Primitivni korijeni i indeksi

Popović, Ana

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Ana Popović

Primitivni korijeni i indeksi

Završni rad

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Ana Popović

Primitivni korijeni i indeksi

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2017.

Sadržaj

Sažetak: U ovom radu bavit ćemo se primitivnim korijenima i indeksima. Definirat ćemo oba pojma, navesti njihova osnovna svojstva te na primjerima pokazati kako se računaju i koriste. Na kraju ćemo izložiti probleme vezane uz primitivne korijene i indekse koji uključuju Artinovu hipotezu, Diffie-Hellmanov problem, ElGamalov kriptosustav te Solovay-Strassenov test.

Ključne riječi: reducirani sustav ostataka, Eulerova funkcija, Mali Fermatov teorem, primitivni korijeni, indeksi, Artinova hipoteza, problem diskretnog logaritma, Diffie-Hellmanov problem, ElGamalov kriptosustav, Solovay-Strassenov test.

Primitive roots and indices

Abstract: This work covers primitive roots and indices. Here we define both terms, specify their basic properties and give some examples that show how to calculate and use them. Finally, we introduce mathematical problems closely related to primitive roots and indices such as Artin's Hypotesis, Diffie-Hellman problem, Elgamal's cryptosystem and Solovay-Strassen test.

Key words: residue system, Euler's totient function, Fermat's Little theorem, primitive roots, indices, Artin's hypothesis, discrete logarihtm problem, Diffie-Hellman problem, ElGamal cryptosystem, Solovay-Strassen test.

Uvod

Primitivni korijeni i indeksi su važni pojmovi u teoriji brojeva. Kao što ćemo vidjeti u ovom radu ovi pojmovi su usko vezani uz modularno potenciranje i red elemenata te Eulerovu funkciju, odnosno Eulerov teorem. Osim primjene u teoriji brojeva, primitivni korijeni i indeksi imaju primjenu i u kriptosustavima s javnim ključem.
U prvom poglavlju rada najprije navodimo definicije i teoreme iz teorije brojeva koji će nam biti potrebni kako bismo precizno definirali primitivne korijene, a zatim dokazujemo njihova svojstva. U drugom poglavlju ćemo obraditi indekse te ćemo na primjerima pokazati njihovu primjenu. U zadnjem poglavlju rada navest ćemo neke probleme koji su vezani uz primitivne korijene i indekse.

1. Primitivni korijeni

1.1. Definicija

Kako bi bolje shvatili definiciju primitivnog korijena prije svega ćemo ponoviti neke bitne pojmove iz teorije brojeva. Dokazi ovih tvrdnji mogu se naći u [4].

Definicija 1.1. *Reducirani sustav ostataka modulo $n \in \mathbb{N}$ je skup cijelih brojeva r_i sa svojstvom $(r_i, n) = 1$, $r_i \not\equiv r_j \pmod{n}$, za $i \neq j$, te da za svaki cijeli broj x takav da je $(x, n) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{n}$.*

Jedan reducirani sustav ostataka modulo n je skup svih brojeva $a \in \{1, 2, \ldots, n\}$ takvih da je $(a, n) = 1$. Jasno je da svi reducirani sustavi ostataka modulo n imaju isti broj elemenata.

Definicija 1.2. *Broj elemenata u reduciranom sustavu ostataka modulo n označavamo s $\varphi(n)$, a funkciju φ nazivamo Eulerova funkcija.*

Primjer 1.1. *Skup $\{1, 5, 7, 11\}$ je reducirani sustav ostataka modulo 12. Svaki element tog skupa je relativno prost s 12, svi elementi ovog skupa su međusobno nekongruentni i svaki cijeli broj koji je relativno prost s 12 je kongruentan modulo 12 nekom od ovih brojeva.*

Teorem 1.1. *Neka je $\{r_1, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo $n \in \mathbb{N}$ te neka je za $a \in \mathbb{Z}$ takav da je $(a, n) = 1$. Tada je $\{ar_1, \ldots, ar_{\varphi(n)}\}$ također reducirani sustav ostataka modulo n.*

Teorem 1.2. *(Eulerov teorem) Neka je $n \in \mathbb{N}$ i $a \in \mathbb{Z}$. Ako je $(a, n) = 1$, onda je $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Teorem 1.3. *(Mali Fermatov teorem) Neka je p prost broj i $a \in \mathbb{Z}$. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki $a \in \mathbb{Z}$ vrijedi $a^p \equiv a \pmod{p}$.*

Definicija 1.3. *Funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*

1. *$\vartheta(1) = 1$,*
2. *$\vartheta(mn) = \vartheta(m)\vartheta(n)$ za sve m,n takve da je $(m, n) = 1$,*

zovemo multiplikativna funkcija.

Teorem 1.4. *Eulerova funkcija φ je multiplikativna. Nadalje, za svaki $n \in \mathbb{N}$ veći od 1 vrijedi*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Teorem 1.5. *Vrijedi*

$$\prod_{d|n} \varphi(d) = n.$$

Definicija 1.4. *Neka su $n \in \mathbb{N}$ i $a \in \mathbb{Z}$ takvi da je $(a, n) = 1$. Red od a modulo n je najmanji $e \in \mathbb{N}$ takav da je $a^e \equiv 1 \pmod{n}$. Red od a modulo n najčešće označavamo s $\mathrm{ord}_n(a)$.*

Primjer 1.2. *Odredimo red od a modulo n, ako je $a = 2$ i $n = 7$.*

Rješenje. Iz kongruencija

$$\begin{aligned} 2^0 &\equiv 1 \pmod 7, \\ 2^1 &\equiv 2 \pmod 7, \\ 2^2 &\equiv 4 \pmod 7, \\ 2^3 &\equiv 1 \pmod 7 \end{aligned}$$

slijedi da je red od 2 modulo 7 jednak 3.

Propozicija 1.1. *Neka su $n \in \mathbb{N}$ i $a \in \mathbb{Z}$ takvi da je $(a, n) = 1$. Ako je $\mathrm{ord}_n(a) = e$, tada za $k \in \mathbb{N}$ vrijedi $a^k \equiv 1 \pmod n$ ako i samo ako $e|k$. Specijalno, $e|\varphi(n)$.*

Dokaz. Neka je $a^k \equiv 1 \pmod n$. Primjenom Teorema o dijeljenju s ostatkom dobivamo $k = qe + r$, gdje je $0 \leq r < e$. Sada je:

$$1 \equiv a^k \equiv a^{qe+r} \equiv (a^e)^q a^r \equiv a^r \pmod n.$$

Kako je e najmanji broj takav da je $a^e \equiv 1 \pmod n$, slijedi da je $r = 0$, stoga $e|k$.

Obratno, pretpostavimo da $e|k$ tj. $k = el$ za neki $l \in \mathbb{N}$. Tada je

$$a^k \equiv (a^e)^l \equiv 1 \pmod n.$$

Posebno, $e|\varphi(n)$ jer je $a^{\varphi(n)} \equiv 1 \pmod n$ po Eulerovom teoremu. □

Posljedica Propozicije 1.1 je da red svakog elementa modulo p, gdje je p prost broj, dijeli $p-1$.

Ako znamo red od a modulo n, lako možemo odrediti red bilo koje potencije od a modulo n što nam pokazuje sljedeći korolar.

Korolar 1.1. *Ako su $d, n \in \mathbb{N}$ i $a \in \mathbb{Z}$ takvi da je $(a, n) = 1$, tada vrijedi*

$$\mathrm{ord}_n(a^d) = \frac{\mathrm{ord}_n(a)}{(d, \mathrm{ord}_n(a))}.$$

Dokaz. Neka su $e = \mathrm{ord}_n(a)$, $f = \mathrm{ord}_n(a^d)$, $g = (d, \mathrm{ord}_n(a))$, $d = bg$, $e = cg$ i $(b, c) = 1$. Tada je

$$(a^d)^c = (a^{bg})^c = (a^{cg})^b = (a^e)^b \equiv 1 \pmod n$$

pa prema Propoziciji 1.1 slijedi $f|c$. Kako je $e = \mathrm{ord}_n(a)$, $(a^{df}) = (a^d)^f \equiv 1 \pmod n$ iz Propozicije 1.1, slijedi $e|df$. Uvrštavanjem vrijednosti za e i d dobivamo da $cg|bgf$ tj. $c|bf$. Budući da je $(b, c) = 1$, c dijeli f. Iz ovih razmatranja slijedi da je $c = f$ pa imamo

$$\mathrm{ord}_n(a^d) = f = c = \frac{e}{g} = \frac{\mathrm{ord}_n(a)}{(d, \mathrm{ord}_n(a))}.$$

□

Korolar 1.2. *Neka su $a \in \mathbb{Z}$, e, $n \in \mathbb{N}$ i $(a, n) = 1$. Tada je*

$$\mathrm{ord}_n(a^e) = \mathrm{ord}_n(a)$$

ako i samo ako $(e, \mathrm{ord}_n(a)) = 1$.

Dokaz. Prema prethodnom korolaru slijedi

$$\mathrm{ord}_n(a^e) = \frac{\mathrm{ord}_n(a)}{(e, \mathrm{ord}_n(a^e))}.$$

Odavde zaključujemo da je $\mathrm{ord}_n(a^e) = \mathrm{ord}_n(a)$ ako i samo ako je $(e, \mathrm{ord}_n(a)) = 1$. □

Primjer 1.3. *Iz Primjera 1.2 znamo da je* $\mathrm{ord}_7(2) = 3$ *pa je prema Korolaru 1.2*

$$\mathrm{ord}_7(2^2) = \mathrm{ord}_7(2) = 3.$$

Lema 1.1. *Neka su* $a \in \mathbb{Z}$ *i* $n \in \mathbb{N}$ *takvi da je* $(a, n) = 1$. *Tada je* $a^i \equiv a^j \pmod{n}$ *za* $i, j \in \mathbb{N}_0$ *ako i samo ako je* $i \equiv j \pmod{\mathrm{ord}_n(a)}$.

Dokaz. Ako je $a^i \equiv a^j \pmod{n}$ za $0 \leqslant i \leqslant j \leqslant \varphi(n)$, te kako je $(a, n) = 1$, imamo $a^{j-i} \equiv 1 \pmod{n}$. Prema Propoziciji 1.1 slijedi da $\mathrm{ord}_n(a) | (j - i)$, odnosno $i \equiv j \pmod{\mathrm{ord}_n(a)}$.

S druge strane, ako je $i \equiv j \pmod{\mathrm{ord}_n(a)}$ za $0 \leqslant i \leqslant j$, tada je $j = i + q \cdot \mathrm{ord}_n(a)$ gdje je $q \geqslant 0$. Dakle,

$$a^j \equiv a^{i+q\cdot \mathrm{ord}_n(a)} \equiv a^i (a^{\mathrm{ord}_n(a)})^q \equiv a^i \cdot 1^q \equiv a^i \pmod{n}.$$

□

Primjer 1.4. *Gledamo li potencije od 2 modulo 11 primjenom Malog Fermatovog teorema dobivamo*

$$2^{10} \equiv 1 \pmod{11}.$$

Prema Propoziciji 1.1 slijedi da trebamo provjeriti jesu li 2^2 *i* 2^5 *kongruentni 1 modulo 11. Kako je* $2^2 \equiv 4 \pmod{11}$, *a* $2^5 \equiv 10 \pmod{11}$ *zaključujemo da je* $\mathrm{ord}_{11}(2) = 10$. *Brojeve koji zadovoljavaju svojstvo da je* $\mathrm{ord}_n(a) = \varphi(n)$ *uveo je 1773. godine Euler i nazivaju se primitivni korijeni.*

Definicija 1.5. *Neka je* $a \in \mathbb{Z}$, $n \in \mathbb{N}$ *i* $(a, n) = 1$. *Kažemo da je a primitivan korijen modulo n ako je red od a modulo n jednak* $\varphi(n)$.

Uočimo da svaki prost broj p ima primitivan korijen.

1.2. Svojstva primitivnih korijena

Teorem 1.6. *Neka je* $a \in \mathbb{Z}$ *i* $n \in \mathbb{N}$. *Ako je a primitivan korijen modulo n, tada je* $\{a, a^2, \ldots, a^{\varphi(n)}\}$ *reducirani sustav ostataka modulo n.*

Dokaz. Neka je a primitivan korijen modulo n, tj. $\varphi(n)$ je red od a modulo n. Tada je $(a, n) = 1$ pa je i $(a^i, n) = 1$, za $i = 1, \ldots, \varphi(n)$. Dokažimo da su elementi skupa $\{a, a^2, \ldots, a^{\varphi(n)}\}$ od $\varphi(n)$ elemenata međusobno nekongurentni modulo n. Ako je $a^i \equiv a^j \pmod{n}$ za $1 \leq i < j \leq \varphi(n)$, tada je prema Lemi 2.1 $i \equiv j \pmod{\varphi(n)}$. Prema tome $\varphi(n)$ dijeli $j - i$ što je nemoguće s obzirom da je $0 < j - i < \varphi(n)$. Odavde slijedi da je $a^i \not\equiv a^j \pmod{n}$ za $1 \leq i < j \leq \varphi(n)$. Zaključujemo da je $\{a, a^2, \ldots, a^{\varphi(n)}\}$ reducirani sustav ostataka modulo n. □

Teorem 1.7. *Neka je p prost broj. Tada postoji točno* $\varphi(p-1)$ *primitivnih korijena modulo p.*

Dokaz. Svaki od $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu, koji je djelitelj od $\varphi(p) = p-1$. Označimo s $\psi(e)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu e. Tada je

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

Pokazat ćemo da je $\psi(e) \neq 0$ i $\psi(e) = \varphi(e)$, za svaki e. Po Teoremu 1.5 slijedi da je

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

Ukoliko bi stavili da je $\psi(e) = 0$ onda bi suma $\sum_{e|p-1} \psi(e)$ bila manja od $p-1$. Stoga je $\psi(e) \neq 0$, za svaki e.
Neka je a broj koji pripada eksponentu e modulo p. Promatramo kongruenciju

$$x^e \equiv 1 \pmod{p}.$$

Rješenja ove kongruencije su $a, a^2, \ldots, a^e$ i svaki od njih ima red e. Uzmemo li bilo koji broj b koji pripada eksponentu e modulo p, tada postoji $m \in \mathbb{N}$ takav da je $b \equiv a^m, 1 \leq m \leq e$. Kako je

$$b^{\frac{e}{(m,e)}} \equiv (a^e)^{\frac{m}{(m,e)}} \equiv 1 \pmod{p},$$

slijedi da je $(m, e) = 1$. Stoga je $\psi(e) = \varphi(e)$, a onda je i $\psi(p-1) = \varphi(p-1)$. □

Ako je a primitivan korijen od p, tada su $\varphi(p-1)$ nekongruentnih primitivnih korijena od p dani s $a^{\alpha_1}, a^{\alpha_2}, \ldots, a^{\alpha_{\varphi(p-1)}}$, gdje su $\alpha_1, \alpha_2, \ldots, \alpha_{\varphi(p-1)}, \varphi(p-1)$ cijelih brojeva manjih od $p-1$ i $(\alpha_i, p-1) = 1$, za $i = 1, 2 \ldots, p-1$.

Ako je $a \in \mathbb{Z}$ i $n \in \mathbb{N}$ i $(a, n) = 1$, tada je a primitivan korijen modulo n ako i samo ako je $a^{\frac{\varphi(n)}{q}} \not\equiv 1 \pmod{n}$, za sve proste djelitelje q od $\varphi(n)$. Općenito, ako primitivan korijen od n postoji, tada postoji $\varphi(\varphi(n))$ nekongruentnih primitivnih korijena od n, što ćemo i dokazati u sljedećem teoremu.

Teorem 1.8. *Ako $n \in \mathbb{N}$ ima primitivan korijen, tada n ima $\varphi(\varphi(n))$ nekongruentnih primitivnih korijena.*

Dokaz. Neka je a primitivan korijen modulo n. Iz Teorema 1.6 slijedi da svaki drugi primitivan korijen mora biti oblika a^e gdje je $1 \leqslant e \leqslant \varphi(n)$. Iz Korolara 1.2 slijedi da je $\mathrm{ord}_n(a) = \mathrm{ord}_n(a^e)$ ako i samo ako je $(e, \varphi(n)) = 1$. Odavde zaključujemo da ima točno $\varphi(\varphi(n))$ brojeva e. □

Teorem 1.9. *Ako je $p > 2$ prost broj, tada postoji primitivan korijen modulo p^m za sve $m \in \mathbb{N}$. Osim toga, ako je $a \in \mathbb{Z}$ primitivan korijen modulo p^2, tada je a primitivan korijen modulo p^m za sve $m \in \mathbb{N}$.*

Dokaz. Neka je a primitivan korijen modulo p.

Tvrdnja 1.1. *Ili a ili $p + a$ je primitivan korijen modulo p^2.*

Kako je $\mathrm{ord}_p(a) = p-1$, stavimo da je $d = \mathrm{ord}_p(a^2)$ pri čemu prema Propoziciji 1.1 vrijedi $(p-1)|d$. Prema Propoziciji 1.1 također slijedi $d|\varphi(p^2)$. Zaključujemo da vrijedi

$$(p-1)|d|p(p-1),$$

pa je ili $d = p-1$ ili $d = p(p-1)$. U drugom slučaju imamo da je a primitivan korijen modulo p^2, a u prvom slučaju imamo

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

U ovom slučaju, stavimo da je $a_1 = a+p$. Iz binomnog teorema i Malog Fermatovog teorema imamo

$$\begin{aligned} a_1^{p-1} \equiv (a+p)^{p-1} &\equiv a^{p-1} + (p-1)a^{p-2}p + \sum_{j=2}^{p-1} \binom{p-1}{j} a^{p-1-j}p^j \pmod{p^2} \\ &\equiv a^{p-1} + (p-1)a^{p-2}p \equiv a^{p-1} - a^{p-2}p \pmod{p^2}. \end{aligned}$$

Ako je $a_1^{p-1} \equiv 1 \pmod{p^2}$, prema zadnjoj kongruenciji i prema (1) slijedi

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

Odavde je $a^{p-2}p \equiv 0 \pmod{p^2}$ odnosno $a^{p-2} \equiv 0 \pmod{p}$. Kako je $(a,p) = 1$ (jer je a primitivan korijen modulo p), to je nemoguće. Time smo dokazali Tvrdnju 1.1. Uočimo da prema ovoj tvrdnji možemo odabrati a takav da je a primitivan korijen modulo p, koji je također primitivan korijen modulo p^2.

Za dokaz drugog dijela teorema dovoljno je pokazati da ako je a primitivan korijen modulo p^{m-1}, tada je a primitivan korijen modulo p^m. Neka je $k = \mathrm{ord}_{p^m}(a)$ tada $k|\varphi(p^m) = (p-1)p^{m-1}$. Kako je $a^k \equiv 1 \pmod{p^m}$, tako je i $a^k \equiv 1 \pmod{p^{m-1}}$. Po pretpostavci kako je a primitivan korijen modulo p^{m-1}, slijedi $\varphi(p^{m-1}) = (p-1)p^{m-2}|k$. Tada je $k = (p-1)p^{m-2}$ ili $k = (p-1)p^{m-1}$. Kako bi dokazali da je a primitivan korijen modulo p^m dovoljno je dokazati da vrijedi sljedeća tvrdnja.

Tvrdnja 1.2. *Za svaki $m \in \mathbb{N}$, $m > 1$, vrijedi $a^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}$.*

Koristimo matematičku indukciju. Ako je $m = 2$, znamo da rezultat vrijedi jer je a primitivan korijen modulo p^2 prema Tvrdnji 1.1. Pretpostavimo da rezultat vrijedi za m, tj.

$$a^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}. \tag{2}$$

Pokažimo da tvrdnja vrijedi za $m+1$. Koristeći Eulerov teorem imamo

$$a^{p^{m-2}(p-1)} \equiv a^{\varphi(p^{m-1})} \equiv 1 \pmod{p^{m-1}}$$

pa postoji $z \in \mathbb{N}$ takav da je

$$a^{p^{m-2}(p-1)} = 1 + zp^{m-1}. \tag{3}$$

Iz (1) i $a^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}$ slijedi da $p \nmid z$. Potenciranjem obje strane od (3) s p te korištenjem binomnog teorema i Malog Fermatovog teorema dobijemo

$$a^{p^{m-1}(p-1)} = (1 + zp^{m-1})^p \equiv 1 + zp^m + \sum_{j=2}^{p} \binom{p}{j} (zp^{m-1})^j \equiv 1 + zp^m \pmod{p^{m+1}}.$$

Kako $p \nmid z$, ne vrijedi da je $a^{p^{m-1}(p-1)} \equiv 1 \pmod{p^{m+1}}$ što vidimo iz Tvrdnje 1.2.
Iz dokazane Tvrdnje 1.2 zaključujemo da je a primitivan korijen modulo p^m. □

Korolar 1.3. *Za bilo koji neparan prost broj p i $m \in \mathbb{N}$ postoji primitivan korijen modulo $2p^m$.*

Dokaz. Neka je a primitivan korijen modulo p^m prema Teoremu 1.9. Bez smanjenja općenitosti možemo pretpostaviti da je a neparan, jer čak i ako je paran tada možemo uzeti $a + p^m$ koji je također primitivan korijen modulo p^m. Prema tome $(2p^m, a) = 1$ i $\varphi(2p^m) = \varphi(2)\varphi(p^m) = \varphi(p^m)$ pa ako je $a^e \equiv 1 \pmod{2p^m}$ onda je i $a^e \equiv 1 \pmod{p^m}$. Dakle, $\varphi(p^m)|e$. Također, kako je a primitivan korijen modulo p^m, $e = \varphi(p^m) = \varphi(2p^m)$ pa time dolazimo do tražene tvrdnje. □

Teorem 1.10. *Postoji primitivan korijen modulo $m = 2^k$ ako i samo ako je $m = 2$ ili $m = 4$.*

Dokaz. Znamo da je 1 primitivan korijen modulo 2 i 3 primitivan korijen modulo 4. Trebamo pokazati da za $k \geq 3$ ne postoji primitivan korijen modulo 2^k. Kako je $\varphi(2^k) = 2^{k-1}$, dovoljno je pokazati da je

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \tag{4}$$

za svaki neparan a i $k \geq 3$. Ovu tvrdnju dokazat ćemo metodom matematičke indukcije po k. Ako je $k = 3$ imamo

$$a^2 \equiv 1 \pmod{2^3} \equiv 1 \pmod{8},$$

a kako vrijedi da je $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, slijedi da je a neparan za $k = 3$.
Neka je $k \geq 3$ i pretpostavimo da je kongruencija (4) istinita. Tada je $a^{2^{k-2}} - 1$ djeljivo s 2^k. Kako je a neparan, slijedi da je $a^{2^{k-2}} + 1$ paran. Dakle,

$$a^{2^{k-1}} - 1 = (a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1)$$

je djeljivo s 2^{k+1} pa je

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

□

Neka je $k \geq 3$. Po prethodnom teoremu ne postoji primitivan korijen modulo 2^k tj. ne postoji neparan broj čiji je red modulo 2^k jednak 2^{k-1}. Međutim, postoji neparan broj čiji je red modulo 2^k jednak 2^{k-2}.

Teorem 1.11. *Neka su $m, n \in \mathbb{N}$ takvi da je $m, n > 2$ i $(m, n) = 1$. Tada umnožak mn nema primitivnih korijena.*

Dokaz. Neka je l najmanji zajednički višekratnik brojeva $\varphi(m)$ i $\varphi(n)$ i $g = (\varphi(m), \varphi(n))$ te neka su $m, n > 2$. Tada $2|\varphi(m)$ i $2|\varphi(n)$ pa je $g \geqslant 2$. Iz svojstva da je $l \cdot g = \varphi(m) \cdot \varphi(n)$ slijedi

$$l = \frac{\varphi(m) \cdot \varphi(n)}{g} \leqslant \frac{\varphi(m) \cdot \varphi(n)}{2}.$$

Uzmimo bilo koji $a \in \mathbb{N}$ takav da je $(a, mn) = 1$. Tada je

$$a^l \equiv (a^{\varphi(m)})^{\frac{\varphi(n)}{g}} \equiv 1 \pmod{m}.$$

Analogno se pokaže da je i $a^l \equiv 1 \pmod{n}$.
Zaključujemo da vrijedi

$$a^l \equiv 1 \pmod{mn}$$

pa je

$$\mathrm{ord}_{mn}(a) < \varphi(mn) = \varphi(m)\varphi(n),$$

za bilo koji a takav da je $(a, mn) = 1$. Prethodna jednakost nam pokazuje da ne postoji primitivan korijen modulo mn. □
Iz dokazanih tvrdnji slijedi sljedeći teorem.

Teorem 1.12. *(Teorem o primitivnim korijenima) Neka je $n \in \mathbb{N}$ i $n > 1$. Tada n ima primitivan korijen ako i samo ako je $n \in \{2, 4, p^a, 2p^a\}$, gdje je p neparan prost broj.*

2. Indeksi

2.1. Definicija

Definicija 2.1. *Neka je $n \in \mathbb{N}$ i neka je m primitivan korijen modulo n. Tada brojevi m^l tvore reducirani sustav ostataka modulo n, za $l = 1, \ldots, \varphi(n)$. Za svaki $a \in \mathbb{Z}$ takav da je $(a, n) = 1$ postoji jedinstveni l takav da je $m^l \equiv a \pmod{n}$. Eksponent l se zove indeks od a u odnosu na m i označava se s $\operatorname{ind}_m a$ ili $\operatorname{ind} a$. Drugi naziv za indeks je diskretan logaritam i označava se s $\log_m a$, ali zbog mogućnosti zabune između običnih i diskretnih logaritama koristit ćemo naziv indeks.*

Primjer 2.1. *Neka je $n = 11$, tada je 2 primitivan korijen modulo 11 i*

$$2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^3 \equiv 8 \pmod{11}, \quad 2^4 \equiv 5 \pmod{11},$$
$$2^5 \equiv 10 \pmod{11}, \quad 2^6 \equiv 9 \pmod{11}, \quad 2^7 \equiv 7 \pmod{11}, \quad 2^8 \equiv 3 \pmod{11},$$
$$2^9 \equiv 6 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11}.$$

Iz prethodnih kongruencija slijedi,

a	$\operatorname{ind}_2(a)$	a	$\operatorname{ind}_2(a)$
1	2	6	9
2	4	7	7
3	8	8	3
4	5	9	6
5	10	10	1

2.2. Svojstva i primjene indeksa

Teorem 2.1. *Ako je $n \in \mathbb{N}$ i m primitivan korijen modulo n, tada za $a, b \in \mathbb{Z}$ vrijedi sljedeće:*

1. $\operatorname{ind}_m(a) + \operatorname{ind}_m(b) \equiv \operatorname{ind}_m(ab) \pmod{\varphi(n)}$,
2. $\operatorname{ind}_m(1) = 0$, $\operatorname{ind}_m(g) = 1$,
3. $\operatorname{ind}_m(a^t) = t \operatorname{ind}_m(a) \pmod{\varphi(n)}$ *za* $m \in \mathbb{N}$,
4. $\operatorname{ind}(-1) = \frac{1}{2}\varphi(n)$ *za* $n \geq 3$.

Dokaz.

1. Neka je $x = \operatorname{ind}_m(ab)$, $y = \operatorname{ind}_m(a)$ i $z = \operatorname{ind}_m(b)$. Kako je $ab \equiv m^x \pmod{n}$, $a \equiv m^y \pmod{n}$ i $b \equiv m^z \pmod{n}$, tada je $m^{y+z} \equiv ab \equiv m^x \pmod{n}$. Zaključujemo da je $m^{y+z-x} \equiv 1 \pmod{n}$ a kako je m primitivan korijen modulo n, slijedi $y + z - x \equiv 0 \pmod{\varphi(n)}$.

2. Neka je $\operatorname{ind}_m(1) = w$. Tada je $1 \equiv m^w \pmod{n}$. Kako je m primitivan korijen modulo n, tada je $w \equiv 0 \pmod{\varphi(n)}$.

3. Neka je kao u dokazu za 1. $a \equiv m^y \pmod{n}$. Stoga je $a^t \equiv m^{yt} \pmod{n}$ pa slijedi da je $\operatorname{ind}_m(a^t) \equiv t \cdot \operatorname{ind}_m(a) \pmod{\varphi(n)}$.

4. Ovo svojstvo slijedi iz $m^{2\text{ind}(-1)} \equiv (-1)^2 \equiv 1 \pmod{n}$ i $\text{ind}(-1) < \varphi(n)$.

Primjetimo da su svojstva 1), 2) i 3) iz teorema analogna svojstvima logaritamske funkcije.

Propozicija 2.1. *Neka su $n, m \in \mathbb{N}$ i $a \in \mathbb{Z}$. Kongruencija $x^m \equiv a \pmod{p}$ ima jedinstveno rješenje ako je $(m, p-1) = 1$.*

Dokaz. Iz pretpostavke propozicije imamo

$$x^m \equiv a \pmod{p}.$$

Koristeći prethodni teorem, tj. 3. svojstvo indeksa dobijemo

$$m \cdot \text{ind}x \equiv \text{ind}a \pmod{p-1},$$

pa kako je po pretpostavci propozicije $(m, p-1) = 1$, slijedi da promatrana kongruencija ima jedinstveno rješenje. □

Definicija 2.2. *Neka su $m, n \in \mathbb{N}$, $b \in \mathbb{Z}$ i $(b, n) = 1$. Kažemo da je b m-ta potencija ostataka modulo n ako je $x^m \equiv b \pmod{n}$, za neki $x \in \mathbb{Z}$ i x se zove m-ti korijen od b modulo n.*

Teorem 2.2. *Neka su $e, n \in \mathbb{N}$ takvi da n ima primitivan korijen te neka je $b \in \mathbb{Z}$ takav da je $(b, n) = 1$ i neka je $g = (e, \varphi(n))$. Tada je kongruencija $x^e \equiv b \pmod{n}$ rješiva ako i samo ako je $b^{\frac{\varphi(n)}{g}} \equiv 1 \pmod{n}$ i ako postoji rješenje kongruencije $x^e \equiv b \pmod{n}$, tada postoji točno g nekongruentnih rješenja x modulo n.*

Dokaz. Neka je a primitivan korijen modulo n i $g = (e, \varphi(n))$. Tada vrijedi

$$x^e \equiv b \pmod{n}$$

ako i samo ako je

$$e \cdot \text{ind}_a(x) \equiv \text{ind}_a(b) \pmod{\varphi(n)}.$$

Prethodna kongruencija ima rješenja ako i samo ako g dijeli $\text{ind}_a(b)$. Ako $g | \text{ind}_a(b)$ tada postoji točno g nekongruentnih rješenja modulo $\varphi(n)$ te kongruencije, tj. tada postoji točno g cijelih brojeva x koji su nekongruentni modulo n u kongruenciji $x^e \equiv b \pmod{n}$. Kako g dijeli $\text{ind}_a(b)$ ako i samo ako je

$$\text{ind}_a(b)\frac{\varphi(n)}{g} \equiv 0 \pmod{\varphi(n)},$$

tj. ako i samo ako je

$$(a^{\text{ind}_a(b)})^{\frac{\varphi(n)}{g}} \equiv b^{\frac{\varphi(n)}{g}} \equiv 1$$

dolazimo do tražene tvrdnje. □

Primjenom prethodnog teorema na proste brojeve dobivamo sljedeći korolar.

Korolar 2.1. *Neka je p neparan prost broj, $c, e \in \mathbb{N}$ i $b \in \mathbb{Z}$ takav da je $(p, b) = 1$, tada je $x^e \equiv b \pmod{p^c}$ ako i samo ako je*

$$b^{\frac{p^{c-1}(p-1)}{g}} \equiv 1 \pmod{p^c},$$

gdje je $g = (e, p^{c-1}(p-1))$. Štoviše, ako postoji rješenje tada postoji točno g nekongruetnih rješenja modulo p^c.

Korolar 2.2. *Ako je $p > 2$ prost broj i $b \in \mathbb{Z}$ takav da je $(p, b) = 1$, tada je kongruencija $x^2 \equiv b \pmod{p}$ rješiva ako i samo ako je $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Dokaz. U Korolaru 2.1 stavimo da je $c = 1$, $e = 2$, $g = 2$ i dolazimo do tražene tvrdnje.□

Korolar 2.3. *Ako je $p > 2$ prost broj, tada za bilo koji $d \in \mathbb{N}$ takav da $d|(p-1)$, kongruencija $x^d \equiv 1 \pmod{p}$ ima točno d mogućih rješenja.*

Dokaz. U Korolaru 2.1 stavimo da je $b = c = 1$ i $e = g = d$. □

Korolar 2.4. *Ako je a primitivan korijen modulo neparni prost broj p i $b \in \mathbb{Z}$, tada je kongruencija $b \equiv x^2 \pmod{p}$ rješiva ako i samo ako $2|\text{ind}_a(b)$.*

Dokaz. Neka je $b \equiv a^j \pmod{p}$, gdje je $j = \text{ind}_a(b)$. Tada je $a \equiv b \cdot (a^{-1})^{j-1} \pmod{p}$, gdje je a^{-1} multiplikativni inverz od a modulo p. Prema Korolaru 2.2, $x^2 \equiv b \pmod{p}$ je rješiva ako i samo ako je $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Ako je j neparan slijedi

$$a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} (a^{\frac{1-j}{2}})^{p-1} \equiv 1 \pmod{p},$$

a to je kontradikcija s pretpostavkom da je a primitivan korijen modulo p. Zaključujemo da je j paran. □

Korolar 2.5. *Neka $n \in \mathbb{N}$ ima primitivan korijen i neka je $b \in \mathbb{Z}$ takav da je $(b, n) = 1$. Tada je b e-ta potencija ostataka modulo n ako i samo ako je $b^{\frac{\varphi(n)}{g}} \equiv 1 \pmod{n}$, gdje je $g = (e, \varphi(n))$. Štoviše, postoji $\frac{\varphi(n)}{g}$ takvih brojeva b i svaki od njih je e-ta potencija od točno g cijelih brojeva modulo n.*

Dokaz. Uočimo da prema Teoremu 2.2 trebamo samo pronaći broj nekongruentnih rješenja od $x^{\frac{\varphi(n)}{g}} \equiv 1 \pmod{n}$. Ako je a primitivan korijen modulo n, tada je $\frac{\varphi(n)}{g}$ brojeva $a^g, a^{2g}, \ldots, a^{\frac{\varphi(n)}{g} \cdot g}$ nekongruentno modulo n. Svaki od tih brojeva služi kao e-ta potencija ostataka što nam daje traženu tvrdnju. □

U nastavku ćemo riješiti nekoliko primjera vezanih za rješavanje kongruencija pomoću primitivnih indeksa.

Primjer 2.2. *Riješimo kongruenciju $7x^3 \equiv 3 \pmod{11}$.*

Rješenje. Uzimamo indekse s obzirom na primitivan korijen 2, što dovodi do

$$\text{ind}_2(7x^3) \equiv \text{ind}_2(3) \pmod{10},$$

iz čega slijedi, prema Teoremu 2.1,

$$\text{ind}_2(7) + 3\text{ind}_2(x) \equiv \text{ind}_2(3) \pmod{10}.$$

Iz Primjera 2.1 imamo da je $\text{ind}_2(3) = 8$ i $\text{ind}_2(7) = 7$, iz čega slijedi

$$\begin{aligned} 3\text{ind}_2(x) &\equiv 1 \pmod{10} \\ \text{ind}_2(x) &\equiv 7 \pmod{10}, \end{aligned}$$

što nam daje $x \equiv 7 \pmod{11}$.

Primjer 2.3. *Riješimo kongruenciju* $7^x \equiv 7 \pmod{17}$.

Rješenje. Uzimamo indekse s obzirom na primitivan korijen 2 pa dolazimo do sljedećeg oblika

$$\text{ind}_2(7^x) \equiv \text{ind}_2(7) \pmod{16},$$

iz čega slijedi, prema Teoremu 2.1,

$$x\text{ind}_2(7) \equiv \text{ind}_2(7) \pmod{16}.$$

Rješenje je $x \equiv 1 \pmod{17}$.

Primjer 2.4. *Nađimo ostatak pri dijeljenju* $3^{24} \cdot 5^{13}$ *brojem 17.*

Rješenje. Dana je kongruencija

$$x \equiv 3^{24} \cdot 5^{13} \pmod{17}.$$

Uzimamo indekse s obzirom na primitivan korijen 3 te dolazimo do

$$\begin{aligned} \text{ind}_3(x) &\equiv 24\text{ind}_3(3) + 13\text{ind}_3(5) \pmod{16} \\ &\equiv 24 \cdot 1 + 13 \cdot 5 \pmod{16} \\ &\equiv 9 \pmod{16}. \end{aligned}$$

Stoga je $x \equiv 14 \pmod{17}$.

3. Problemi vezani uz primitivne korijene i indekse

3.1. Artinova hipoteza

Artinova hipoteza o primitivnim korijenima iz 1927. godine dana je s: za bilo koji dani cijeli broj $a \neq 0, -1$ različit od potpunog kvadrata postoji beskonačno mnogo prostih brojeva p za koje je a primitivan korijen modulo p. Asimptotska gustoća ovih prostih brojeva usko je vezana uz tzv. Artinovu konsantnu koja je dana sljedećom formulom

$$C_{Artin} = \prod_{p \text{ primitivan}} \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\cdots$$

Primjer 3.1. *Uzmimo da je $a = 2$. Hipoteza tvrdi da skup prostih brojeva p za koji je 2 primitivni korijen ima gustoću C_{Artin} u skupu prostih brojeva. Skup takvih prostih brojeva je*

$$S(2) = \{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101,$$
$$107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227,$$
$$269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443,$$
$$461, 467, 491, \cdots\}.$$

Ima 38 takvih elemenata manjih od 500 i 95 prostih brojeva manjih od 500. Omjer (koji teži C_{Artin}) je $\frac{38}{95} = 0.4$.

Godine 1967. Hooley [9] je objavio uvjetni dokaz za hipotezu, baziran na generaliziranoj Riemannovoj hipotezi. Više o Artinovoj hipotezi može se naći u [14].

3.2. Kriptosustavi s javnim ključem

Kriptosustav s javnim ključem je bilo koji kriptosustav koji koristi: javni ključ koji može biti poznat svima i privatni ključ koji je poznat samo vlasniku. Svi simetrični kriptosustavi su temeljeni na tome da pošiljatelj i primatelj biraju ključ K, te na osnovu njega iz kriptosustava dobiju funkcije za šifriranje i dešifriranje čiji je argument šifrat. Kriptosustav se sastoji od dva skupa funkcija: funkcije za šifriranje e_K i funkcije za dešifriranje d_K, gdje K prolazi skupom svih mogućih ključeva. Pošto šifriranje većeg broja poruka istim ključem znatno smanjuje sigurnost, pošiljatelj i primatelj moraju često mijenjati ključ.

Definicija 3.1. *Neka je G grupa obzirom na operaciju $*$. Problem diskretnog logaritma u G je pronaći, za bilo koja dva elementa $g, a \in G$, x koji zadovoljava*

$$\underbrace{g * g * g * \ldots * g}_{x \text{ puta}} = a$$

3.2.1. Diffie-Hellman problem

Whitfield Diffie i Martin Hellman [3] su ponudili rješenje problema razmjene ključeva, koje je zasnovano na činjenici da je potenciranje u nekim grupama jednostavnije od logaritmiranja. U nastavku ćemo opisati Diffie–Hellmanov algoritam za razmjenu ključeva putem nesigurnog komunikacijskog kanala, koji je nastao 1976. godine, a zasniva se na teškoći računanja g^{ab} iz poznavanja g^a i g^b. Osobe koje razgovaraju imaju, za kriptografiju standardna imena, Alice i Bob. Neka su A i B osobe koje se pokušavaju dogovoriti o tajnom slučajnom elementu u cikličkoj grupi G, bez da su prethodno razmijenile bilo kakvu informaciju. Osobe A i B

moraju provesti taj dogovor preko nesigurnog komunikacijskog kanala. Znaju jedino informaciju da je G grupa i da je g generator grupe G.

Diffie-Hellmanov algoritam za razmjenu ključeva:

1. Odabere se veliki prost broj p i generator g grupe $\mathbb{Z}_p^*$ i objave se kao javni.
2. Osoba A generira slučajan prirodan broj $a \in \{1, 2, \ldots, p-1\}$. Ona pošalje osobi B rezultat $A = g^a \mod p$.
3. Osoba B generira slučajan prirodan broj $b \in \{1, 2, \ldots, p-1\}$ te pošalje osobi A rezultat $B = g^b \mod p$.
4. Osoba A izračuna $B^a = (g^b \mod p)^a = g^{ab} \mod p$.
5. Osoba B izračuna $A^b = (g^a \mod p)^b = g^{ab} \mod p$.

Sada je njihov tajni ključ $K = g^{ab} \mod p$.

Njihov protivnik, koji može prisluškivati njihovu komunikaciju preko nesigurnog kanala, sazna generator g, grupu G (tj. prost broj n) te vrijednosti g^a i g^b. Cilj mu je izračunati g^{ab}, tj. riješiti Diffie–Hellmanov problem. Ukoliko je on u mogućnosti riješiti problem diskretnog logaritma pa iz g^a i g izračunati a, onda mu je lako, pomoću a i g^b, izračunati g^{ab}. Vjeruje se da su Diffie–Hellmanov problem i problem diskretnog logaritma, u većini grupa koje se koriste u kriptografiji, ekvivalentni.

Primjer 3.2. *Alice i Bob kreiraju tajni ključ preko nesigurnog komunikacijskog kanala.*

Rješenje

1. U telefonskom razgovoru (javno) se dogovore da uzmu $p = 13$ i $g = 2$ kao generator grupe $\mathbb{Z}_{13}^*$.
2. Alice bira $a = 11$ i računa $A = 2^{11} \mod 13 = 7$ te šalje Bobu $A = 7$.
3. Bob bira $b = 9$ i računa $B = 2^9 \mod 13 = 5$ i šalje Alice $B = 5$.
4. Alice računa $B^a = 5^{11} \mod 13 = 8$, a Bob računa $A^b = 7^9 \mod 13 = 8$.

Alice i Bob su dobili isti rezultat pa je njihov tajni ključ $K = 8$.

3.2.2. ElGamalov kriptosustav

U ovom odjeljku opisat ćemo ElGamalov kriptosustav koji je 1985. godine predložio Taher ElGamal [7], a zasnovan je na teškoći računanja diskretnog logaritma odnosno indeksa u grupi $(\mathbb{Z}_p^*, \cdot_p)$. Može se pokazati da je po složenosti ovaj problem vrlo sličan problemu faktorizacije, a i metode koje se koriste u najboljim poznatim algoritmima za rješavanje tih problema su vrlo slične.

Definicija 3.2. *Neka je p prost broj i $\alpha \in \mathbb{Z}_p^*$ primitivan korijen modulo p. Neka je prostor otvorenih tekstova $\mathcal{N} = \mathbb{Z}_p^*$, prostor šifrata $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ i prostor ključeva*

$$\mathcal{K} = (p, \alpha, a, \beta) : \beta = \alpha^a \mod p.$$

Vrijednosti p, α i β su javne, a vrijednost a je tajna. Za $K = (p, \alpha, a, \beta) \in \mathcal{K}$ i tajni slučajni broj $k \in \mathbb{Z}_{p-1}$ definiramo

$$e_K(x, k) = (\alpha^k \mod p, x\beta^k \mod p).$$

Za $y_1, y_2 \in \mathbb{Z}_p^*$ definiramo

$$d_K(y_1, y_2) = y_2(y_1^a)^{-1} \mod p.$$

Otvoreni tekst x se sakrije množeći s β^k. Osoba koja zna tajni eksponent a može iz α^k izračunati β^k i tako otkriti tekst. Da bi eksponent a bio tajan, prost broj p mora biti jako velik da bi problem diskretnog logaritma u $\mathbb{Z}_p^*$ bilo takoreći nemoguće rješiti.

Primjer 3.3. *Neka je $p = 23, \alpha = 5, a = 17, \beta = 15$. Dešifrirajmo $(y_1, y_2) = (17, 6)$.*

Rješenje Računamo $y_1 = 17^{17} \equiv 11 \mod 23$, zatim tražimo inverz od 11 modulo 23. Dobije se da je to $-2 \equiv 21 \mod 23$. Na kraju izračunamo $6 \cdot 21 \mod 23$ i dobije se $x = 11$.

3.2.3. Solovay - Strassenov test prostosti

Solovay - Strassenov test prostosti, kojeg su razvili Robert M. Solovay i Volker Strassen [16], određuje je li neki broj prost ili složen. Za ispitivanje prostosti broja potrebno je računanje najvećih zajedničkih djelitelja i Jacobijevih simbola. U nastavku navodimo jednu od verzija ovog algoritma.

Algoritam za odeđivanje prostosti broja n preko Solovay - Strassenovog testa:

1. Izabrati bilo koji broj $a < n$.
2. Ako je $(a, n) > 1$, tada je n složen broj.
3. Ako je $(a, n) = 1$, tada izračunaj $\left(\frac{a}{n}\right)$ i $a^{\frac{n-1}{2}}$.
4. Ako je $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod p$, onda je n složen, u suprotnom se vrati na korak 1.
5. Ukoliko test ne staje nakon određenog broja pokušaja, broj je vjerojatno prost.

Tvrdnje na kojima se bazira Solovay - Strassenov test prostosti se dokazuju korištenjem primitivnih korijena i indeksa. Više o Solovay - Strassenovom testu prostosti može se naći u [5] i [12].

Literatura

[1] *Artin's conjecture on primitive roots*,
URL: https://en.wikipedia.org/wiki/Artin%27s_conjecture_on_primitive_roots

[2] M. Baker, *Notes on primitive roots,*
URL: http://people.math.gatech.edu/~mbaker/pdf/primroots.pdf

[3] W. Diffie, M.E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, 22, 109–112, 1976.

[4] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta).

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

[6] A. Dujella, *Kriptosustavi zasnovani na problemu diskretnog logaritma u konačnoj grupi*, PMF-MO, Sveučilište u Zagrebu,
URL: https://web.math.pmf.unizg.hr/~duje/ecc/dlp.html

[7] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10–18. Springer-Verlag New York, Inc., 1985.

[8] J. Hoffstein, J. Pipher, J. H. Silverman, *An introduction to mathematical cryptography, Springer*, New York, 2008.

[9] C. Hooley, *On Artin's conjecture*, Journal für die reine und angewandte Mathematik 225(1967), 209-220.

[10] B. Ibrahimpašić, D. Kovačević, *Diskretni logaritam* , Banja Luka
URL: http://elib.mi.sanu.ac.rs/files/journals/mk/2/mkn2p43-52.pdf

[11] A. A. Karatsuba, *Complex analysis in number theory*, Steklov Mathematical Institute Russian Academy of Sciences Moscow, 1995.

[12] P. P. Kurur, *Computational Number Theory*,
URL: http://www.cmi.ac.in/~ramprasad/lecturenotes/comp_numb_theory/lecture2021.pdf

[13] R.A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, New York, 2008.

[14] P. Moree, *Artin's primitive root conjecture*,
URL: http://guests.mpim-bonn.mpg.de/moree/surva.pdf

[15] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer-Verlag, NY, 2000.

[16] R. Solovay, V. Strassen, *A fast Monte-Carlo test for primality*, Siam J. Comput., 6 (1977), pp. 84-85.

[17] J. J. Tattersall, *Elementary Number Theory in Nine Chapters*, Springer-Verlag, NY, 2000.