	3	2	5	3	2	7	2	2	3	3	11	2	13	5	2
n	26	27	29	31	34	37	38	41	43	46	47	49	50	53	54	58	59
r	15	2	2	3	3	2	21	6	3	5	5	3	27	2	29	31	2
n	61	62	67	71	73	74	79	81	82	83	86	89	94	97	98		
r	2	3	2	7	5	39	3	2	47	2	3	3	5	5	3		

Tablica 1.1: Tablica najmanjih primitivnih korijena modulo n za $1 \leq n \leq 100$

Na slikama u 1.1 dani su grafički prikazi najmanjih primitivnih korijena modulo prosti broj p za $p < 50$ i $p < 1000$.



Slika 1.1: Primitivni korijen modulo prosti broj p za $p < 50$ (lijevo) i $p < 1000$ (desno)

n	skup svih primitivnih korijena modulo n
2	$\{1\}$
3	$\{2\}$
4	$\{3\}$
5	$\{2, 3\}$
6	$\{5\}$
7	$\{3, 5\}$
9	$\{2, 5\}$
10	$\{3, 7\}$
11	$\{2, 6, 7, 8\}$
13	$\{2, 6, 7, 11\}$
14	$\{3, 5\}$
17	$\{3, 5, 6, 7, 10, 11, 12, 14\}$
18	$\{5, 11\}$
19	$\{2, 3, 10, 13, 14, 15\}$
22	$\{7, 13, 17, 19\}$
23	$\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$
25	$\{2, 3, 8, 12, 13, 17, 22, 23\}$
26	$\{7, 11, 15, 19\}$
27	$\{2, 5, 11, 14, 20, 23\}$
29	$\{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27\}$
31	$\{3, 11, 12, 13, 17, 21, 22, 24\}$
34	$\{3, 5, 7, 11, 23, 27, 29, 31\}$
37	$\{2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35\}$
38	$\{3, 13, 15, 21, 29, 33\}$
41	$\{6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35\}$
43	$\{3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34\}$
46	$\{5, 7, 11, 15, 17, 19, 21, 33, 37, 43\}$
47	$\{5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45\}$
49	$\{3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47\}$
50	$\{3, 13, 17, 23, 27, 33, 37, 47\}$

Tablica 1.2: Tablica svih primitivnih korijena modulo n za $1 \leq n \leq 50$

Poglavlje 2

Primjena primitivnih korijena

2.1 Indeksi

Neka je r primitivni korijen modulo m, $m \in \mathbb{N}$. Prema teoremu 1.2.2 slijedi da skup

$$\{1, r, r^2, \ldots, r^{\varphi(m)-1}\}$$

čini reducirani sustav ostataka modulo m. Stoga, ako je $\text{nzd}(a, m) = 1, a \in \mathbb{N}$, tada postoji jedinstven x, $0 \leq x \leq \varphi(m) - 1$ takav da je

$$r^x \equiv a \pmod{m}. \tag{2.1}$$

Definicija 2.1.1. *Neka je m prirodan broj, r primitivni korijen modulo m, te $a \in \mathbb{Z}$ relativno prost s m. Eksponent $x \in \{0, 1, \ldots, \varphi(m) - 1\}$ za koji vrijedi* (2.1) *se naziva* indeks *ili* diskretni logaritam *od a u odnosu na r modulo m i označava se s* $\text{ind}_r a$ *ili* $\text{ind}\, a$.

Iz definicije 2.1.1 slijedi

$$r^{\text{ind}_r a} \equiv a \pmod{m}. \tag{2.2}$$

Primjer 2.1.1. *Odredite* $\text{ind}_r a$ *gdje je r primitivni korijen modulo* 7 *i* $a \in \mathbb{Z}$, $\text{nzd}(a, 7) = 1$.

Rješenje. U primjeru 1.4.1 odredili smo najmanji primitivni korijen modulo 7 i on je jednak $r = 3$. Nije moguće direktno izračunati $\text{ind}_r a$, već je potrebno redom odrediti sve potencije $r^k \mod 7$ za $k = \{0, 1, \ldots, \varphi(7) - 1 = 5\}$. Iz

$$3^0 \equiv 1 \pmod{7},\ 3^1 \equiv 3 \pmod{7},\ 3^2 \equiv 2 \pmod{7},$$

$$3^3 \equiv 6 \pmod{7},\ 3^4 \equiv 4 \pmod{7},\ 3^5 \equiv 5 \pmod{7},$$

dobivamo

$$\text{ind}_3 1 = 0,\ \text{ind}_3 2 = 2,\ \text{ind}_3 3 = 1,$$

$$\text{ind}_3\, 4 = 4,\ \text{ind}_3\, 5 = 5,\ \text{ind}_3\, 6 = 3.$$

Ako uzmemo neki drugi primitivni korijen od 7, na primjer 5, dobivamo različite indekse:

$$\text{ind}_5\, 1 = 0,\ \text{ind}_5\, 2 = 4,\ \text{ind}_5\, 3 = 5,$$

$$\text{ind}_5\, 4 = 2,\ \text{ind}_5\, 5 = 1,\ \text{ind}_5\, 6 = 3.$$

□

Indeksi imaju brojna svojstva slična logaritmima pri čemu su jednakosti zamijenjene s kongruencijama modulo $\varphi(m)$.

Teorem 2.1.2. *Neka je $m > 1$ prirodan broj, a, b cijeli brojevi koji su relativno prosti s m te r primitivni korijen modulo m. Tada vrijedi:*

(i) $\text{ind}_r\, 1 \equiv 0 \pmod{\varphi(m)}$;

(ii) $\text{ind}_r(ab) \equiv \text{ind}_r\, a + \text{ind}_r\, b \pmod{\varphi(m)}$;

(iii) $\text{ind}_r\, a^k \equiv k \cdot \text{ind}_r\, a \pmod{\varphi(m)}$, $k \in \mathbb{N}$.

Dokaz. (i) Prema Eulerovom teoremu 1.1.4, vrijedi

$$r^{\varphi(m)} \equiv 1 \pmod{m}.$$

r je primitivni korijen modulo m pa ne postoji manja pozitivna potencija od r koja je kongruentna 1 modulo m. Slijedi

$$\text{ind}_r\, 1 \equiv 0 \pmod{\varphi(m)}.$$

(ii) Prema relaciji (2.2) je

$$r^{\text{ind}_r\, ab} \equiv ab \pmod{m} \tag{2.3}$$

i

$$r^{\text{ind}_r\, a + \text{ind}_r\, b} \equiv r^{\text{ind}_r\, a} \cdot r^{\text{ind}_r\, b} \equiv ab \pmod{m}. \tag{2.4}$$

Iz kongruencija (2.3) i (2.4) slijedi

$$r^{\text{ind}_r\, ab} \equiv r^{\text{ind}_r\, a + \text{ind}_r\, b} \pmod{m}.$$

Prema teoremu 1.1.8 slijedi

$$\text{ind}_r\, ab \equiv \text{ind}_r\, a + \text{ind}_r\, b \pmod{\varphi(m)}$$

(iii) Prema relaciji (2.2) je

$$r^{\operatorname{ind}_r a^k} \equiv a^k \pmod{m} \tag{2.5}$$

i

$$r^{k\cdot\operatorname{ind}_r a} \equiv (r^{\operatorname{ind}_r a})^k \pmod{m}. \tag{2.6}$$

Iz kongruencija (2.5) i (2.6) zaključujemo da vrijedi

$$r^{\operatorname{ind}_r a^k} \equiv r^{k\cdot\operatorname{ind}_r a}.$$

Koristeći teorem 1.1.8 dobivamo

$$\operatorname{ind}_r a^k \equiv k \cdot \operatorname{ind}_r a \pmod{\varphi(m)}.$$

□

Primjer 2.1.2. *Odredite* $\operatorname{ind}_5 24$ *i* $\operatorname{ind}_5 16$ *modulo* 7 *koristeći indekse* $\operatorname{ind}_5 2 = 4$ *i* $\operatorname{ind}_5 3 = 5$.

Rješenje. Prema teoremu 2.1.2 je

$$\operatorname{ind}_5 24 = \operatorname{ind}_5 8 \cdot 3 \equiv \operatorname{ind}_5 8 + \operatorname{ind}_5 3 \equiv 3\operatorname{ind}_5 2 + \operatorname{ind}_5 3 = 17 \equiv 5 \pmod{6},$$

$$\operatorname{ind}_5 16 = \operatorname{ind}_5 2^4 \equiv 4\operatorname{ind}_5 2 = 4 \cdot 4 \equiv 4 \pmod{6}.$$

Na drugi način, iz $24 \equiv 3 \pmod 7$ slijedi da je $\operatorname{ind}_5 24 = \operatorname{ind}_5 3 = 5$, a iz $16 \equiv 2 \pmod 7$ da je $\operatorname{ind}_5 16 = \operatorname{ind}_5 2 = 4$. □

2.2 Rješavanje nekih kongruencija pomoću indeksa

Neka je p polinom s cjelobrojnim koeficijentima. Izraz oblika

$$p(x) \equiv 0 \pmod{m}$$

nazivamo *polinomijalna kongruencija*. *Broj rješenja* polinomijalne kongruencije je broj međusobno nekongruentnih rješenja, odnosno broj rješenja u potpunom sustavu ostataka modulo m. Polinomijalne kongruencije oblika

$$ax^n \equiv b \pmod{m}, \tag{2.7}$$

gdje su $a, b \in \mathbb{Z}$ i $m, n \in \mathbb{N}$, mogu se riješiti pomoću indeksa uz uvjet da postoji primitivni korijen modulo m. Naime, prema teoremu 2.1.2 slijedi da je

$$\operatorname{ind}_r a + n\operatorname{ind}_r x \equiv \operatorname{ind}_r b \pmod{\varphi(m)}.$$

To znači da se kongruencija (2.7) svodi na rješavanje linearne kongruencije

$$n \cdot y \equiv \operatorname{ind}_r b - \operatorname{ind}_r a \pmod{\varphi(m)},$$

pri čemu je $y = \operatorname{ind}_r x$. Prethodna linearna kongruencija ima rješenja ako i samo $d = \operatorname{nzd}(n, \varphi(m))$ dijeli broj $\operatorname{ind}_r b - \operatorname{ind}_r a$, a ako je rješiva broj rješenja je upravo jednak d. U specijalnom slučaju vrijedi sljedeća propozicija.

Propozicija 2.2.1. *Neka je $n \in \mathbb{N}$ i p prosti broj. Ako je* $\operatorname{nzd}(n, p-1) = 1$*, onda kongruencija*

$$x^n \equiv a \pmod{p}$$

ima jedinstveno rješenje.

Dokaz. Iz $x^n \equiv a \pmod{p}$ prema teoremu 2.1.2(iii) slijedi

$$n \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}.$$

Uz $y = \operatorname{ind} x$ prethodna linearna kongruencija $n \cdot y \equiv \operatorname{ind} a \pmod{p-1}$ ima jedinstveno rješenje y_0 u skupu $\{0, 1, \ldots, p-2\}$ jer je $\operatorname{nzd}(n, p-1) = 1$. Stoga početna kongruencija ima jedinstveno rješenje $x_0 = r^{y_0}$ (pri čemu je r primitivni korijen modulo p). □

Primjer 2.2.1. *Riješimo kongruenciju* $6x^{12} \equiv 11 \pmod{17}$.

Rješenje. Najmanji primitivni korijen od 17 je $r = 3$. Dana kongruencija ekvivalentna je kongruenciji

$$\operatorname{ind}_3 6 + 12 \cdot \operatorname{ind}_3 x \equiv \operatorname{ind}_3 11 \pmod{16}.$$

U sljedećoj tablici odredimo sve $r^k \mod 17$ za $k = 0, 1, \ldots, 15$:

$k = \operatorname{ind}_3 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^k \mod 17 = a$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Iz tablice očitamo da je $\operatorname{ind}_3 11 = 7$ i $\operatorname{ind}_3 6 = 15$ pa je

$$12 \cdot \operatorname{ind}_3 x \equiv 8 \pmod{16}.$$

S obzirom da je $\operatorname{nzd}(12, 16) = 4$ i $4 \mid 8$, postoje točno četiri nekongruentna rješenja (modulo 16) takva da je

$$3 \cdot \operatorname{ind}_3 x \equiv 2 \pmod{4},$$

odnosno

$$-\operatorname{ind}_3 x \equiv 2 \pmod{4}.$$

To znači da je

$$\operatorname{ind}_3 x \equiv 2, 6, 10, 14 \pmod{16},$$

odnosno da su

$$x \equiv 3^2, 3^6, 3^{10}, 3^{14} \equiv 9, 15, 8, 2 \pmod{17}$$

sva rješenja kongruencije $6x^{12} \equiv 11 \pmod{17}$. □

Neka je $\text{nzd}(a, m) = 1$. Pomoću indeksa mogu se riješiti i eksponencijalne kongruencije oblika

$$a^x \equiv b \pmod{m}. \tag{2.8}$$

Ako postoji r – primitivni korijen modulo m, onda je prethodna kongruencija ekvivalentna linearnoj kongruenciji

$$x \cdot \text{ind}_r\, a \equiv \text{ind}_r\, b \pmod{\varphi(m)}.$$

Uočimo da ako je x_0 rješenje od (2.8), onda su rješenja i svi cijeli brojevi oblika $x_0 + k \cdot d$, tj. $x \equiv x_0 \pmod{d}$, gdje je d red od a modulo m. Zaista,

$$a^{x_0+k\cdot d} = a^{x_0} a^{k\cdot d} \equiv b \cdot 1 = b \pmod{m}.$$

Primjer 2.2.2. *Pronađite sva rješenja kongruencije* $3^x \equiv 2 \pmod{23}$.

Rješenje. Kako je $r = 5$ najmanji primitivni korijen modulo 23, dobivamo

$$x \cdot \text{ind}_5\, 3 \equiv \text{ind}_5\, 2 \pmod{22}.$$

Pomoću tablice

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$\cdots$
$5^k \mod 23$	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	$\cdots$

dobijemo da je $\text{ind}_5\, 2 = 2$ i $\text{ind}_5\, 3 = 16$ pa je

$$16 \cdot x \equiv 2 \pmod{22},$$

to jest

$$8 \cdot x \equiv 1 \pmod{11}.$$

Sva rješenja prethodne, ali i početne kongruencije $3^x \equiv 2 \pmod{23}$ su

$$x \equiv 7 \pmod{11}.$$

(Uočimo da je 11 upravo red od 3 modulo 23). □

2.3 Testovi prostosti

Testovi prostosti su algoritmi pomoću kojih se provjerava je li neki broj prost. Najjednostavnija provjera prostosti broja n sastoji se od uzastopnog dijeljenja broja n prostim brojevima manjim od $\sqrt{n}$. No, taj test je neefikasan pa ćemo stoga predstaviti neke učinkovitije testove prostosti koji imaju veze s primitivnim korijenima modulo prosti broj p. Prisjetimo se da ako za cijeli broj a i prosti broj p vrijedi da

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p},$$

za sve proste djelitelje q od $p-1$, onda je a primitivni korijen modulo p, odnosno a^{p-1} je najmanja potencija broja a koja je kongruentna 1 modulo p. Postavlja se pitanje što ako prethodni uvjeti umjesto za prosti broj p vrijede za neki prirodan broj n – mora li n tada biti prost? Odgovor je potvrdan. Dakle, ako postoji cijeli broj čiji je red modulo n jednak $n-1$, onda je n prost broj. Na tome se upravo bazira tzv. *Lucasov test prostosti*.

Teorem 2.3.1 (Lucasov test prostosti)**.** *Neka je $n \in \mathbb{N}$, $n > 2$. Ako postoji $x \in \mathbb{Z}$ takav da vrijedi*

$$x^{n-1} \equiv 1 \pmod{n} \quad i \quad x^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$$

za sve proste brojeve q koji dijele $n-1$, tada je n prost broj.

Dokaz. Ako je $x^{n-1} \equiv 1 \pmod{n}$, prema propoziciji 1.1.7 vrijedi $d \mid (n-1)$ pri čemu je d red od x modulo n. Dokazat ćemo da je $d = n-1$.

Pretpostavimo suprotno, tj. da $d \neq n-1$. S obzirom da $d \mid (n-1)$, postoji $k \in \mathbb{N}$, $k > 1$, takav da $n-1 = k \cdot d$. Neka je q prost broj takav da je $q \mid k$. Tada vrijedi

$$x^{\frac{n-1}{q}} = x^{\frac{k \cdot d}{q}} = (x^d)^{\frac{k}{q}} \equiv 1 \pmod{n},$$

čime smo došli do kontradikcije s pretpostavkom. Dakle, $d = n-1$.

S obzirom da vrijedi $d \leq \varphi(n)$ i $\varphi(n) \leq n-1$, slijedi $\varphi(n) = n-1$. Dakle, n je prost broj. □

Vrijedi i sljedeća varijanta Lucasovog testa prostosti.

Korolar 2.3.2. *Neka je n neparan prirodan broj. Ako je $x \in \mathbb{Z}$ takav da vrijedi*

$$x^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad i \quad x^{\frac{n-1}{q}} \not\equiv -1 \pmod{n},$$

za sve neparne proste djelitelje q od n, onda je n prost broj.

Dokaz. Vrijedi $x^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, pa iz toga slijedi

$$x^{n-1} = (x^{\frac{n-1}{2}})^2 \equiv (-1)^2 \equiv 1 \pmod{n}.$$

Prema prethodnom teoremu 2.3.1 slijedi da je n prost broj. □

Primjer 2.3.1. *Pomoću Lucasovog testa prostosti provjerite je li broj* 2003 *prost broj.*

Rješenje. Neka je $n = 2003$. Tada je $n - 1 = 2002$. Neparni prosti djelitelji od 2002 su 7, 11 i 13. Za vrijednosti iz $x \in \{2, \ldots, 2002\}$ provjeravamo uvjete korolara 2.3.2. Za $x = 2$ vrijedi

$$2^{\frac{2002}{2}} = 2^{1001} \equiv -1 \pmod{2003}, 2^{\frac{2002}{7}} = 2^{286} \equiv 1 \pmod{2003},$$

a to znači da $x = 2$ nije prošao test iz korolara 2.3.2 pa ne možemo zaključiti da je prost. Za $x = 3$ je

$$3^{\frac{2002}{2}} = 3^{1001} \equiv 1 \pmod{2003},$$

odnosno ni $x = 3$ ne prolazi test. Budući da 2 nije prošao test, neće proći ni $4 = 2^2$ pa zato testiramo $x = 5$. Vrijedi

$$5^{\frac{2002}{2}} = 5^{1001} \equiv -1 \pmod{2003}, \quad 5^{\frac{2002}{7}} = 5^{286} \equiv 874 \pmod{2003},$$

$$5^{\frac{2002}{11}} = 5^{183} \equiv 886 \pmod{2003}, \quad 5^{\frac{2002}{13}} = 5^{154} \equiv 633 \pmod{2003}.$$

Dakle, $x = 5$ je prošao test iz korolara2.3.2 što znači da je 2003 prost broj. □

Kod primjene Lucasovog testa za ispitivanje prostosti danog broja n se izabiru slučajni brojevi iz skupa $\{2, 3, \ldots, n-1\}$. Ako test ne prolazi za dovoljan broj kandidata, tada se ne može zaključiti da je n složen, već da je *vjerojatno složen*. U suprotnom, ako se pronađe $x \in \{2, 3, \ldots, n-1\}$ za kojeg vrijede uvjeti iz teorema 2.3.1 ili korolara 2.3.2, tada je n sigurno prost. Broj $x < n$ za koji je $x^{n-1} \equiv 1 \pmod{n}$ zove se *Fermatov svjedok* složenosti broja n.

Za primjenu Lucasovog testa prostosti potrebna nam je faktorizacija broja $n - 1$. Taj proces može biti dugotrajan ako je broj n velik. Test prostosti kojeg je iskazao Henry Pocklington koristi parcijalnu faktorizaciju od $n - 1$, tj. $n - 1 = F \cdot R$ pri čemu je poznat kanonski rastav broja F na proste faktore, a R je tzv. ostatak faktorizacije koji je manji od F i čiji kanonski rastav ne poznajemo.

Teorem 2.3.3 (Pocklingtonov test prostosti)**.** *Neka je n prirodan broj takav da je* $n - 1 = F \cdot R$ *pri čemu su ispunjeni sljedeći uvjeti*

- $F = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, *gdje su* $p_1, \cdots, p_r$ *različiti prosti brojevi,* $\alpha_1, \cdots, \alpha_r \in \mathbb{N}$;
- $\text{nzd}(F, R) = 1$;
- $R < F$.

Ako za svaki $i \in \{1, \ldots, r\}$ *postoji* $a_i \in \mathbb{N}$ *takav da je*

$$a_i^{n-1} \equiv 1 \pmod{n} \quad i \quad \text{nzd}(a_i^{\frac{n-1}{p_i}} - 1, n) = 1, \tag{2.9}$$

tada je n prost broj.

Dokaz. Neka je p prosti djelitelj od n takav da $p \leq \sqrt{n}$. Iz pretpostavke da je $a_i^{n-1} \equiv 1 \pmod{n}$ slijedi da je

$$a_i^{n-1} \equiv 1 \pmod{p},\ i = 1, \ldots, r.$$

Nadalje, ako je r_i red od a_i modulo p_i, tada $r_i \mid (n-1)$, odnosno

$$n - 1 = t_i \cdot r_i,$$

za neki $t_i \in \mathbb{N}$. S druge strane je

$$n - 1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \cdot R.$$

Pretpostavimo da p_i dijeli t_i, za neki $i \in \{1, \ldots, r\}$. Tada je

$$a_i^{\frac{n-1}{p_i}} = a_i^{r_i \cdot \frac{t_i}{p_i}} \equiv 1 \pmod{p},$$

odnosno

$$p \mid a_i^{\frac{n-1}{p_i}} - 1.$$

Budući da $p \mid n$ to povlači da

$$p_i \mid \text{nzd}(a_i^{\frac{n-1}{p_i}} - 1, n) = 1,$$

što nije moguće, odnosno zaključujemo da p_i ne dijeli t_i. Stoga jedino preostaje da

$$p_i^{\alpha_i} \mid r_i.$$

Nadalje, kako r_i dijeli $p - 1$, slijedi da $p_i^{\alpha_i} \mid p - 1$, za sve $1, \ldots, r$. Budući da su $p_1, \ldots, p_r$ različiti prosti brojevi, dobivamo da

$$F = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \mid p - 1.$$

Dakle, $F < p$ pa zbog $R < F$ dobivamo sljedeće nejednakosti

$$n - 1 = F \cdot R < F^2 < p^2.$$

Otuda je $p > \sqrt{n}$. Stoga, n nema prostog djelitelja manjeg ili jednakog od $\sqrt{n}$ pa je n prosti broj. □

Primjer 2.3.2. *Pokažite da je* 23801 *prost broj koristeći Pocklingtonov test prostosti.*

Rješenje. Neka je $n = 23801$ te $n - 1 = 23800 = FR$, pri čemu je

$$F = 200 = 2^3 5^2, \ R = 119.$$

Vrijede uvjeti teorem 2.3.3: $\text{nzd}(F, R) = 1$ i $F > R$. Nadalje, za $a = 3$ vrijedi

$$3^{23800} \equiv 1 \pmod{23801}.$$

Sada još treba provjeriti drugi uvjet iz (2.9):

$$\text{nzd}(a^{\frac{n-1}{p_i}} - 1, n) = 1,$$

za $p_1 = 2$ i $p_2 = 5$. Kako je

$$3^{\frac{23800}{2}} \equiv -1 \pmod{23801}, \ 3^{\frac{23800}{5}} \equiv 19672 \pmod{23801},$$

slijedi

$$\text{nzd}(3^{\frac{23800}{2}} - 1, 23801) = \text{nzd}(-2, 23801) = 1,$$
$$\text{nzd}(3^{\frac{23800}{5}} - 1, 23801) = \text{nzd}(19671, 23801) = 1.$$

Dakle $n = 23801$ je prost broj.

Kada bismo koristili teorem 2.3.1, morali bismo provesti testiranje i za proste djelitelje 7 i 17 jer je $23801 = 2^3 \cdot 5^2 \cdot 7 \cdot 17$. □

Nadalje ćemo navesti test prostosti koji je koristan za testiranje brojeva koji imaju oblik $n = k \cdot 2^m + 1$ pri čemu je k neparan prirodan broj i $m \in \mathbb{Z}$ takav da $k < 2^m$. Brojevi tog oblika se nazivaju *Prothovi brojevi*.

Korolar 2.3.4 (Prothov test prostosti)**.** *Neka je n prirodan broj oblika $n = k \cdot 2^m + 1$, pri čemu je k neparan prirodan broj i $m \in \mathbb{Z}$ takav da $k < 2^m$. Ako postoji $a \in \mathbb{Z}$ takav da*

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

tada je n prost broj.

Dokaz. Neka je $s = 2^m$ i $t = k$, takav da $s > t$. Ako je

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}, \tag{2.10}$$

pokazat ćemo da vrijedi $\text{nzd}(a^{\frac{n-1}{2}} - 1, n) = 1$. Ako $d \mid (a^{\frac{n-1}{2}} - 1)$ i $d \mid n$, tada prema kongruenciji (2.10) slijedi $d \mid (a^{\frac{n-1}{2}} + 1)$. Dakle, d dijeli $(a^{\frac{n-1}{2}} - 1) + (a^{\frac{n-1}{2}} + 1) = 2$. Znamo da je d prost broj pa slijedi da je $d = 1$. Prema teoremu 2.3.1, n je prost broj. □

Primjer 2.3.3. *Pokažite da je broj* 3329 *prost broj.*

Rješenje. Primjetimo da je $n = 3329 = 13 \cdot 2^8 + 1$ i $13 < 2^8 = 256$. Za $a = 3$ vijedi

$$3^{\frac{n-1}{2}} = 3^{\frac{3328}{2}} = 3^{1664} \equiv -1 \pmod{3329}.$$

Prema korolaru 2.3.4 slijedi da je 3329 prost broj. □

Pomoću Prothovog testa prostosti pokazalo se da su mnogi Prothovi brojevi prosti. Prvih desetak prostih Prothovih brojeva je

$$3 = 2 + 1, 5 = 2^2 + 1, 13 = 3 \cdot 2^2 + 1, 17 = 2^4 + 1, 41 = 5 \cdot 2^2 + 1, 97 = 3 \cdot 2^5 + 1,$$

$$113 = 7 \cdot 2^4 + 1, 193 = 3 \cdot 2^6 + 1, 241 = 15 \cdot 2^4 + 1, 257 = 2^8 + 1, 353 = 11 \cdot 2^5 + 1.$$

Do sada najveći pronađeni prosti Prothov broj je $10223 \cdot 2^{31172165} + 1$ – broj s 9 383 761 znamenaka, a pronađen je 2016. godine. U tablici 2.1 dani su najveći do sada pronađeni prosti Prothovi brojevi. Napomenimo da ih se često dovodi u vezu s s Fermatovim brojevima $F_n = 2^{2^n} + 1$ jer su jedini mogući djelitelji broja F_n upravo Prothovi brojevi.

Mjesto	Broj	Broj znamenaka	Godina
1	$10223 \cdot 2^{31172165} + 1$	9 383 761	2016
2	$202705 \cdot 2^{21320516} + 1$	6 418 121	2021
3	$168451 \cdot 2^{19375200} + 1$	5 832 522	2017
4	$7 \cdot 2^{18233956} + 1$	5 488 969	2020
5	$3 \cdot 2^{16408818} + 1$	4 939 547	2020

Tablica 2.1: Prvih 5 najvećih Prothovih prostih brojeva

Najveći do sada pronađeni prosti brojevi su oblika $2^p - 1$, gdje je p prosti broj i nazivaju se prosti Mersennovi brojevi. Među 10 najvećih do sada otkrivenih prostih brojeva nalazi se i jedan Prothov prosti broj (tablica 2.2).

Mjesto	Broj	Broj znamenaka	Godina
1	$2^{82589933} - 1$	24 862 048	
2	$2^{77232917} - 1$	23 249 425	
3	$2^{74207281} - 1$	22 338 618	
4	$2^{57885161} - 1$	17 425 170	
5	$2^{43112609} - 1$	12 978 189	
6	$2^{42643801} - 1$	12 837 064	
7	$2^{37156667} - 1$	11 185 272	
8	$2^{32582657} - 1$	9 808 358	
9	$10223 \cdot 2^{31172165} + 1$	9 383 761	
10	$2^{30402457} - 1$	9 152 052	

Tablica 2.2: Prvih 10 najvećih prostih brojeva

2.4 Protokol za razmjenu ključeva

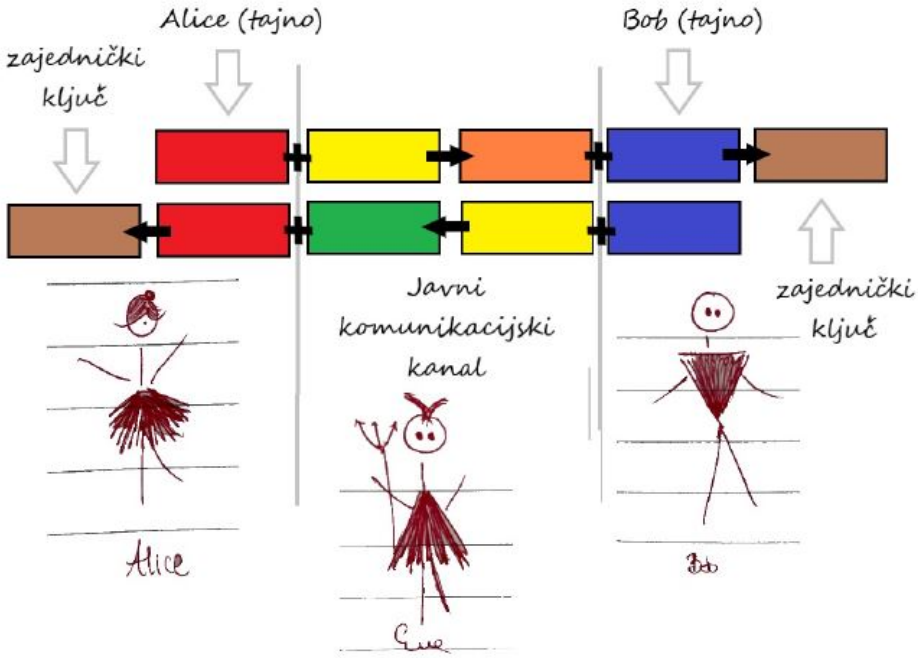
Kriptografija je znanstvena disciplina koja se bavi metodama za slanje poruka koje će moći pročitati samo oni kojima su namijenjene. Obično pretpostavljamo da pošiljatelj, kojeg nazvamo Alice, šalje šifriranu poruku primatelju, kojeg zovemo Bob, preko nesigurnog komunikacijskog kanala koji je nadziran od treće strane (zvana Eve). Alice šifrira poruku pomoću ključa za šifriranje i dobiva šifrat, a Bob do originalne poruke dolazi pomoću ključa za dešifriranje. Kod klasičnih kriptosustava, odnosno općenitije tzv. simetričnih kriptosustava, iz ključa za šifriranje lako je otkriti ključ za dešifriranje, a često su ta dva ključa i jednaka. Zbog toga Alice i Bob mogu sigurno komunicirati samo ako svoje ključeve dobro čuvaju u tajnosti. No, problem koji se prirodno nameće jest kako sigurno razmijeniti ključeve. Ovdje ćemo opisati *protokol za razmjenu ključeva* kojeg su 1976. godine osmislili američki kriptografi Whitfield Diffie i Martin Hellman, a važnu ulogu imat će primitivni korijen. Ideju za ovaj protokol Diffie i Hellman pronašli su u tzv. *jednosmjernim* funkcijama kojima je teško odrediti inverz. Često se kaže da se te funkcije u jednom smjeru računaju lako, a u drugom teško. Jednosmjernu funkciju koju su odabrali bila je potenciranje u konačnoj cikličkoj grupi.

Diffie- Hellmanov protokol za razmjenu ključeva

Neka je G ciklička grupa reda N čiji je generator $g \in G$.

1. Alice odabire slučajan prirodan broj $a \in \{1, 2, \ldots, N-1\}$, te pošalje Bobu element g^a.
2. Bob odabire slučajan prirodan broj $b \in \{1, 2, \ldots, N-1\}$, te pošalje Alice element g^b.
3. Alice izračuna $(g^b)^a = g^{ab}$.
4. Bob izračuna $(g^a)^b = g^{ab}$.

Tajni ključ je $K = g^{ab}$.



Slika 2.1: Shema Diffie - Hellmanovog protokola

Navedeni prokol može se konkretno realizirati u konačnoj cikličkoj grupi

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\},$$

gdje je p prosti broj. Naime, već smo spomenuli da $\mathbb{Z}_p^*$ čini Abelovu grupu uz operaciju množenja modulo p te da je primitivni korijen modulo p generator grupe. Ako je g primitivni korijen modulo p, tada se protokol u $\mathbb{Z}_p^*$ sastoji od sljedećih koraka:

1. Alice odabire slučajan prirodan broj $a \in \{1, 2, \ldots, p-2\}$, te pošalje Bobu element
$$x = g^a \mod p.$$
2. Bob odabire slučajan prirodan broj $b \in \{1, 2, \ldots, p-2\}$, te pošalje Alice element
$$y = g^b \mod p.$$
3. Alice računa ključ $K = y^a \mod p$.
4. Bob računa ključ $K = x^b \mod p$.

Na slici 2.1 je prikazan Diffie- Hellmanov protokol pomoću miješanja boja.

Primjer 2.4.1. *Pretpostavimo da Alice i Bob žele dogovoriti zajednički ključ pomoću Diffie- Hellmanovog protokola u grupi* $\mathbb{Z}_{23}^*$. *Najmanji primitivni korijen modulo* 23 *je* $g = 5$. *Alice i Bob najprije biraju slučajne brojeve a i b iz skupa* $\{1, 2, \ldots, 21\}$.

1. *Alice je odabrala* $a = 7$ *pa Bobu šalje*
$$x = 5^7 \mod 23 = 17.$$
2. *Bob je odabrao broj* $b = 10$ *pa šalje Alice*
$$y = 5^{10} \mod 23 = 9.$$
3. *Alice računa* $K = 9^7 \mod 23 = 4$.
4. *Bob računa* $x^b = 17^{10} \mod 23 = 4$.

Dakle, Alice i Bob posjeduju isti tajni ključ $K = 4$.

Sada recimo nešto o sigurnosti ovog protokola. Eve, koja može prisluškivati komunikaciju preko nesigurnog komunikacijskog kanala, može biti u posjedu sljedećih podataka:

- grupa G;
- generator grupe g;
- element $x = g^a \in G$ kojeg Alice šalje Bobu;

- element $y = g^b \in G$ kojeg Bob šalje Alice.

Protokol će biti siguran ako Eve iz navedenih informacija ne može odrediti g^{ab}, odnosno ne može riješiti tzv. *Diffie-Hellmanov problem*. Specijalno, ako je $G = \mathbb{Z}_p^*$ i g primitivni korijen modulo p, Eve treba pronaći

$$\operatorname{ind}_g x \text{ ili } \operatorname{ind}_g y,$$

odnosno riješiti *problem diskretnog logaritma*. S tim problemom susreli smo se i u primjerima 2.2.1 i 2.2.2 gdje je za određivanje indeksa, odnosno diskretnog logaritma bilo potrebno redom računati sve potencije g^k.

Primjer 2.4.2. *Pretpostavimo da je Eve prisluškivala komunikaciju između Alice i Boba te posjeduje sljedeće podatke:*

$$G = \mathbb{Z}_{23}^*,\ g = 5,\ x = 17,\ y = 9.$$

Treba odrediti a ili b iz skupa $\{0, 1, \ldots, 21\}$ *za koje je*

$$5^a \equiv 17 \pmod{23},\ 5^b \equiv 9 \pmod{23}$$

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$5^k \mod 23$	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14

Tablica 2.3: Elementi cikličke grupe $\mathbb{Z}_{23}^* = (5)$

Iz tablice 2.3 Eve zaključuje da je $a = 7$ *i može odrediti zajednički ključ kojeg su dogovorili Alice i Bob:* $K = y^a \mod p = 9^7 \mod 23 = 4$.

U prethodnom se primjeru nije morala računati čitava tablica 2.3, već se moglo stati s računanjem kad se u donjem retku pojavio broj 17, no ona je tu s razlogom da za, već i za ovako mali red grupe, možemo uočiti da se potencije $5^k \mod 23$, $k = 0, 1, \ldots, 21$, ponašaju vrlo nepravilno. To još bolje možemo uočiti iz slika 2.3 i 2.4 koje prikazuju grafove funkcija $k \mapsto g^k \mod p$, $0 \leq k \leq p - 2$ za proste brojevi $p = 23$ i $p = 229$, odnosno distribuciju elemenata cikličke grupe $\mathbb{Z}_p^*$ reprezentiranih pomoću generatora grupe - primitivnog korijena modulo p. Stoga težina rješavanja problema diskretnog logaritma jednim dijelom leži u slučajnoj distribuciji elemenata g^k iz $\mathbb{Z}_p^*$, no valja još opravdati zašto je računanje jedne potencije $g^k \mod p$ moguće efikasno izračunati. Razlog za to je brzi algoritam za modularno potenciranje koji se naziva *kvadriraj i množi*.

Zapišimo cijeli broj k u bazi 2:

$$k = \sum_{i=0}^{s-1} c_i \cdot 2^i,$$

pri čemu su $c_i \in \{0, 1\}$ za sve $k = 0, 1, \ldots, s-1$. Tada je

$$\begin{aligned} g^k &= g^{c_{s-1}\cdot 2^{s-1} + c_{s-2}\cdot 2^{s-2} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0} \\ &= g^{c_{s-1}\cdot 2^{s-1}} g^{c_{s-2}\cdot 2^{s-2}} \cdots g^{c_1 \cdot 2} g^{c_0 \cdot 1} \\ &= \left(\left(\left(g^{c_{s-1}} \right)^2 g^{c_{s-2}} \right)^2 \cdots \right)^2 g^{c_1} \Bigg)^2 g^{c_0}. \end{aligned}$$

Nadalje, kako je $c_i \in \{0, 1\}$, tada je $g^{c_i} \in \{1, g\}$ pa se prema prethodnoj formuli uzastopno ponavlja: množenje s g i kvadriranje ako je $c_i = 1$ ili samo kvadriranje ako je $c_i = 0$.

Algoritam *kvadriraj i množi*

ulaz(x, $(c_0, c_1, \ldots, c_{s-1})$, n)
$y = 1$
za $i = s-1, s-2, \ldots, 1, 0$ radi:
    $y = y^2 \mod n$
    ako je $c_i = 1$, onda $y = y \cdot x \mod n$
izlaz(y)

Primjer 2.4.3. *Izračunajte potencije iz primjera 2.4.1 pomoću algoritma* kvadriraj i množi.

Rješenje. Potrebno je izračunati potencije: 5^7, 5^{10}, 9^7, 17^{10} modulo 23. Binarni zapisi eksponenata su

$$7 = (111)_2, \ 10 = (1010)_2.$$

Računamo $5^7 \mod 23$. Ulazni podatci: $x = 5$, $(c_0, c_1, c_2) = (1, 1, 1)$, $n = 23$.
$y = 1$

$i = 2$: $y = y^2 \mod 23 = 1$
$c_2 = 1 \Rightarrow y = y \cdot x = 1 \cdot 5 \mod 23 = 5$

$i = 1$: $y = y^2 = 5^2 \mod 23 = 2$
$c_1 = 1 \Rightarrow y = y \cdot x = 2 \cdot 5 \mod 23 = 10$

$i = 0$: $y = y^2 = 10^2 \mod 23 = 8$
$c_0 = 1 \Rightarrow y = y \cdot x = 8 \cdot 5 \mod 23 = 17 \Rightarrow 5^7 \mod 23 = 17$

Računamo $5^{10} \mod 23$. Ulazni podatci: $x = 5$, $(c_0, c_1, c_2, c_3) = (0, 1, 0, 1)$, $n = 23$.
$y = 1$

$i = 3$: $y = y^2 \mod 23 = 1$

$c_3 = 1 \Rightarrow y = y \cdot x = 1 \cdot 5 \mod 23 = 5$

$i = 2$: $y = y^2 = 5^2 \mod 23 = 2$

$i = 1$: $y = y^2 = 2^2 \mod 23 = 4$

$c_1 = 1 \Rightarrow y = y \cdot x = 4 \cdot 5 \mod 23 = 20$

$i = 0$: $y = y^2 = 20^2 \mod 23 = 9 \Rightarrow 5^{10} \mod 23 = 9$

Računamo $9^7 \mod 23$. Ulazni podatci: $x = 9$, $(c_0, c_1, c_2) = (1, 1, 1)$, $n = 23$
$y = 1$

$i = 2$: $y = y^2 \mod 23 = 1$

$c_2 = 1 \Rightarrow y = y \cdot x = 1 \cdot 9 \mod 23 = 9$

$i = 1$: $y = y^2 = 9^2 \mod 23 = 12$

$c_1 = 1 \Rightarrow y = y \cdot x = 12 \cdot 9 \mod 23 = 16$

$i = 0$: $y = y^2 = 16^2 \mod 23 = 3$

$c_0 = 1 \Rightarrow y = y \cdot x = 3 \cdot 9 \mod 23 = 4 \Rightarrow 9^7 \mod 23 = 4$

Računamo $17^{10} \mod 23$. Ulazni podatci: $x = 17$, $(c_0, c_1, c_2, c_3) = (0, 1, 0, 1)$, $n = 23$.
$y = 1$

$i = 3$: $y = y^2 \mod 23 = 1$

$c_3 = 1 \Rightarrow y = y \cdot x = 1 \cdot 17 \mod 23 = 17$

$i = 2$: $y = y^2 = 17^2 \mod 23 = 13$

$i = 1$: $y = y^2 = 13^2 \mod 23 = 8$

$c_1 = 1 \Rightarrow y = y \cdot x = 8 \cdot 17 \mod 23 = 21$

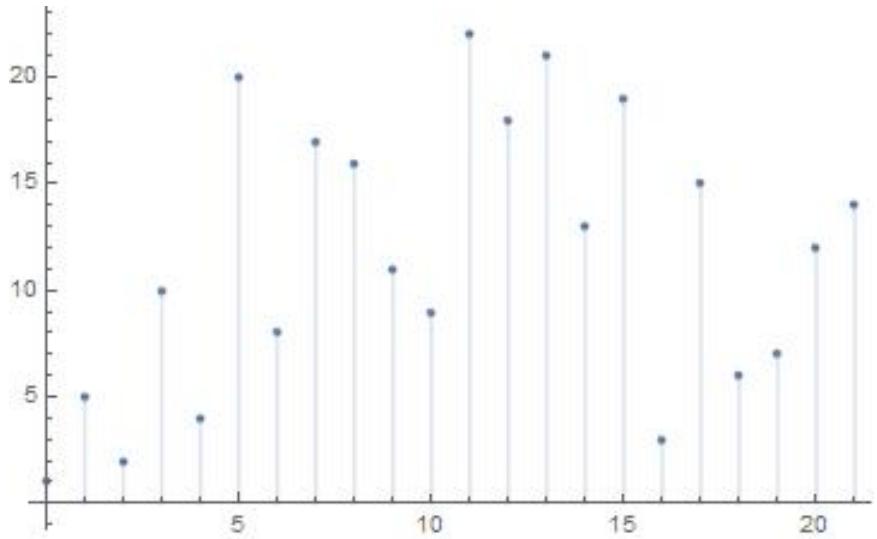
$i = 0$: $y = y^2 = 21^2 \mod 23 = 4 \Rightarrow 17^{10} \mod 23 = 4$

□

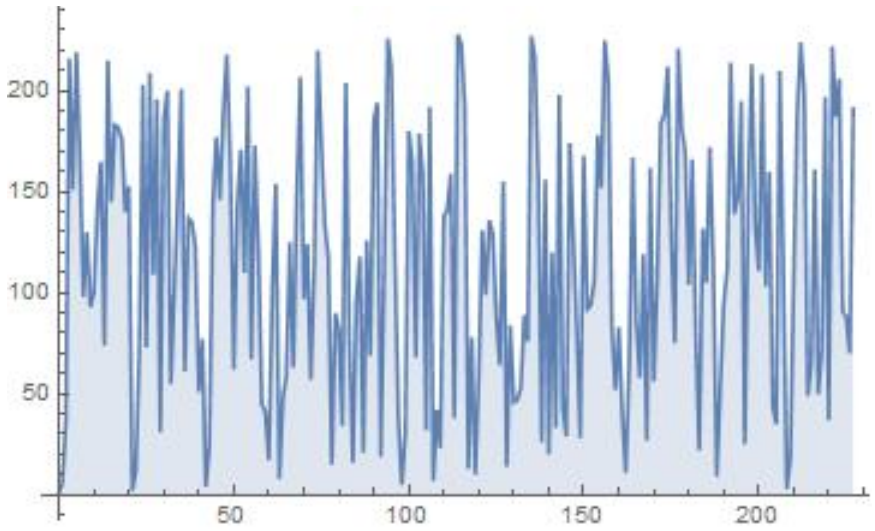
Kao što smo već spomenuli, kada su brojevi jako veliki, izračune je bolje provesti pomoću računala. Na slici 2.2 je prikazan algoritam ”Kvadriraj i množi” implementiran u programskom jeziku C.

```
int kvadriraj_i_mnozi(int x, int s, int n, int *c) {
    int y=1;
    for(int i=s-1;i>=0;--i) {
        y=(y*y)%n;
        if(c[i]==1) y=(y*x)%n;
    }
    return y;
}
```

Slika 2.2: Algoritam ”kvadriraj i množi”



Slika 2.3: Graf funkcije $k \mapsto 5^k \mod 23$, $k \in \{0, 1, \ldots, 21\}$



Slika 2.4: Graf funkcije $k \mapsto 6^k \mod 229$, $k \in \{0, 1, \ldots, 227\}$

Bibliografija

[1] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[2] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[3] Z. Franušić, *O matematici digitalnog potpisa*, preprint.

[4] K. H. Rosen, *Elementary number theory and its applications*, Addison Wesley, 1993.

[5] Prime Pages, The Largest Known Primes - A Summary, `https://primes.utm.edu/largest.html` (siječanj 2022.)

[6] Slika 2.1., Izvor: Z. Franušić, *O matematici digitalnog potpisa*, preprint.

Sažetak

Prema Eulerovom teoremu za relativno proste brojeve $a \in \mathbb{Z}$ i $n \in \mathbb{N}$ vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se *red* od a modulo n. Ako je $d = \varphi(n)$, a se naziva *primitivni korijen modulo n*, a skup $\{a^1, a^2, \ldots, a^{\varphi(n)}\}$ čini reducirani sustav ostataka modulo n. To povlači da je $\mathbb{Z}_n^*$ ciklička grupa, pri čemu je a generator te grupe.

Ne postoji primitivni korijen modulo n za svaki prirodan broj n. Pokazuje se da primitivni korijen modulo n postoji ako i samo ako je $n = 2, 4, p^k$ ili $n = 2p^k$, pri čemu je p prost broj i $k \in \mathbb{N}$.

S obzirom da $\{a^0, a^1, \ldots, a^{\varphi(n)-2}\}$ čini reducirani sustav ostataka modulo n, to nam omogućava definiciju *indeksa* (*diskretnog logaritma*) od a u odnosu na primitivni korijen modulo n. Ako je $y \in \mathbb{Z}$ relativno prost s n, tada je *index* od y s obzirom na a modulo n jednak $x \in \{0, 1, \ldots, \varphi(n) - 1\}$ za koji je $y \equiv a^x \pmod{n}$. Indeksi imaju svojstva koja su slična onima za logaritme pri čemu se jednakosti zamjenjuju kongruencijama modulo $\varphi(n)$.

U radu su opisane i neke primjene primitivnih korijena i diskretnog logaritma kao što su rješavanje polinomijalnih i eksponencijalnih kongruencija, testovi prostosti i protokol za razmjenu ključeva koji se koristi u kriptografiji.

Summary

According to Euler's theorem, for relatively prime numbers $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, it holds that $a^{\varphi(n)} \equiv 1 \pmod{n}$. The smallest natural number d with the property $a^d \equiv 1 \pmod{n}$ is called the *order* of a modulo n. If $d = \varphi(n)$, then a is called a *primitive root modulo n* and the set $\{a^1, a^2, \ldots, a^{\varphi(n)}\}$ forms a reduced system of residues modulo n. This implies that $\mathbb{Z}_n^*$ is a cyclic multiplicative group, where the primitive root a is its generator.

A primitive root modulo n does not exist for every natural number n. It is shown that a primitive root modulo n exists if and only if $n = 2, 4, p^k$ or $n = 2p^k$, where p is a prime number and $k \in \mathbb{N}$.

Considering that $\{a^0, a^1, \ldots, r^{\varphi(n)-1}\}$ is a reduced system of residues modulo n, it leads to a definition of the *index* (*discrete logarithm*). If $y \in \mathbb{Z}$ is relatively prime to n, then the *index* of y to the base a modulo n equals $x \in \{0, 1, \ldots, \varphi(n) - 1\}$ such that $y \equiv a^x \pmod{n}$. Indices have many properties similar those of logarithms where equalities are replaced with congruences modulo $\varphi(n)$.

In this graduate thesis, some applications of primitive roots and discrete logarithms are described, such as solving polynomial and exponential congruences, primality testing, and the key exchange protocol which is used in cryptography.

Životopis

Rođena sam 22.11. 1996. godine u Bjelovaru. Godine 2003. započinjem osnovnoškolsko obrazovanje u Osnovnoj školi Velika Pisanica. Školovanje nastavljam u Općoj gimnaziji Bjelovar koju završavam 2015. godine, te upisujem preddiplomski sveučilišni studij Matematike, smjer nastavnički na Prirodoslovno - matematičkom fakultetu Sveučilišta u Zagrebu. Nakon završetka preddiplomskog studija, iste godine upisujem diplomski studij Matematike, također nastavnički smjer, na Sveučilištu u Zagrebu. Tijekom diplomskog studija radim kao kreator matematičkog sadržaja u Photomath-u.