Primitivni korijeni i njihova primjena

Semeš, Sara

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Sara Semeš

Primitivni korijeni i njihova primjena

Završni rad

Osijek, 2021.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Sara Semeš

Primitivni korijeni i njihova primjena

Završni rad

Mentor: izv.prof. dr. sc. Ivan Soldo

Osijek, 2021.

Sažetak

Tema ovoga rada su primitivni korijeni, indeksi i njihove primjene. Najprije ćemo uvesti bitne rezultate teorije brojeva koji će nam kasnije u radu pomoći definirati pojmove primitivnih korijena i indeksa te primijeniti to na različitim primjerima i vidjeti kako se oni računaju. Na kraju ćemo vidjeti neke poznatije probleme kao što su Artinova hipoteza, Diffie-Hellmanov problem te Shanksov algoritam.

Ključne riječi

Wilsonov teorem, Eulerova funkcija, Eulerov teorem, Mali Fermatov teorem, indeksi, primitivni korijeni, Artinova hipoteza, Diffie-Hellmanov, Shanksov algoritam

Primitive roots and their applications

Summary

In this paper, we will deal with primitive roots, indices, and their applications. Firstly, we will introduce some important results in theory of numbers which will help us later in the paper to define terms of primitive roots and indices. Further, we will apply it to different examples and see how they are calculated. Finally, we will see some well-known problems related to primitive roots and indices such as the Artin's hypothesis, the Diffie-Hellman problem and the Shanks algorithm.

Keywords

Wilson theorem, Euler function, Euler theorem, Fermat Little theorem, indices, primitive roots, Artin hypothesis, Diffie-Hellman problem, Shanks algorithm

Sadržaj

Uvod **i**

1 Djeljivost **1**

2 Kongruencije **3**

2.1 Linearne kongruencije 5

2.2 Reducirani sustav ostataka 7

2.3 Kineski teorem o ostacima 9

3 Primitivni korijeni **11**

3.1 Red i definicija primitivnog korijena 11

3.2 Egzistencija primitivnog korijena 12

4 Neke primjene primitivnih korijena **19**

4.1 Artinova hipoteza 19

4.2 Diffie-Hellmanov problem 19

4.3 Shanksov algoritam 21

Literatura **22**

Uvod

Primitivni korijeni jedni su od temeljnih i važnijih pojmova u teoriji brojeva. Stoga ćemo u ovom završnom radu vidjeti koji prirodni brojevi imaju primitivne korijene, koja su njihova svojstva te koja je njihova primjena. U prvom i drugom poglavlju navest ćemo osnovne rezultate teorije brojeva, odnosno rezultate iz poglavlja djeljivosti i kongruencija. U trećem poglavlju definirat ćemo pojam reda i primitivnih korijena te iskazati neka njihova svojstva. U četvrtom poglavlju upoznat ćemo se važnim primjenama indeksa i primitivnih korijena.

1 Djeljivost

Teorija brojeva jedna je od područja matematike u kojem se proučavaju karakteristike pozitivnih cijeli brojeva uključujući djeljivost, najveći zajednički djelitelj te proste brojeve. Djeljivost je temeljni pojam u teoriji brojeva te će nam pomoći kasnije u radu za definiranje reda i primitivnih korijena. U ovome poglavlju iskazat ćemo definicije djeljivosti, najvećeg zajedničkog djelitelja i prostih brojeva te iskazati jedan od najbitnijih rezultata ovoga dijela gradiva. Iskažimo sada definiciju djeljivosti.

Definicija 1. *Ako su $a \neq 0$ i b cijeli brojevi takvi da je $b = ax$ za neki cijeli broj x, onda kažemo da a dijeli b i pišemo $a|b$. Ako a ne dijeli b, tada pišemo $a \nmid b$. Dodatno, za a kažemo da je djelitelj broja b, a za b kažemo da je višekratnik broja a.*

Primjer 1. *Vrijedi $2|4$, $7|21$, $3|0$.*

Sada ćemo iskazati jedan od osnovnih i najvažnijih teorema teorije brojeva.

Teorem 1 (Teorem o dijeljenju s ostatkom, [3, Teorem 2.2.])**.** *Za proizvoljne brojeve $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ postojat će jedinstveni brojevi $q, r \in \mathbb{Z}$ takvi da je $b = qa + r$, za $0 \leq r < a$.*

Dokaz. Može se vidjeti u [3]. □

Primjer 2. *Prema Teoremu 1. primijetimo da vrijedi $17 = 5 \cdot 3 + 2$ i $-17 = -5 \cdot 4 + 3$.*

Definicija 2. *Za cijele brojeve a,b i c takve da a dijeli b i a dijeli c kažemo da je a zajednički djelitelj brojeva b i c. Postojat će konačno mnogo zajedničkih djelitelja brojeva b i c ako je barem ili b ili c različit od nule. Najveći takav zajednički djelitelj nazivamo najveći zajednički djelitelj brojeva b i c i pišemo $nzd(b, c)$.*

Primjer 3. *Odredimo najveći zajednički djelitelj brojeva 3 i 9 te najveći zajednički djelitelj brojeva 2 i 4. Vrijedi: $(3, 9) = 3$, $(2, 4) = 2$.*

Definicija 3. *Reći ćemo da je pozitivan cijeli broj $p > 1$ prost ako p nema nijednog djelitelja d takvog da je $1 < d < p$. Za pozitivan cijeli broj $a > 1$ koji nije prost reći ćemo da je složen.*

Primjer 4. *Brojevi $2, 3, 5, 7, 11, 13 \ldots$ su prosti brojevi.*

Definicija 4. *Ako je $nzd(a, b) = 1$ za neke cijele brojeve a i b, onda kažemo da su a i b relativno prosti. Reći ćemo da su cijeli brojevi $a_1, a_2, \ldots, a_n$ relativno prosti ako je njihov najveći zajednički djelitelj jednak 1, a ako je $nzd(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n, i \neq j$, tada ćemo reći da su oni u parovima relativno prosti.*

Primjer 5. *Vrijedi $(2, 3) = 1$, $(9, 7) = 1$.*

Napomena 1. *Ako su neki cijeli brojevi u parovima relativno prosti, oni su i relativno prosti. S druge strane, relativno prosti cijeli brojevi ne moraju biti u parovima relativno prosti.*

Primjer 6. *Pogledajmo brojeve 10, 15 i 6. Primijetimo kako vrijedi $(10, 6, 15) = 1$, ali ne vrijedi da su ti brojevi u parovima relativno prosti.*

Sada ćemo iskazati i dokazati propoziciju koja govori o jednom važnom svojstvu djeljivosti.

Propozicija 1 (vidjeti [3, Propozicija 2.11.]). *Ako za prost broj p vrijedi da p dijeli produkt ab, tada p dijeli a ili p dijeli b. Generalno, ako p dijeli produkt $a_1a_2 \cdot \cdots \cdot a_n$, tada p mora dijeliti barem jedan od faktora.*

Dokaz. Ako prosti broj p ne dijeli a, tada će značiti kako su oni relativno prosti, pa će zbog toga postojati cijeli brojevi x i y takvi da će biti $ax + py = 1$. Množeći obje strane s b, dobit ćemo $abx + pby = b$, što povlači kako će p dijeliti b. Drugi dio propozicije dokazuje se indukcijom. Pretpostavimo kako $p|a_1 \cdot a_2 \cdot a_3 \cdots a_n$. Znači da će p dijeliti ili a_1 ili $a_2 \cdot a_3 \cdots a_n$, a ako p dijeli $a_2 \cdot a_3 \cdots a_n$, onda će p dijeliti neki a_i za $i = 2, \ldots, n$. □

Sljedeći teorem naziva se Osnovni teorem aritmetike i jedan je od najvažnijih karakterizacija prostih brojeva. Naime, svaki prirodni broj koji je veći od 1, možemo na jedinstveni način napisati u obliku produkta prostih brojeva.

Teorem 2 (Osnovni teorem aritmetike [3, Propozicija 2.12.]). *Za svaki prirodan broj n veći od 1, faktorizacija na proste faktore bit će jedinstvena do na poredak prostih faktora.*

Dokaz. Može se pogledati u [3]. □

2 Kongruencije

Teoriju kongruencija uveo je njemački matematičar Carl Friedrich 1801. godine. U ovome poglavlju definirat ćemo i iskazati, a i navesti dokaze nekih bitnih rezultata i svojstava teorije kongruencija koji će nam kasnije u radu pomoći kod definiranja reda i primitivnih korijena. Najprije, iskažimo definiciju kongruencije.

Definicija 5. *Ako je $m \neq 0$ pozitivan cijeli broj takav da $m|a-b$, za neke cijele brojeve a i b, onda ćemo reći da je a kongruentan b modulo m. Ako m ne dijeli razliku $a-b$, kažemo da a nije kongruentan b modulo m i označavamo $a \not\equiv b \pmod{m}$.*

Primjer 7. *Primijetimo kako vrijedi $-3 \equiv 4 \pmod 7$, $6 \equiv 13 \pmod 7$.*

Kao prvo svojstvo kongruencija, u sljedećoj propoziciji, pokazat ćemo da je relacija "biti kongruentan modulo m" relacija ekvivalencije na skupu cijelih brojeva.

Propozicija 2 (vidjeti [3, Propozicija 3.1.])**.** *Relacija "biti kongruentan modulo m" relacija je ekvivalencije na skupu cijelih brojeva.*

Dokaz. Relacija ekvivalencije je svaka relacija koja je refleksivna, simetrična i tranzitivna. Refleksivnost i simetričnost slijede direktno iz definicije kongruencije. Za dokaz tranzitivnosti pretpostavimo da su $a \equiv b \pmod m$ i $b \equiv c \pmod m$. Dakle, postojat će cijeli brojevi x i y takvi da je $a-b=mx$ i $b-c=my$. Kako je:

$$a-c=(a-b)+(b-c)=mx+my=m(x+y),$$

slijedi da je $a \equiv c \pmod m$. □

U idućoj propoziciji vidjet ćemo sličnosti između kongruencija i klasične jednakosti. Naime, kongruencije na sličan način kao i jednakosti možemo zbrajati, oduzimati i množiti.

Propozicija 3 (vidjeti [3, Propozicija 3.2.])**.** *Za cijele brojeve a,b,c i d vrijedi:*

(*i*) *Ukoliko je $a \equiv b \pmod m$, tada je $a+c \equiv b+d \pmod m$, $a-c \equiv b-d \pmod m$ i $ac \equiv bd \pmod m$.*

(*ii*) *Ukoliko je $a \equiv b \pmod m$ i ako d dijeli m, tada je $a \equiv b \pmod m$.*

(*iii*) *Ukoliko je $a \equiv b \pmod m$, tada je za svaki $c \neq 0$ $ac \equiv bd \pmod{mc}$.*

Dokaz.

(i) Uzmemo da su $a-b=mx$ i $c-d=my$. Iz $(a+c)-(b+d)=m(x+y)$ i $(a-c)-(b-d)=m(x-y)$ slijedit će nam kako je $a+c \equiv b+d \pmod m$ i $a-c \equiv b-d \pmod m$. Zbog $ac-bd=a(c-d)+d(a-b)=amy+dmx=m(ay+dx)$ slijedi $ac \equiv bc \pmod{mc}$.

(ii) Uzmimo da je $m=dz$. Onda će iz $a-b=mx$ slijediti $a-b=d\cdot(zx)$, pa je $a \equiv b \pmod d$.

(iii) Ako je $a - b = mx$, tada je $ac - bc = (mc) \cdot x$, pa slijedi da je $ac \equiv bc \pmod{mc}$.

□

Pogledajmo sada kako neke tvrdnje iz prethodne propozicije funkcioniraju na primjeru.

Primjer 8.

1) Ako su $-3 \equiv 4 \pmod 7$ *i* $6 \equiv 13 \pmod 7$, *imamo da je* $-3 + 6 \equiv 4 + 13 \pmod 7$, *odnosno* $3 \equiv 17 \pmod 7$.

2) Ako je $-3 \equiv 4 \pmod 7$, *onda je i* $-3 \cdot 2 \equiv 4 \cdot 2 \pmod{7 \cdot 2}$, *tj.* $-6 \equiv 8 \pmod{14}$.

U idućoj propoziciji vidjet ćemo svojstvo kongruencija s obzirom na polinome s cjelobrojnim koeficijentima.

Propozicija 4 (vidjeti [3, Propozicija 3.3.])**.** *Ako je* $a \equiv b \pmod m$, *tada za polinom* f *s cjelobrojnim koeficijentima vrijedi* $f(a) \equiv f(b) \pmod m$.

Dokaz. Uzmimo polinom f s cjelobrojnim koeficijentima. Dakle, $f(x) = d_n x^n + d_{n-1}x^{n-1} + \cdots + d_0$. Kako vrijedi $a \equiv b \pmod m$, a s obzirom na to da se kongruencije s istim modulima mogu množiti, zbrajati i oduzimati na isti način kao kod jednakosti, imamo da je $a^2 \equiv b^2 \pmod m, \cdots, a^n \equiv b^n \pmod m$. Nadalje, iz ovoga će slijediti kako je $d_i a^i \equiv d_i b^i \pmod m$, pa vrijedi:

$$d_n a^n + d_{n-1}a^{n-1} + \cdots + d_0 \equiv d_n b^n + d_{n-1}b^{n-1} + \cdots + d_0 \pmod m.$$

□

Klasa ekvivalencije relacije biti kongruentan modulo m kojoj pripada cijeli broj a, zapisuje se kao $a + m\mathbb{Z}$. Dakle, $a + m\mathbb{Z}$ je skup svih cijelih brojeva b tako da je $b \equiv a \pmod m$, odnosno skup svih cijelih brojeva oblika $a + mx$ za neki cijeli broj x. Ako $(a + m\mathbb{Z}) \cap (b + m\mathbb{Z}) \neq \emptyset$, tada je $a + m\mathbb{Z} = b + m\mathbb{Z}$. Prema teoremu o dijeljenju s ostatkom, postoji točno m različitih klasa ekvivalencije: $[0], [1], \ldots, [m-1]$. S $\mathbb{Z}/m\mathbb{Z}$ označavamo skup svih klasa ekvivalencije, tj. kvocijentni skup po relaciji biti kongruentan modulo m. Klasu ekvivalencije relacije biti kongruentan modulo m nazivamo klasa ostataka modulo m.

Definicija 6. *Ako za svaki cijeli broj* y *postoji točno jedan* x_i *iz skupa* $\{x_1, x_2, \ldots, x_n\}$ *takav da je* $y \equiv x_i \pmod m$, *onda kažemo da je skup* $\{x_1, x_2, \ldots, x_n\}$ *potpuni sustav ostataka modulo* m. *Odnosno, ako uzmemo po jedan član iz svake klase ekvivalencije modulo* m *dobit ćemo potpuni sustav ostataka.*

Primjer 9. *Na primjer, skup* $\{1, 2, \ldots, m-1\}$ *čini potpun sustav ostataka modulo* m, *ili recimo skup* $\{0, 1, 2, 3, 4, 5\}$ *čini potpun sustav ostataka modulo* 6.

Sljedeći rezultat govori nam o jednom važnom svojstvu potpunih sustava ostataka modulo m.

Teorem 3 (vidjeti [3, Teorem 3.5.]). *Ako je skup* $\{x_1, \ldots, x_m\}$ *potpun sustav ostataka modulo* m *i ako za cijeli broj* a *vrijedi da su* a *i* m *relativno prosti, onda će skup* $\{ax_1, \ldots, ax_m\}$ *također biti potpun sustav ostataka modulo* m.

Dokaz. Potrebno je samo dokazati da je za $i \neq j$ vrijedi $ax_i \not\equiv ax_j \pmod{m}$. Pa pretpostavimo suprotno, odnosno neka je $ax_i \equiv ax_j \pmod{m}$. Kako su a i m relativno prosti, slijedi $x_i \equiv x_j \pmod{m}$, odnosno $i = j$. □

Primjer 10. *Uzmimo jedan potpuni sustav ostataka modulo* 6, *npr.* $\{0, 1, 2, 3, 4, 5\}$. *Kako su* $(5, 6) = 1$, *slijedi kako je i* $\{0, 5, 10, 15, 20, 25\}$ *također potpun sustav ostataka modulo* 6.

2.1 Linearne kongruencije

U ovome poglavlju proučavat ćemo linearne kongruencije oblika $ax \equiv b \pmod{m}$. Pokazat ćemo na primjerima kada takva kongruencija ima rješenja i probat ćemo izračunati sva rješenja. Sljedeći je teorem jedan od najkorisnijih i najvažnijih alata u elementarnoj teoriji brojeva.

Teorem 4 (vidjeti [6, Theorem 2.2.]). *Ako su* a, b *i* $m \geq 1$, *cijeli brojevi i* $d = (a, m)$ *najveći zajednički djelitelj brojeva* a *i* m, *tada će kongruencija*

$$ax \equiv b \pmod{m} \tag{1}$$

imati rješenja onda i samo onda ako je

$$b \equiv 0 \pmod{d}.$$

Ako je $b \equiv 0 \pmod{d}$, *onda kongruencija* (1) *ima točno* d *rješenja. Nadalje, ako su* a *i* m *relativno prosti, tada za svaki cijeli broj* b *kongruencija* (1) *ima jedinstveno rješenje modulo* m.

Dokaz. Može se vidjeti u [6]. □

Primjer 11. *Uzmimo kongruenciju* $21x \equiv 20 \pmod{42}$. *Znamo da je* $d = (21, 42) = 21$. *Prema prethodnom teoremu, možemo zaključiti kako ova kongruencija nema rješenja s obzirom na to kako* $d = 21$ *ne dijeli 20.*

U idućem rezultatu saznat ćemo nešto više o kompletnom skupu nekongruentnih rješenja modulo m.

Teorem 5 (vidjeti [7, Corollary 4.1.]). *Ako je* x_0 *rješenje kongruencije* $ax \equiv b \pmod{m}$ *i* $d = (a, m)$, *brojevi*

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$$

čine kompletni skup nekongruentnih rješenja modulo m.

Sljedeći je teorem vrlo važan u teoriji kongruencija. Naime, pomoću Euklidovog teorema možemo na jednostavan način doći do rješenja linearnih kongruencija.

Teorem 6 (Euklidov algoritam [3, Theorem 2.7.]). *Ako su b i c pozitivni cijeli brojevi takvi da je $b > c$ i ako je uzastopnom primjenom Teorema 1. dobiven niz jednakosti*

$$\begin{aligned} b &= cq_1 + r_1, \ 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \ 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \ 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j, \ 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_j + 1, \end{aligned}$$

onda će najveći zajednički djelitelj brojeva b i c biti jednak posljednjem ostatku r_j koji nije nula. Vrijednosti brojeva x i y iz izraza $nzd(b, c) = bx + cy$ dobivaju se izražavanjem svakog ostatka r_i koji će biti linearna kombinacija brojeva b i c.

Dokaz. Može se vidjeti u [3]. □

Primijenimo sada Teorem 5. i Euklidov algoritam na primjeru.

Primjer 12. *Riješimo sada linearnu kongruenciju $27x \equiv 36 \pmod{45}$ koristeći Euklidov algoritam.*
Rješenje:
Primijetimo kako je $(27, 45) = 9$ i kako $9|36$. Tada slijedi da postoje 9 rješenja modulo 45. Podijelimo sada početnu linearnu kongruenciju s 9. Dobijemo da je $3x \equiv 4 \pmod{5}$. Sada slijedi $(3, 5) = 1$ pa postoje cijeli brojevi u i v takvi da je $3u + 5v = 1$, odnosno $3u \equiv 1 \pmod{5}$. Kako vrijedi:

$$\begin{aligned} 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2, \end{aligned}$$

imamo sljedeću tablicu:

i	-1	0	1	2
q_i			1	1
v_i	1	0	1	-1
u_i	0	1	-1	2

.

Dakle za $u = 2$ vrijedit će

$$\begin{aligned} 3u &\equiv 1 \pmod{5} \\ \Rightarrow 3 \cdot (4u) &\equiv 4 \pmod{5} \\ x_0 = 4u &\equiv 3 \pmod{5}, \end{aligned}$$

gdje je x_0 rješenje kongruencije $3x \equiv 4 \pmod{5}$. Tada će sva rješenja početne kongruencije biti

$$x \equiv 3, 3 + 5, 3 + 2 \cdot 5, 3 + 3 \cdot 5, \ldots, 3 + 8 \cdot 5 \pmod{45}.$$

Sljedeći rezultat govori nam o bitnom svojstvu kongruencija ako imamo prost broj p.

Teorem 7 (Wilsonov teorem [3, Teorem 3.13.]). *Neka je p prost broj. Tada je* $(p-1)! \equiv -1 \pmod{p}$.

Dokaz. Može se vidjeti u [3]. □

Primjer 13. *Uzmimo prost broj 7. Prema Wilsonovom teoremu slijedi kako je* $(7-1)! \equiv -1 \pmod{7}$. *Odnosno, imamo* $720 \equiv -1 \pmod{7}$, *a 7 dijeli 721.*

2.2 Reducirani sustav ostataka

U ovome poglavlju reći ćemo nešto više o načinu dobivanja reduciranog sustava ostataka modulo m. Vidjet ćemo neke bitne rezultate i svojstva takvih reduciranih sustava, ali najprije iskažimo definiciju reduciranih sustava.

Definicija 7. *Za skup cijelih brojeva r_i kažemo da je reducirani sustav ostataka modulo m ako je $nzd\ (r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ za $i \neq j$ te ako za svaki cijeli broj x relativno prost s m postoji r_i takav da je $x \equiv r_i \pmod{m}$.*

Ako imamo potpun sustav ostataka modulo m, reducirani sustav ostataka će činiti svi brojevi toga skupa koji su relativno prosti s m. Pokažimo to na primjeru.

Primjer 14. *Ako je skup $\{0, 1, 2, 3, 4, 5\}$ potpuni sustav ostataka modulo 6, onda će reducirani sustav ostataka modulo 6 biti skup $\{1, 5\}$.*

Aritmetička funkcija je funkcija definirana na pozitivnim cijelim brojevima. Eulerova funkcija $\varphi(m)$ aritmetička je funkcija koja broji broj cijelih brojeva u skupu $\{0, 1, 2, \ldots, m-1\}$ koji su relativno prosti s m. Imamo

$$\begin{aligned} \varphi\ (1) &= 1, \quad \varphi\ (6) = 2 \\ \varphi\ (2) &= 2, \quad \varphi\ (7) = 6 \\ \varphi\ (3) &= 3, \quad \varphi\ (8) = 4 \\ \varphi\ (4) &= 2, \quad \varphi\ (9) = 6 \\ \varphi\ (5) &= 4, \quad \varphi\ (10) = 4. \end{aligned}$$

Ako je p prost broj, tada je $(a,\ m) =\ 1$ za $a =\ 1, \ldots, p-1$ i $\varphi\ (p) = p-1$.
Sada ćemo vidjeti jedno bitno svojstvo reduciranih sustava ostataka modulo m.

Teorem 8 (vidjeti [3, Teorem 3.8.]). *Ako je skup $\{r_1, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m i ako je a cijeli broj koji je relativno prost s m, onda skup $\{ar_1, \ldots, ar_{\varphi(m)}\}$ također čini reducirani sustav ostataka modulo m.*

Dokaz. Slijedi izravno iz činjenice da ako su a i m te b i m relativno prosti, tada su ab i m relativno prosti te iz Teorema 3. □

Primjer 15. *Kako je skup* $\{1,5\}$ *reducirani sustav ostataka modulo 6, a* $(5,6)=1$*, prema prethodnom teoremu slijedi kako je onda i skup* $\{5,25\}$ *reducirani sustav ostataka modulo 6.*

Sljedeći rezultat daje nam bitno svojstvo Eulerove funkcije.

Teorem 9 (Eulerov teorem [3, Teorem 3.9.])**.** *Ako su a i m relativno prosti, onda je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz. Može se vidjeti u [3]. □

Pogledajmo sada jednu kratku primjenu Eulerovog teorema u rješavanju sljedeće linearne kongruencije.

Primjer 16. *Treba riješiti kongruenciju* $6x \equiv 13 \pmod 7$ *koristeći Eulerov teorem.*
Rješenje:
Kako su $(6,7)=1$ *i* $\varphi(7)=7-1=6$*, prema Eulerovom teoremu znamo da vrijedi* $6^6 \equiv 1 \pmod 7$*. Množeći početnu kongruenciju sa* 6^5 *imat ćemo* $6^6x \equiv 6^5 \cdot 13 \pmod 7$*, a kako znamo da je* $6^6 \equiv 1 \pmod 7$ *vrijedi* $x \equiv 6^5 \cdot 13 \pmod 7$*. Preostalo je još odrediti ostatak pri dijeljenju broja* 6^5 *s brojem* 7*. Kako vrijedi* $6^5 \equiv 6 \pmod 7$*, slijedi*

$$x = 6 \cdot 13 = 1 \pmod 7.$$

Pogledajmo još jedno svojstvo kongruencija s obzirom na prost broj p.

Teorem 10 (Mali Fermatov teorem [3, Teorem 3.10.])**.** *Za prost broj p takav da p ne dijeli a, vrijedi* $a^{p-1} \equiv 1 \pmod p$*. Nadalje, vrijedi* $a^p \equiv a \pmod p$ *za svaki cijeli broj a.*

Dokaz. S obzirom na to kako su brojevi $1, 2, \ldots, p-1$ relativno prosti s p, vrijedi da je $\varphi(p) = p-1$ te ako još p ne dijeli a, iz Eulerovog teorema slijedi tvrdnja. No, ako p dijeli a, onda će biti $a^p \equiv a \pmod p$. □

Primjer 17. *Trebamo odrediti ostatak pri dijeljenju broja* 5^{38} *brojem* 17*.*
Rješenje:
Primjenom Fermatovog teorema imamo da je $5^{16} \equiv 1 \pmod{17}$*.*
Slijedi:

$$\begin{aligned} 5^{38} &\equiv (5^{16})^2 \cdot 5^6 \pmod{17} \\ &\equiv 1^2 \cdot 5^6 \pmod{17} \\ &\equiv 5^6 \pmod{17} \\ &\equiv 2 \pmod{17}. \end{aligned}$$

Dakle, ostatak pri dijeljenju broja 5^{38} *brojem* 17 *je* 2*.*

Definicija 8. *Za funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ koja ima sljedeća svojstva:*

1) $\vartheta(1) = 1$,

2) $\vartheta(mn) = \vartheta(m)\vartheta(n)$, *za sve cijele brojeve m i n koji su relativno prosti,*

kažemo da je multiplikativna funkcija.

Teorem 11 (vidjeti [3, Teorem 3.11.]). *Eulerova funkcija φ je multiplikativna. Posebno, za svaki pozitivan cijeli broj n veći od 1 vrijedi*

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

Dokaz. Može se vidjeti u [3]. □

2.3 Kineski teorem o ostacima

U ovome poglavlju vidjet ćemo kako pronaći rješenje ako imamo sustav linearnih kongruencija i pretpostavku da su one u parovima relativno prostih modula. O načinu pronalaska takvih rješenja govori nam Kineski teorem o ostacima (KTO).

Teorem 12 (Kineski teorem o ostacima [3, Teorem 3.7.]). *Ako su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti pozitivni cijeli brojevi i ako su $a_1, a_2, \ldots, a_r$ cijeli brojevi, onda će sustav kongruencija*

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, \ldots,\ x \equiv a_r \pmod{m_r} \tag{2}$$

imati rješenje. Ako znamo jedno rješenje x_0, tada će sva rješenja od (2) biti dana s $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz. Može se vidjeti u [3]. □

Primijenimo sada prethodni teorem na primjeru.

Primjer 18. *Dan je sustav kongruencija*

$$x \equiv 2 \pmod{11}, \qquad x \equiv 2 \pmod{5}, \qquad x \equiv 6 \pmod{7}.$$

Kako su 11,5 i 7 u parovima relativno prosti, prema kineskom teoremu o ostacima imamo da je $m = 11 \cdot 5 \cdot 7$.
Nadalje, imamo $n_1 = \frac{11 \cdot 5 \cdot 7}{11} = 35$, $n_2 = \frac{11 \cdot 5 \cdot 7}{5} = 77$, $n_3 = \frac{11 \cdot 5 \cdot 7}{7} = 55$. Tada će slijediti

$$\begin{aligned} 35x_1 \equiv 2 \pmod{11} &\Leftrightarrow 2x_1 \equiv 2 \pmod{11} \Leftrightarrow x_1 \equiv 1 \pmod{11}, \\ 77x_2 \equiv 2 \pmod{5} &\Leftrightarrow 2x_2 \equiv 2 \pmod{5} \Leftrightarrow x_2 \equiv 1 \pmod{5}, \\ 55x_3 \equiv 6 \pmod{7} &\Leftrightarrow 6x_3 \equiv 6 \pmod{7} \Leftrightarrow x_3 \equiv 1 \pmod{7}. \end{aligned}$$

Uzmemo sada da su $x_1 = 1, x_2 = 1, x_3 = 1$.
Tada će rješenje sustava biti dano s

$$\begin{aligned} x &\equiv 1 \cdot 35 + 1 \cdot 77 + 1 \cdot 55 \ (mod\ 385) \\ x &\equiv 167 \pmod{385}. \end{aligned}$$

Promotrimo u idućem primjeru slučaj u kojem moduli nisu u parovima relativno prosti. Tada nećemo moći direktno primijeniti Kineski teorem o ostacima nego moramo svojstvima kongruencija svesti početni sustav linearnih kongruencija na sustav s relativno prostim modulima.

Primjer 19. *Trebamo riješiti sustav linearnih kongruencija*

$$x \equiv 1 \pmod 8, \qquad x \equiv 5 \pmod{18}, \qquad x \equiv 4 \pmod 5.$$

Rješenje:
Primijetimo kako 8, 18 i 5 nisu u parovima relativno prosti, dakle, ne možemo primijeniti direktno KTO. No, koristeći se svojstvima kongruencija, početni sustav kongruencija ekvivalentan je sljedećem:

$$\begin{aligned} &x \equiv 1 \pmod 2, \qquad x \equiv 5 \pmod 9, \qquad x \equiv 4 \pmod 5, \\ &x \equiv 1 \pmod 4, \qquad x \equiv 5 \pmod 2. \end{aligned}$$

Nadalje, kako vrijedi $x \equiv 1 \pmod 4 \Rightarrow x \equiv 1 \pmod 2$, $x \equiv 5 \pmod 9 \Rightarrow x \equiv 5 \pmod 3$ *i* $x \equiv 5 \pmod 2 \Leftrightarrow x \equiv 1 \pmod 2$, *sustav svodimo na:*

$$x \equiv 1 \pmod 2, \qquad x \equiv 5 \pmod 3, \qquad x \equiv 4 \pmod 5.$$

Moduli 2,9 i 6 su u parovima relativno prosti pa zato možemo primijeniti KTO. Slijedi kako je $m = 2 \cdot 3 \cdot 5 = 30$. *Nadalje,* $n_1 = \frac{2\cdot3\cdot5}{2} = 15$, $n_2 = \frac{2\cdot3\cdot5}{3} = 10$, $n_3 = \frac{2\cdot3\cdot5}{5} = 6$. *Tada će slijediti*

$$\begin{aligned} 15x_1 &\equiv 1 \pmod 2, \qquad 10x_2 \equiv 5 \pmod 3, \qquad 6x_3 \equiv 4 \pmod 5, \\ x_1 &\equiv 1 \pmod 2, \qquad x_2 \equiv 2 \pmod 3, \qquad x_3 \equiv 4 \pmod 5. \end{aligned}$$

Stoga je rješenje dano s $x \equiv 15 \cdot 1 + 10 \cdot 2 + 6 \cdot 4 \equiv 29 \pmod{30}$

3 Primitivni korijeni

U ovome poglavlju definirat ćemo pojam reda cijelog broja a modulo m te pomoću reda definirati pojam primitivnih korijena. Nadalje, iskazat ćemo, dokazati i na primjerima ilustrirati bitna svojstva primitivnih korijena i proučiti bitne rezultate o njihovoj egzistenciji. Kasnije u poglavlju saznat ćemo nešto više o samoj primjeni primitivnih korijena.

3.1 Red i definicija primitivnog korijena

Definicija 9. *Neka je m pozitivan cijeli broj veći od 1 te a cijeli broj takav da je relativno prost s m. Red od a po modulu m, označen s $ord_m(a)$, najmanji je cijeli pozitivni broj d takav da je $a^d \equiv 1 \pmod{m}$. Također, $ord_m(a)$ djelitelj je Eulerove funkcije φ. Također kažemo kako a pripada eksponentu d modulo m.*

Primjer 20. *Kako je $5^6 \equiv 1 \pmod{7}$, slijedit će da 5 pripada eksponentu 6 modulo 7. Odnosno, $ord_7(5) = 6$.*

Primjer 21. *Kako vrijedi $3^6 \equiv 1 \pmod{7}$, slijedi da je $ord_7(3) = 6$.*

U sljedećem teoremu vidjet ćemo neka svojstva reda cijelih brojeva po modulu m.

Teorem 13 (Vidjeti [1, Theorem 6.2.])**.** *Ako je m pozitivan cijeli broj takav da su a i m relativno prosti, tada vrijedi:*

(i) $a^s \equiv 1 \pmod{m}$ *onda i samo onda ako red od a dijeli s. Posebno, red od a dijeli $\varphi(m)$.*

(ii) $a^s \equiv a^t \pmod{m}$ *onda i samo onda ako* $s \equiv t \pmod{ord_m(a)}$.

Dokaz.

(i) Ako vrijedi $s = k \cdot ord_m(a)$, onda je $a^s = (a^{ord_m(a)})^k \equiv 1^k \equiv 1 \pmod{m}$. Obratno, pretpostavimo da je $a^s \equiv 1 \pmod{m}$. Prema Teoremu 1. slijedi $s = q \cdot ord_m(a) + r$, za $0 \leq r < ord_m(a)$, pa je $1 \equiv a^s = (a^{ord_m(a)})^q a^r \equiv a^r \pmod{m}$. Slijedi kako je $r = 0$ s obzirom da je prema definiciji $a^{ord_m(a)}$ najmanja pozitivna potencija od a kongruentno 1 modulo m. Drugi dio tvrdnje (i) slijedi iz Eulerovog teorema.

(ii) Možemo pretpostaviti da je $s \geq t$. Ako je $a^s \equiv a^t \pmod{m}$, onda je $a^s = a^t a^{s-t} \equiv a^s a^{s-t} \pmod{m}$. Kako su $(a^s, m) = 1$ slijedi da je $a^{s-t} \equiv 1 \pmod{m}$. Sada primijenimo dio pod (i). Obrnuto, ako je $s \equiv t \pmod{ord_m(a)}$, pišemo $s = t + k \cdot ord_m(a)$ za neki cijeli broj k. Onda je $a^s = a^t (a^{ord_m(a)})^k \equiv a^t \pmod{m}$.

□

Ilustrirajmo prethodni rezultat na primjeru.

Primjer 22. *Ako je $5^6 \equiv 1 \pmod{7}$, znači da je $ord_7(5) = 6$ pa će onda prema Teoremu 13. i dijelu (i) vrijediti da je $5^{12} \equiv 1 \pmod{7}$ (zato što red od 5 dijeli 12).*

U idućem rezultatu vidjet ćemo još jedno svojstvo reda cijelih brojeva modulo m koje nam govori kako je red produkta jednak produktu redova.

Teorem 14 (Vidjeti [1, Theorem 6.4.]). *Pretpostavimo da su $h = ord_m\ (a)$ i $k = ord_m(b)$. Ako su h i k relativno prosti, tada je $ord_m\ (ab) = hk$. Generalno, postojat će cijeli broj c za koji će njegov red biti najmanji zajednički višekratnik brojeva h i k.*

Dokaz. Može se vidjeti u [1]. □

Navedimo sada i potkrijepimo primjerom definiciju primitivnog korijena modulo n.

Definicija 10. *Ako je red cijelog broja a modulo m jednak $\varphi(m)$, tada a nazivamo primitivni korijen modulo m.*

Primjer 23. *Vidjeli smo kako je $5^6 \equiv 1 \pmod 7$, odnosno kako je $ord_7(5) = 6$. Osim toga, $3^6 \equiv 1 \pmod 7$, pa je također $ord_7(3) = 6$. To znači da su 3 i 5 primitivni korijeni modulo 7.*

3.2 Egzistencija primitivnog korijena

U ovome poglavlju promatrat ćemo egzistenciju primitivnih korijena. Dakle, saznat ćemo koji moduli će imati primitivni korijen te vidjet ćemo koliko postoji primitivnih korijena modulo p za neki prost broj p.

Teorem 15 (Vidjeti [3, Teorem 3.19.]). *Za prost broj p postojat će točno $\varphi(p-1)$ primitivnih korijena modulo p.*

Dokaz. Može se vidjeti u [3]. □

Primjer 24. *Uzmimo prost broj 17. Znači da će postojati $\varphi(17-1) = \varphi(16) = 8$ primitivnih korijena modulo 17, a to su brojevi 3,5,6,7,10,11,12 i 14.*

Sljedeći teorem reći će nam koji brojevi će formirati reducirani sustav ostataka modulo p za neki primitivni korijen modulo p.

Teorem 16 (Vidjeti [7, Theorem 11.]). *Ako je g primitivni korijen modulo p, onda brojevi $g, g^2, \ldots, g^{p-1}$ formiraju reducirani sustav ostataka modulo p.*

Primjer 25. *Kako je 3 primitivni korijen modulo 7, tada će skup $\{3, 3^2, 3^3, \ldots, 3^6\}$ formirati reducirani sustav ostataka modulo 7.*

U idućem rezultatu vidjet ćemo kada će za pozitivan cijeli broj n postojati primitivni korijen modulo n.

Teorem 17 (Vidjeti [3, Teorem 3.21.]). *Za pozitivan cijeli broj n postojat će primitivni korijen modulo n onda i samo onda ako je n jednak $2, 4, p^j$ ili $2p^j$, za neparni prost broj p.*

Dokaz. Znamo da je 1 primitivni korijen modulo 2, a 3 je primitivni korijen modulo 4. Uzmimo da je g primitivni korijen modulo p^j. Između brojeva g i $g+p^j$ odabrat ćemo onaj koji nije paran i on će biti primitivni korijen modulo p^j zato što vrijedi da je $\varphi(2p^j) = \varphi(p^j)$. Pokažimo sada drugi smjer. Uzmimo da je $n = 2^j$, za $j \geq 3$. Onda će za neparan broj a vrijediti $a^2 \equiv 1 \pmod 8$. Kako vrijedi da 8 dijeli $a^2 - 1$ i da 2 dijeli $a^2 + 1$ imat ćemo da je $a^4 \equiv 1 \pmod 1)6$. Ponavljajući taj postupak imat ćemo da je $(a^2)^{j-2} \equiv 1 \pmod{2^j}$, za $j \geq 3$. Kako je $\varphi(2^j) = 2^{j-1}$, pokazali smo kako nema primitivnih korijena modulo 2^j, za $j \geq 3$.
Nadalje, uzmimo n takav da je $n = n_1 n_2$, gdje su n_1 i n_2 relativno prosti i oba strogo veća od 2. Brojevi $\varphi(n_1)$ i $\varphi(n_2)$ će biti parni, pa ćemo za broj a koji je relativno prost s n imati:

$$\begin{aligned} a^{\frac{1}{2}\varphi(n)} &\equiv (a^{\varphi(n_1)})^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1}, \\ a^{\frac{1}{2}\varphi(n)} &\equiv (a^{\varphi(n_2)})^{\frac{1}{2}\varphi(n_1)} \equiv 1 \pmod{n_2}. \end{aligned}$$

Stoga je $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod n$, pa ne postoje primitivni korijeni modulo n. □

Primjer 26. *Uzmimo npr. prirodne brojeve 10 i 15. Za njih će postojati primitivni korijen modulo 10 i modulo 15 onda i samo onda ako su oblika* $2, 4, p^j$ *ili* $2p^j$*, za* p *neparan prost broj. Broj 10 možemo zapisati kao* $10 = 2 \cdot 5^1$ *pa za broj 10 postoji primitivni korijen modulo 10 jer smo ga uspjeli zapisati kao produkt dvojke i neparnog prostog broja. Nadalje, broj 15 ne možemo zapisati ni u jednom od oblika, što znači da 15 nema primitivnih korijena modulo 15.*

Pogledajmo sada rezultat u kojem sada imamo modul po pozitivnom cijelom broju koji nije potencija broja 2.

Teorem 18 (Vidjeti [6, Theorem 3.5.])**.** *Ako je* m *pozitivan cijeli broj takav da nije potencija broja 2 i ako* m *ima primitivni korijen, tada je* $m = pk$ *ili* $2pk$*, za* p *neparan prost broj i* k *prirodan broj.*

Dokaz. Može se vidjeti u [6]. □

Pogledajmo sada kako prethodni teorem izgleda na primjeru.

Primjer 27. *Uzmimo pozitivan cijeli broj 18. Dakle, da bi broj 18 imao primitivni korijen modulo 18, mora biti produkt neparnog prostog broja* p *i pozitivnog cijelog broja* k*. Primijetimo kako 18 možemo upravo zapisati kao produkt takvih brojeva* $18 = 3 \cdot 6$*. Dakle, broj 18 će imati primitivni korijen modulo 18.*

Pogledajmo još jedno bitno svojstvo egzistencije primitivnih korijena.

Teorem 19 (Vidjeti [6, Theorem 3.8.])**.** *Postoji primitivni korijen modulo* $m = 2k$ *onda i samo onda ako je* m *jednak* 2 *ili* 4*.*

Dokaz. Treba dokazati da ako je $k \geq 3$, onda nema primitivnih korijena modulo 2^k. Kako je $\varphi(2^k) = 2^{k-1}$, treba dokazati kako je $a^{2^{k-2}} \equiv 1 \pmod{2^k}$, gdje je a neparan broj i $k \geq 3$.

To se pokaže indukcijom po $k \geq 3$. Za $k = 3$ imamo kongruenciju $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. Nadalje, neka je $k \geq 3$ i neka vrijedi $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Slijedi da je $a^{2^{k-2}} - 1$ djeljivo s 2^k. S obzirom na to da je broj a neparan, onda je $a^{2^{k-2}} + 1$ paran. Tada slijedi da je $a^{2^{k-1}} - 1 = (a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1)$ djeljivo s 2^{k+1} pa je $a^{2^{k-1}} \equiv 1 \ (mod\ 2^{k+1})$. □

Korolar 1 (Vidjeti [7, Corollary 12.1.]). *Ako je $m = 2^\alpha$ ($\alpha \geq 3$) ili $m = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, gdje su $\alpha \geq 2$ ili $k \geq 2$, onda nema primitivnih korijena modulo m.*

Teorem 20 (Vidjeti [7, Lemma 2.]). *Za neparan prost broj p postoji neparan cijeli broj koji je primitivni korijen modulo p i modulo p^2.*

Dokaz. Može se vidjeti u [7]. □

Primjer 28. *Uzmimo prost broj 5. Prema prethodnom teoremu znači da postoji neparan cijeli broj koji će biti primitivni korijen modulo p i modulo p^2. Primitivni korijeni modulo 5 su brojevi 2 i 3, dakle 3 je neparan cijeli broj koji je primitivni korijen modulo 5. Kako su brojevi 2,3,8,12,13,17,22 i 23 primitivni korijeni modulo 25, značit će da za neparan prost broj 5, 3 će biti primitivni korijen modulo 5 i modulo 25.*

Pogledajmo sada rezultat koji vrijedi za svaki prirodan broj k.

Teorem 21 (Vidjeti [6, Theorem 3.9.]). *Za svaki prirodan broj k vrijedi*

$$5^{2^k} \equiv 1 + 3 \cdot 2^{k+2} \pmod{2^{k+4}}.$$

Dokaz. Dokaz ide indukcijom po k. Za $k = 1$ imamo

$$5^{2^1} = 25 \equiv 1 + 3 \cdot 2^3 \pmod{2^5}.$$

Slično, za $k = 2$ imamo

$$5^{2^2} = 625 = 1 + 48 + 576 \equiv 1 + 3 \cdot 2^4 \pmod{2^6}.$$

Ako teorem vrijedi za $k \geq 1$, onda postoji cijeli broj u takav da

$$5^{2^k} = 1 + 3 \cdot 2^{k+2} + 2^{k+4}u = 1 + 2^{k+2}(3 + 4u).$$

Budući da je $2k + 4 \geq k + 5$, imamo

$$\begin{aligned} 5^{2^{k+1}} &= (5^{2^k})^2 \\ &= (1 + 2^{k+2}(3 + 4u))^2 \\ &\equiv 1 + 2^{k+3}(3 + 4u) \pmod{2^{2k+4}} \\ &\equiv 1 + 3 \cdot 2^{k+3} \pmod{2^{k+5}}. \end{aligned}$$

□

Idući teorem daje nam vrlo važno svojstvo primitivnih korijena prostih brojeva.

Teorem 22 (vidjeti [2, Theorem 7-6]). *Za svaki prost broj p postoje primitivni korijeni modulo p.*

Dokaz. Može se vidjeti u [2]. □

Primjer 29. *Uzmimo na primjer proste brojeve 13, 23, 17, 19.*
Primitivni korijeni modulo 13 su: 2,6,7 i 11.
Primitivni korijeni modulo 17 su: 3,5,6,7,10,11,12 i 14.
Primitivni korijeni modulo 19 su: 2,3,10,13,14 i 15.
Primitivni korijeni modulo 23 su: 5,7,10,11,14,15,17,19,20 i 21.

Pogledajmo još jedno svojstvo primitivnih korijena koristeći Eulerovu funkciju.

Teorem 23 (vidjeti [1, Theorem 6.12]). *Neka je g primitivni korijen modulo m. Broj g^k bit će primitivni korijen modulo m onda i samo onda ako su k i $\varphi(m)$ relativno prosti.*

Dokaz. Kako je $ord_m(g) = \varphi(m)$ slijedi da je $ord_m(g^k) = \frac{\varphi(m)}{(k,\varphi(m))}$. Odnosno, g^k će biti primitivni korijen modulo m, takav da je $ord_m(g^k) = \varphi(m)$ onda i samo onda ako su k i $\varphi(m)$ relativno prosti. □

Ilustrirajmo to sada na primjeru.

Primjer 30. *U prethodnom primjeru vidjeli smo kako je 3 primitivni korijen modulo 17. Kako je $\varphi(17) = 16$, iz Teorema 20. slijedi kako su svi primitivni korijeni od 17 dani pomoću 3^k, za neki $1 \leq k \leq 16$ takav da je $(k, 16) = 1$. Tada ima $\varphi(16) = 8$ takvih k-ova: 1,3,5,7,9,11,13 i 15.*

Sljedeći rezultat reći će nam nešto više o egzistenciji nekongruentnih primitivnih korijena.

Teorem 24 (vidjeti [1, Theorem 6.13]). *Neka postoji primitivni korijen modulo m. Onda ima $\varphi(\varphi(m))$ nekongruentnih primitivnih korijena modulo m.*

Dokaz. Neka je g primitivni korijen modulo m. Tada će h biti primitivni korijen modulo m onda i samo onda ako je $h \equiv g^k \pmod{m}$, za neki $k \leq \varphi(m)$ gdje su k i $\varphi(m)$ relativno prosti. Očito takvih k-ova ima $\varphi(\varphi(m))$ pa slijedi rezultat. □

Primijenimo prethodni teorem na primjeru.

Primjer 31. *Uzmimo prost broj 19. Znamo da onda ima $\varphi(\varphi(19)) = \varphi(18) = 6$ nekongruentnih primitivnih korijena modulo 19. Za svaki k koji je $1 \leq k \leq 18$ imamo da je $(k, 19) = 1$. Tražimo onakve $k^i \pmod{19}$ za sve $i > 0$ takve da i dijeli 18, a to su $\{1, 2, 3, 6, 9, 18\}$. Iz Malog Fermatovog teorema znamo kako je $k^{18} \equiv 1 \pmod{19}$, tako da su primitivni korijeni modulo 19 one vrijednosti k-ova takve da je $k^i \not\equiv 1 \pmod{19}$ za sve $i \in \{1, 2, 3, 6, 9\}$. Stajemo kada nađemo tih 6 vrijednosti za k; to vrijedi za $\{2, 3, 10, 13, 14, 15\}$.*

Definicija 11. *Za p prost broj, g primitivni korijen modulo p i a cijeli broj koji nije djeljiv s p postoji jedinstveni cijeli broj k takav da je $g^k \equiv a \pmod{p}$ i $k \in \{0, 1, \ldots, p-2\}$. Cijeli broj k naziva se indeks (ili diskretni logaritam) od a s obzirom na primitivni korijen g i pišemo $k = ind_g(a)$ ili $k = ind\ a$.*

Primijenimo prethodnu definiciju na primjeru.

Primjer 32. *Neka je $p = 13$ i 7 primitivni korijen modulo 13.*

$$7^1 \equiv 7 \pmod{13}, \quad 7^2 \equiv 10 \pmod{13}, \quad 7^3 \equiv 5 \pmod{13}, \quad 7^4 \equiv 9 \pmod{13},$$
$$7^5 \equiv 11 \pmod{13}, \quad 7^6 \equiv 12 \pmod{13}, \quad 7^7 \equiv 6 \pmod{13}, \quad 7^8 \equiv 3 \pmod{13},$$
$$7^9 \equiv 8 \pmod{13}, \quad 7^{10} \equiv 4 \pmod{13}, \quad 7^{11} \equiv 2 \pmod{13}, \quad 7^{12} \equiv 1 \pmod{13}.$$

Možemo primijetiti kako s obzirom primitivni korijen 7 modulo 13, imamo najviše $p-1 = 12$ različitih indeksa od broja a.

Napomena 2. *Ako su k_1 i k_2 cijeli brojevi takvi da je $k_1 \leq k_2$ i $a \equiv g^{k_1} \equiv g^{k_2} \pmod{p}$, imamo $g^{k_2-k_1} \equiv 1 \pmod{p}$ i $k_1 \equiv k_2 \pmod{p-1}$. Za $a \equiv g^k \pmod{p}$ i $b \equiv g^l \pmod{p}$, slijedi da je $ab \equiv g^k g^l = g^{k+l} \pmod{p}$ i $ind_g(ab) \equiv k + l \equiv ind_g(a) + ind_g(b) \pmod{p-1}$.*

U idućem teoremu vidjet ćemo svojstvo indeksa od a s obzirom na primitivni korijen g modulo p, ako su a i p relativno prosti.

Teorem 25 (Vidjeti [7, Lemma])**.** *Za prost broj p, g primitivni korijen modulo p i cijeli broj a takav da su a i p relativno prosti, slijedi da je $g^t \equiv a \pmod{p}$ onda i samo onda ako je $t \equiv ind_g(a) \pmod{p-1}$.*

Primjer 33.

Dokaz. Ako je $t \equiv ind_g(a) \pmod{p-1}$, možemo pisati $t = ind_g(a) + m \cdot (p-1)$. Odnosno,

$$g^t \equiv g^{ind_g(a)+m(p-1)} \equiv g^{ind_g(a)}(g^{p-1})^m \equiv g^{ind_g(a)} \equiv a \pmod{p}.$$

S druge strane, ako je $g^t \equiv a \equiv g^{ind_g(a)} \pmod{p}$, onda

$$g^{|t-ind_g(a)|} \equiv 1 \pmod{p}.$$

Kako g pripada eksponentu $p-1 \pmod{p}$, onda je

$$t \equiv ind_g(a) \pmod{p-1}.$$

□

Primjer 34. *Uzmimo prost broj 17 i njegov primitivni korijen 12 modulo 17. Prema definiciji indeksa znamo:*

$$12^1 \equiv 12 \pmod{17}, \quad 12^2 \equiv 8 \pmod{17}, \quad 12^3 \equiv 11 \pmod{17}, \quad 12^4 \equiv 13 \pmod{17},$$
$$12^5 \equiv 3 \pmod{17}, \quad 12^6 \equiv 2 \pmod{17}, \quad 12^7 \equiv 7 \pmod{17}, \quad 12^8 \equiv 16 \pmod{17},$$
$$12^9 \equiv 5 \pmod{17}, \quad 12^{10} \equiv 9 \pmod{17}, \quad 12^{11} \equiv 6 \pmod{17}, \quad 12^{12} \equiv 4 \pmod{17},$$
$$12^{13} \equiv 14 \pmod{17}, \quad 12^{14} \equiv 15 \pmod{17}, \quad 12^{15} \equiv 10 \pmod{17}, \quad 12^{16} \equiv 1 \pmod{17}.$$

Nadalje, vrijednosti broja a će biti oni brojevi koji su relativno prosti sa 17. Da bi vrijedilo da je $12^t \equiv a \pmod{17}$, za $t = 1, 2, \ldots 16$ i $a \in \{1, 2, 3, \ldots, 16\}$, mora vrijediti da je $t \equiv ind_{12}(a) \pmod{16}$. Uzmimo da je npr. $t = 12$. Znači da će $12^{12} \equiv 4 \pmod{17}$ ako i samo ako je $12 \equiv 12 \pmod{16}$. Jer je $12 \equiv 12 \pmod{16}$, vrijedi da je $12^{12} \equiv 4 \pmod{17}$ i obratno.

Korolar 2 (Vidjeti [7, Corollary 15.1.]). *Cijeli broj a je primitivni korijen modulo p onda i samo onda ako vrijedi*

$$(\varphi(p), ind\ a) = 1.$$

Primjer 35. *Uzmimo prost broj 13. Primitivni korijeni modulo 13 su: 2,6,7 i 11. Također, znamo da za primitivni korijen 2 modulo 13 vrijedi:*

$$\begin{aligned}
&2^1 \equiv 2 \pmod{13}, \quad 2^2 \equiv 4 \pmod{13}, \quad 2^3 \equiv 8 \pmod{13}, \quad 2^4 \equiv 3 \pmod{13},\\
&2^5 \equiv 6 \pmod{13}, \quad 2^6 \equiv 12 \pmod{13}, \quad 2^7 \equiv 11 \pmod{13}, \quad 2^8 \equiv 9 \pmod{13},\\
&2^9 \equiv 5 \pmod{13}, \quad 2^{10} \equiv 10 \pmod{13}, \quad 2^{11} \equiv 7 \pmod{13}, \quad 2^{12} \equiv 1 \pmod{13}.
\end{aligned}$$

Dakle, koristeći prethodni korolar, cijeli broj a će biti primitivni korijen modulo 13 ako će vrijediti $(\varphi(13), ind_2 a) = (12, ind_2 a) = 1$. *Na primjer, uzmimo da je* $a = 11$. *Broj 11 će biti primitivni korijen modulo 13 ako i samo ako vrijedi da* $(12, \underbrace{ind_2 11}_{=7}) = 1$, *a to očito vrijedi pa je 11 primitivni korijen modulo 13. Analogno vrijedi kada je* $a \in \{2, 6, 7, 11\}$.

U sljedećem teoremu vidjet ćemo još neka bitna svojstva indeksa.

Teorem 26 (Vidjeti [3, Teorem 3.22.]). *Vrijedi:*

1) $ind_g\ a + ind\ b \equiv ind_g\ (ab) \pmod{\varphi(n)}$;

2) $ind_g\ 1 = 0, ind_g\ g = 1$;

3) $ind_g(a^m) \equiv m \cdot ind_g \pmod{\varphi(n)}$ *za* $m \in \mathbb{N}$;

4) $ind_g(-1) = \frac{1}{2}\varphi(n)$ *za* $n \geq 3$.

Dokaz. Prva tri svojstva slijede iz definicije indeksa te svojstva potenciranja i množenja potencija. Dokaz svojstva 4) slijedi iz:

$$g^{2 \cdot ind_g(-1)} \equiv (-1)^2 \equiv 1 \pmod{n} \quad \text{i} \quad 2 \cdot ind_g(-1) < 2\varphi(n)$$

□

Ilustrirajmo prethodna svojstva na primjeru.

Primjer 36. *Treba naći ostatak pri dijeljenju* $2^{28} \cdot 6^{17}$ *brojem 19.*
Rješenje:
Imamo kongruenciju

$$x \equiv 2^{28} \cdot 6^{17} \pmod{13}.$$

Uzet ćemo indekse s obzirom na primitivni korijen 2 modulo 19:

$$\begin{aligned}
ind_2(x) &\equiv 28 \cdot ind_2(2) + 17 \cdot ind_2(6) \pmod{12}\\
&\equiv 28 \cdot 1 + 17 \cdot 5 \pmod{12}\\
&\equiv 5 \pmod{12}.
\end{aligned}$$

Iz toga slijedi kako je $x \equiv 2^5 \equiv 6 \pmod{13}$.

Iduća propozicija reći će nam nešto više o jedinstvenosti rješenja kongruencije $x^n \equiv a \pmod{p}$.

Propozicija 5 (Vidjeti [3, Teorem 3.23.]). *Neka je* $nzd(n, p-1) = 1$. *Tada će kongruencija* $x^n \equiv a \pmod{p}$ *imati jedinstveno rješenje.*

Dokaz. Iz kongruencije $x^n \equiv a \pmod{p}$ prema svojstvu 3) iz prethodnog teorema slijedi $n\ ind\ x \equiv ind\ a \pmod{p-1}$, a kako su n i $p-1$ relativno prosti, slijedi da kongruencija ima jedinstveno rješenje. □

Primjer 37. *Ispitajmo ima li kongruencija* $17x^8 \equiv 9 \pmod{23}$ *rješenja?*
Rješenje:
S obzirom na primitivni korijen 5 modulo 23 imamo da je

$$8\ ind_5(x) \equiv ind_5(9) - ind_5(17) \equiv 10 - 7 \equiv 3 \pmod{22}.$$

Kako $nzd(8, 22) = 2$ *ne dijeli 3, znači da ova kongruencija nema rješenja.*

4 Neke primjene primitivnih korijena

U ovome poglavlju pokazat ćemo kako primitivne korijene i indekse možemo lako primijeniti na nekim problemima kao što su Artinova hipoteza i Shanksov algoritam, ali vidjet ćemo i jednu njihovu zanimljivu primjenu na matematičkom problemu u kontekstu kriptografije pod nazivom Diffie-Hellmanov problem.

4.1 Artinova hipoteza

Artinovu hipoteza govori da za prirodni broj a, koji nije potencija pozitivnog cijelog broja, vrijedit će $\nu_a(N) \sim A \cdot \pi(N)$.

- $\pi(N)$ - broj onih prostih brojeva koji su manji ili jednaki N.
- $\nu_a(N)$ - broji broj prostih brojeva koji su manji ili jednaki N, ali za koje će a biti primitivni korijen modulo p.
- A - Artinova konstanta

Artinova je konstanta dana sljedećom formulom:

$$A = \prod_{p\ prost} (1 - \frac{1}{p(p-1)}) \approx 0.3739558.$$

Primjer 38. *Uzmimo da je $a = 3$ modulo p. Prema Artinovoj hipotezi skup svih prostih brojeva p za koje je 3 primitivni korijen modulo p je jednak:*
$S(3) = \{5, 7, 17, 19, 29, 31, 43, 53, 79, 89, 101, 113, 127, 137, 139, 149, 163, 173, 197, 199, 211,$
$223, 233, 257, 269, 281, 283, 293, 317, 331, 353, 379, 389, 401, 449, 461, 463, 487\}$
Ukupno ima 38 prostih brojeva p manjih od 500 za koje je 3 primitivni korijen modulo p, a kako ima 95 prostih brojeva koji su manji od 500, tada omjer koji će težiti Artinovoj konstanti iznosi $\frac{38}{95} = 0.4$.

4.2 Diffie-Hellmanov problem

Definicija 12. *Ako je $(G, *)$ konačna grupa i $H = \{g^i : i \geq 0\}$ njezina podgrupa koja je generirana elementom $g \in G$, potrebno je naći najmanji cijeli broj x koji je veći ili jednak nuli takav da je $h = g^x$, za $h \in H$, gdje je $g^x = \underbrace{g * g * \cdots * g}_{x\ puta}$. Takav broj x zovemo diskretni logaritam i pišemo $log_g h$.*

Diffie – Hellmanov problem (DHP) je matematički problem koji su prvi put predložili Whitfield Diffie i Martin Hellman u kontekstu kriptografije. Motivacija ovog problema je u tome što mnogi sigurnosni sustavi koriste jednosmjerne funkcije: matematičke operacije koje se brzo izračunavaju, ali ih je teško preokrenuti. Na primjer, omogućuju šifriranje poruke, ali je dešifriranje teško. Da je rješavanje DHP -a jednostavno, ti bi se sustavi lako razbili.
Diffie -Hellmanov problem neformalno se navodi na sljedeći način:

S obzirom na element g i vrijednosti g^x i g^y, kolika je vrijednost g^{xy}? Formalno, g je generator neke skupine, a x i y su nasumično odabrani cijeli brojevi.

Diffie-Hellmanov protokol

Naslutimo da se dvije osobe X i Y žele dogovoriti o jednom elementu u cikličkoj grupi G koji će biti tajan. One će morati provesti taj razgovor preko nekog komunikacijskog kanala koji neće biti siguran, uz uvjet da prethodno nisu razmjenjivali nikakve informacije. Jedina informacija koju ove osobe imaju su javno dostupna informacija o grupi G i o njezinu generatoru g. Najprije se odaberu prost broj p i njegov primitivni korijen g modulo p.

1) Osoba X će generirati slučajni prirodni broj $x \in \{1, 2, \ldots, p-1\}$, dok će osobi Y poslati element $g^x \pmod{p}$.

2) Osoba Y će generirati slučajni prirodni broj $y \in \{1, 2, \ldots, p-1\}$, dok će osobi X poslati element $g^y \pmod{p}$.

3) Osoba X treba izračunati $(g^y)^x = g^{xy} \pmod{p}$.

4) Osoba Y treba izračunati $(g^x)^y = g^{xy} \pmod{p}$.

Njihov je tajni ključ jednak $A = g^{xy} \pmod{p}$.
Ako postoji treća osoba, recimo osoba Z, koja želi prisluškivati komunikaciju osoba X i Y, ona će znati činjenicu da je G grupa generirana elementom g i poznavat će vrijednosti g^x i g^y. Cilj osobe Z bit će izračunati g^{xy}, odnosno osoba Z morat će riješiti Diffie-Hellmanov problem (DHP). Ako će osoba Z znati riješiti problem diskretnog logaritma (PDL), odnosno ako će iz poznavanja g i g^a moći izračunati x, onda će lako iz poznavanja x i g^y znati izračunati g^{xy}.
Mnogi vjeruju kako su Diffie–Hellmanov problem i PDL ekvivalentni. Ilustrirajmo sada Diffie-Hellmanov protokol na primjeru.

Primjer 39. *Osobe X i Y dogovore se da će uzeti prost broj $p = 11$ i njegov primitivni korijen 2 modulo 11.*

- *Osoba X uzela je slučajan prirodan broj 6 i osobi Y poslala broj* $2^6 \pmod{11}$.
- *Osoba Y generira slučajan prirodan broj 8 i osobi X šalje broj* $2^8 \pmod{11}$.
- *Osoba X računa* $(2^8)^6 = 2^{8 \cdot 6} \pmod{11}$.
- *Osoba Y računa* $(2^6)^8 = 2^{6 \cdot 8} \pmod{11}$.

Osobe X i Y dobiju isti rezultat pa je njihov tajni ključ jednak $2^{8 \cdot 6} \pmod{11} = 3$.

4.3 Shanksov algoritam

Shanksov algoritam kaže da ako će za konačnu cikličku grupu G generiranu elementom g, reda n i za neki $a \in G$ vrijediti $x = log_g a$, onda će se x moći i to na jedinstven način napisati kao $x = im + j$, za $0 \leq i, j < m$, gdje je $m = \lceil \sqrt{d} \rceil$. Prema tome, vrijedi $g^x = g^{im} g^j$, a to implicira $a(g^{-m})^i = g^j$. Nadalje, kako prolazimo vrijednostima i i j, za $0 \leq i, j < m$, zanimaju nas oni koji će zadovoljavati $a(g^{-m})^i = g^j$. Time dobivamo i vrijednost x, a on je diskretni logaritam koji smo i tražili. **Algoritam za izračunavanje PDL u grupi $\mathbb{Z}_p^*$.**

- Najprije saznamo vrijednost $m = \lceil \sqrt{p-1} \rceil$
- Izračunamo mali korak i nakon toga ćemo formirati tablicu T_1 uređenih parova $(j,\ g^j \pmod p)$, za $(0 \leq j < m)$.
- Računamo veliki korak i formiramo tablicu T_2 uređenih parova $(i,\ a(g^{-m})^i \pmod p)$, za $(0 \leq i < m)$.
- Sada tražimo one uređene parove $(j, y) \in L_1$ i $(i, y) \in L_2$ koji se podudaraju u drugoj koordinati i zatim izračunamo $x = log_g a = im + j$.

Primjer 40. *Odaberemo primitivni korijen 2 modulo 13 i izračunamo* $m = \lceil \sqrt{12} \rceil = 4$ *i neka je* $a = 11$.
Najprije računamo mali korak i formiramo tablicu uređenih parova $(j,\ g^j \pmod p)$, $(0 \leq j < m)$.

j	0	1	2	3
$2^j \pmod{13}$	1	2	4	8

.

Također je $2^4 \equiv 3 \pmod{13}$ *i 9 je inverz od 3 modulo 13, tj.* $2^4 \cdot 9 \equiv 1 \pmod{13}$. *Zatim, računamo veliki korak i formiramo tablicu uređenih parova* $(i,\ a(g^{-m})^i \pmod p)$, $(0 \leq i < m)$.

i	0	1	2	3
$11 \cdot 9^i \pmod{13}$	11	8	7	5

.

Vidimo da je broj 8 prvi koji se pojavio u obje liste, pa je tada:

$$11 \cdot 9^1 \equiv 8^1 \pmod{13}$$
$$11 \equiv 2^3 \cdot 2^4 \equiv 2^7 \pmod{13}.$$

Dakle, indeks od a=11 s obzirom na primitivni korijen 2 modulo 13 jednak je 7.

Literatura

[1] A. Adler, J. E. Coury, *The theory of numbers: a Text and Source Book of Problems*, The University of British Columbia, 1995.

[2] G. E. Andrews, *Number Theory*, W.B. Saunders Company, 1971.

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

[4] A. Dujella, *Diffie-Hellmanov protokol za razmjenu ključeva*, Sveučilište u Zagrebu, dostupno na https://web.math.pmf.unizg.hr/ duje/ecc/dlp.

[5] B. Ibrahimpašić, D. Kovačević, *Diskretni logaritam*, MAT-KOL (Banja Luka), Vol. XVII (2)(2011).

[6] M. B. Nathanson, *Elementary Methods in Number Theory*, Department of Mathematics, 2000.

[7] J. E. Shockley, *Introduction to number theory*, Virginia Polytechnic Institute, 1967.