Primitivni korijeni

Rezo, Ana

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
Financijska matematika i statistika

Ana Rezo

Primitivni korijeni

Diplomski rad

Osijek, 2023.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
Financijska matematika i statistika

Ana Rezo

Primitivni korijeni

Diplomski rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2023.

Sadržaj

Uvod

Glavna tema ovog diplomskog rada su primitivni korijeni. Da bismo definirali primitivne korijene, u prvom ćemo poglavlju uvesti neke osnovne definicije i teoreme koji su nam potrebni kao što su reducirani sustav ostataka modulo n, red broja modulo n, Eulerov teorem, Mali Fermatov teorem.
Na početku drugog poglavlja uvest ćemo traženu definiciju primitivnih korijena te osnovne tvrdnje vezane za primitivne korijene poput broj primitivnih korijena modulo n u reduciranom sustavu ostataka. Navest ćemo i osnovne primjere za važne tvrdnje.
U prvom potpoglavlju drugog poglavlja bavimo se primitivnim korijenima prostih brojeva. Ovdje ćemo navesti Lagrangeov teorem koji nam kaže koliko najviše rješenja ima kongruencija oblika $f(x) \equiv 0 \pmod{p}$ ako su prethodno zadovoljene pretpostavke teorema. Teorem ćemo potkrijepiti primjerom. Navest ćemo još nekoliko tvrdnji vezanih za primitivne korijene prostih brojeva.
U sljedećem potpoglavlju bavit ćemo se egzistencijom primitivnih korijena. Tražit ćemo sve prirodne brojeve za koje postoje primitivni korijeni. Neke od tvrdnji potkrijepit ćemo i primjerom.
U sljedećem poglavlju razmotrit ćemo u kojim sve slučajevima možemo primijeniti primitivne korijene. U prvom potpoglavlju ovog poglavlja uvest ćemo definiciju i važan teorem vezan za indeks prirodnog broja u odnosu na primitivni korijen modulo n. Sljedeće ćemo uz pomoć indeksa riješiti neke polinomijalne i eksponencijalne kongruencije. Nadalje ćemo se upoznati s nekim testovima prostosti (kao što je Lucasov test prostosti), a to su algoritmi s kojima možemo provjeriti je li dani broj prost.
U posljednjem poglavlju ovoga rada bavimo se univerzalim eksponentima. Upoznat ćemo se i s najmanjim univerzalnim eksponentima prirodnih brojeva te ćemo navesti i važnu tvrdnju vezanu za minimalne univerzalne eksponente. Na kraju ćemo se još upoznati s Carmichaelovim brojevima. Naći ćemo najmanji Carmichaelov broj te dokazati neke važne teoreme vezane uz spomenute brojeve.

1 Red broja modulo n

U ovom ćemo poglavlju navesti neke važne teoreme i definicije koji će nam trebati u daljnjem dijelu rada. Za početak ćemo uvesti definicije potpunog i reduciranog sustava ostataka moduo n i navesti primjer.

Definicija 1. *Neka je $n \in \mathbb{N}$. Skup $S = \{x_1, x_2, \ldots, x_n\}$ nazivamo potpun sustav ostataka modulo n ako*

$$\forall y \in \mathbb{Z}, \exists!\ x_i \in S : y \equiv x_i \pmod{n}.$$

Drugim riječima, potpun sustav ostataka modulo n dobivamo tako da iz svake klase ekvivalencije modulo n uzmemo po jedan član. Jasno je kako postoji beskonačno mnoogo potpunih sustava ostataka modulo n.

Definicija 2. *Reducirani sustav ostataka modulo n je skup $S = \{a_1, a_2, ..., a_k\}$ sa svojstvom:*

$$\forall b \in \mathbb{Z}, (b, n) = 1, \exists!\ a_i \in S : b \equiv a_i \pmod{n}.$$

Dakle, iz potpunog sustava ostataka modulo n izbacimo one elemente koji nisu relativno prosti s n. Primjer jednog reduciranog sustava ostataka modulo n je skup svih $b \in \{1, 2, ..., n\}$ za koje vrijedi da su relativno prosti s brojem n.

Primjer 1. *Neka je $n = 5$. Jedan potpun sustav ostataka modulo 5 je $\{1, 2, 3, 4, 5\}$. Reducirani sustav ostataka modulo 5 je $\{1, 2, 3, 4\}$.*

Za sve reducirane sustave ostataka modulo n vrijedi da imaju isti broj elemenata kojeg označavamo s $\varphi(n)$. Tako definiranu fukncju $\varphi : \mathbb{N} \to \mathbb{N}$ nazivamo *Eulerova funkcija*. Stoga, možemo reći kako $\varphi(n)$ predstavlja broj brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n.
Prema tome, ako je

$$U_n = \{a \in \mathbb{N} : 1 \leq a \leq n, (a, n) = 1\},$$

tada funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ definiranu s

$$\varphi(n) = \#U_n$$

zovemo Eulerova funkcija.

Iz definicije vidimo kako vrijedi sljedeće:

- $\varphi(n) \leq n - 1, \forall n > 1$,
- $\varphi(1) = 1$,
- ako je $(m, n) = 1$, tada je $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$,
- ako je p prost, tada za Eulerovu funkciju vrijedi $\varphi(p) = p - 1$.

Teorem 1. *Neka skup* $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ *čini reducirani sustav ostataka modulo* n *i neka je* $(b, n) = 1$. *Tada je i skup* $S = \{bb_1, bb_2, \ldots, bb_{\varphi(n)}\}$ *također reducirani sustav ostataka modulo* n.

Uočimo kako prethodni teorem vrijedi i kad imamo potpun sustav ostataka modulo n.

Propozicija 1. *Ako je* p *prost broj i* k *neki prirodan broj, onda je*

$$\varphi(p^k) = p^k - p^{(k-1)} = p^{(k-1)}(p-1).$$

Dokaz. Kako bismo dokazali ovu propoziciju, potrebno je pronaći broj svih elemenata u reduciranom sustavu ostataka modulo p^k, odnosno broj brojeva u skupu $S = \{1, 2, \ldots, p^k\}$ za koje vrijedi da su relativno prosti s p^k. Vrijedi:

$$a \in \mathbb{Z}, (a, p^k) = 1 \iff (a, p) = 1.$$

Dakle, iz skupa S treba isključiti sve višekratnike broja p, odnosno brojeve $m \cdot p$ sa svojstvom:

$$p \leq m \cdot p \leq p^k \Rightarrow 1 \leq m \leq p^{(k-1)}.$$

Dakle, imamo $p^{(k-1)}$ izbora za m pa je $\varphi(p^k) = p^k - p^{(k-1)} = p^{(k-1)}(p-1)$ □

Sljedeći teorem koji navodimo posljedica je multiplikativnosti Eulerove funkcije.

Teorem 2. *Ako je* $n \in \mathbb{N}$ *oblika* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, *pri čemu su* $p_1, \ldots, p_k$ *prosti brojevi, onda je* $\varphi(n) = n \cdot \prod_i^k \left(1 - \frac{1}{p_i}\right)$.

Posljedica prethodnog teorema je sljedeći korolar.

Korolar 1. *Ako je* $n = \prod_i^k {p_i}^{\alpha_{p_i}}$, *tada je* $\varphi(n) = \prod_i^k {p_i}^{\alpha_{p_i}-1}(p_i - 1)$.

Navest ćemo sada jedan primjer u kojem se vidi primjena prethodnog korolara.

Primjer 2. $\varphi(1000) = \varphi(10 \cdot 100) = \varphi(5 \cdot 2 \cdot 2^2 \cdot 5^2) = \varphi(2^3 \cdot 5^3) = 2^2 \cdot (2-1) \cdot 5^2 \cdot (5-1) = 400.$

Teorem 3 (Eulerov teorem)**.** *Ako je* $b \in \mathbb{Z}$ *i* $n \in \mathbb{N}$ *te ako vrijedi* $(b, n) = 1$, *tada je* $b^{\varphi(n)} \equiv 1 \pmod{n}$.

Dokaz. Neka skup $S = \{b_1, b_2, \ldots, b_{\varphi(n)}\}$ čini reducirani sustav ostataka modulo n. Zbog $(b, n) = 1$ i Teorema 1, skup $S_b = \{bb_1, bb_2, \ldots, bb_{\varphi(n)}\}$ je također reducirani sustav ostataka modulo n. Sada zbog definicije reduciranog sustava ostataka modulo n vrijedi:

$$\forall bb_j \in S_b \;\; \exists!\, b_i \in S : bb_j \equiv b_i \pmod{n}, \; j, i = 1, \ldots, \varphi(n).$$

Sada primjenom svojstva kongruencija slijedi:

$$\begin{aligned} bb_1 \cdot bb_2 \cdots bb_{\varphi(n)} &\equiv b_1 b_2 \cdots b_{\varphi(n)} \pmod{n} \\ b^{\varphi(n)} b_1 b_2 \cdots b^{\varphi(n)} &\equiv b_1 b_2 \cdots b_{\varphi(n)} \pmod{n} \end{aligned}$$

Zbog $(b_i, n) = 1, i = 1, \ldots, \varphi(n)$, uzastopnim dijeljenjem s b_i dobivamo $b^{\varphi(n)} \equiv 1 \pmod{n}$. □

U sljedećem korolaru navodimo jedan od važnijih teorema teorije brojeva.

Korolar 2 (Mali Fermatov teorem)**.** *Neka je dan prost broj p i neka je $a \in \mathbb{Z}$. Ako vrijedi $p \nmid a$, tada je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki $a \in \mathbb{Z}$ vrijedi $a^p \equiv a \pmod{p}$.*

Iz Eulerovog teorema slijedi ako sa n označimo prirodan broj i ako je $a \in \mathbb{Z}$ takav da je $(a, n) = 1$, tada vrijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$. Dakle, barem jedan prirodni broj d zadovoljava kongruenciju $a^d \equiv 1 \pmod{n}$. Slijedom toga, postoji najmanji prirodan broj koji zadovoljava navedenu kongruenciju.

Definicija 3. *Neka je $(a, n) = 1$. Najmanji prirodni broj d koji zadovoljava da je $a^d \equiv 1 \pmod{n}$ nazivamo red od a modulo n.*

Primjer 3. *U ovom primjeru promađimo red od 2 modulo 5. Vrijedi:*

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

Budući da je 4 najmanji prirodan broj za kojeg vrijedi $2^4 \equiv 1 \pmod{5}$, tada je 4 red od 2 modulo 5.

Sljedeća propozicija potrebna nam je kako bismo mogli pronaći sva rješenja kongruencije $a^x \equiv 1 \pmod{n}$.

Propozicija 2. *Ako je d red od a modulo n, onda je $x \in \mathbb{N}$ rješenje kongruencije*

$$a^x \equiv 1 \pmod{n} \iff d \mid x.$$

Dokaz. Pretpostavimo kako vrijedi $d \mid x$. Tada postoji $l \in \mathbb{Z} : x = d \cdot l \Rightarrow$
$a^x \equiv a^{d \cdot l} \equiv (a^d)^l \equiv 1^l \equiv 1 \pmod{n}$.
Pretpostavimo sada kako vrijedi $a^x \equiv 1 \pmod{n}$. Zbog definicije reda znamo $a^d \equiv 1 \pmod{n}$ i $d \leq x$. Sada koristeći Teorem o dijeljenju s ostatkom slijedi:

$$\begin{gathered} \exists\, q, r \in \mathbb{Z} : x = d \cdot q + r,\ 0 \leq r \leq d \\ 1 \equiv a^x \equiv a^{dq+r} \equiv (a^d)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n}. \end{gathered}$$

Dakle, imamo: $a^r \equiv 1 \pmod{n}$, gdje je $r \in \{0, \ldots, d-1\}$. Budući da je d red od a modulo n te kako tada d mora biti minimalan, mora vrijediti $r = 0 \Rightarrow x = d \cdot q \Rightarrow d \mid x$. □

Posljedica prethodne propozicije je sljedeći korolar.

Korolar 3. *Ako su $a, n \in \mathbb{Z}$ relativno prosti brojevi, pri čemu je $n > 0$ te ako sa d označimo red od a modulo n, tada vrijedi $d \mid \varphi(n)$.*

Dokaz. Budući da vrijedi $(a, n) = 1$, iz Eulerovog teorema slijedi $a^{\varphi(n)} \equiv 1 \pmod{n}$. Koristeći prethodno navedenu propoziciju, zaključujemo kako $d \mid \varphi(n)$. □

Primjer 4. *Pronađimo sada red od* 3 *modulo* 19. *Prije svega, uočimo da je* $\varphi(19) = 18$. *Jedini pozitivni djelitelji broja* 18 *su sljedeći:* $1, 2, 4, 8$ *i* 16. *Prema Korolaru 3 ovo su jedine moguće vrijednosti za red od* 3 *modulo* 19. *Budući da vrijedi*

$$\begin{aligned} 3^1 &\equiv 3 \pmod{19}, \quad 3^2 \equiv 9 \pmod{19}, \\ 3^3 &\equiv 8 \pmod{19}, \quad 3^6 \equiv 7 \pmod{19}, \\ 3^9 &\equiv 18 \pmod{19}, \quad 3^{18} \equiv 1 \pmod{19}, \end{aligned}$$

zaključujemo kako je 18 *red od* 3 *modulo* 19.

Sljedeći teorem kojeg navodimo koristit ćemo u daljnjem dijelu ovoga rada.

Teorem 4 ([3, Theorem 8.1.])**.** *Neka je* d *red od* a *modulo* n. *Ako su* a *i* n *relativno prosti cijeli brojevi pri čemu je* $n > 0$, *onda je* $a^i \equiv a^j \pmod{n}$ *ako i samo ako vrijedi* $i \equiv j \pmod{d}$, *pri čemu su* $i, j \in \mathbb{N}_0$.

Dokaz. Prvo ćemo pretpostaviti da vrijedi $i \equiv j \pmod{d}$ i neka je $0 \leq j \leq i$. Tada imamo $i = j + s \cdot d$, gdje je s neki prirodan broj. Stoga je

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

jer je $a^d \equiv 1 \pmod{n}$.
Za drugi dio dokaza pretpostavimo kako je $a^i \equiv a^j \pmod{n}$ te neka je $i \geq j$. Budući da je $(a, n) = 1$, znamo da vrijedi i $(a^j, n) = 1$. Navedenu kongruenciju možemo zapisati kao

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

te budući da vrijedi $(a, n) = 1$, slijedi

$$a^{i-j} \equiv 1 \pmod{n}.$$

Sada, koristeći Propoziciju 2 dobivamo kako $d \mid i - j$ što je ekvivalentno s $i \equiv j \pmod{d}$ □

2 Primitivni korijeni

U ovom će nas poglavlju za dani cijeli broj n zanimati cijeli brojevi a koji imaju red po modulu n jednak $\varphi(n)$. Ovo je najveći mogući red modulo n.

Definicija 4. *Ako su $a, n \in \mathbb{Z}$ relativno prosti brojevi takvi da je $n > 0$ i ako je red od a modulo n jednak $\varphi(n)$, onda kažemo da je a primitivni korijen modulo n.*

Primjer 5. *U Primjeru 3 pokazali smo kako je 4 red od 2 modulo 5. Budući da vrijedi da je $\varphi(5) = 4$, zaključujemo da je 2 primitivni korijen modulo 5.*

Sljedeći primjer pokazuje kako nemaju svi cijeli brojevi primitivne korijene.

Primjer 6. *Pokažimo kako ne postoji primitivni korijen modulo 8. Znamo kako su $1, 3, 5$ i 7 kandidati za primitivne korijene modulo 8, odnosno svi prirodni brojevi koji su manji od 8 i koji su relativno prosti s 8. Znamo kako za svaki modulo n vrijedi da je red od 1 uvijek jednak 1. Stoga vrijedi i da je red od 1 modulo 8 jednak 1. Nadalje, može se pokazati kako je red od 3 modulo 8 jednak 2. Također je 2 red brojeva 5 i 7 modulo 8. Budući da je $\varphi(8) = 4$, zaključujemo kako ne postoje primitivni korijeni modulo 8.*

Sljedeći teorem nam pokazuje jedan od slučajeva u kojima su primitivni korijeni korisni.

Teorem 5 ([3, Theorem 8.3.])**.** *Ako su $b, n \in \mathbb{N}$ relativno prosti te ako za b vrijedi da je primitivni korijen modulo n, tada je skup*

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

reducirani sustav ostataka modulo n.

Dokaz. Želimo pokazati da prvih $\varphi(n)$ potencija primitivnog korijena b čini reducirani sustav ostataka modulo n. Da bismo to učinili, samo trebamo pokazati kako su sve one relativno proste s n i kako nikoje dvije nisu kongruentne modulo n.
Budući da vrijedi $(b, n) = 1$, slijedi kako je $(b^s, n) = 1$ za bilo koji prirodan broj s. Dakle, $b^1, b^2, \ldots, b^{\varphi(n)}$ su relativno prosti s brojem n.
Da bismo pokazali da nikoje dvije potencije primitivnog korijena b nisu kongruentne modulo n, neka vrijedi

$$b^i \equiv b^j \pmod{n}.$$

Prema Teoremu 4 vrijedi $i \equiv j \pmod{d}$, gdje je d red od b modulo n. Budući da smo rekli da je b primitivni korijen od n, slijedi da je $d = \varphi(n)$, to jest, vrijedi $i \equiv j \pmod{\varphi(n)}$. Međutim, za $1 \leq i \leq \varphi(n)$ i $1 \leq j \leq \varphi(n)$, kongruencija $i \equiv j \pmod{\varphi(n)}$ implicira da vrijedi $i = j$. Dakle, $r^i \not\equiv r^j \pmod{n}$, za sve i, j za koje je $1 \leq i \leq j \leq \varphi(n)$. Time smo pokazali da imamo reducirani sustav ostataka modulo n. □

Primjer 7. *Znamo da je* 2 *primitivni korijen modulo* 9 *jer vrijedi* $2^6 \equiv 1 \pmod 9$ *i* $\varphi(9) = 6$. *Iz prethodnog teorema vrijedi da prvih* $\varphi(9) = 6$ *potencija broja* 2 *čini reducirani sustav ostataka modulo* 9. *To su:*

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

Ako neki cijeli broj ima primitivni korijen, tada on ne mora biti jedinstven. Da bismo to pokazali, prvo ćemo dokazati sljedeći teorem.

Teorem 6 ([3, Theorem 8.4.])**.** *Neka je* d *red od* a *modulo* n *i neka je* m *neki prirodan broj. Tada je red od* a^m *modulo* n *jednak* $\frac{d}{(d,m)}$.

Dokaz. Označimo sa s red od a^m modulo n, neka je $v = (d, m)$. Stoga je $d = d_1 v$ i $m = m_1 v$, za neke $d_1, m_1 \in \mathbb{N}$ koji su relativno prosti. Iz [3, Proposition 2.1.], slijedi $(d_1, m_1) = 1$.
Budući da je red od a modulo n jednak d, znamo da je

$$(a^m)^{d_1} = (a^{m_1 v})^{t/v} = \left(a^t\right)^{m_1} \equiv 1 \pmod n.$$

Stoga, iz Propozicije 2 slijedi kako $s \mid d_1$.
Nadalje, budući da je

$$(a^m)^s = a^{ms} \equiv 1 \pmod m,$$

znamo da vrijedi $d \mid ms$. Dakle, $d_1 v \mid m_1 vs$, odnosno $d_1 \mid m_1 s$. Budući da su d_1 i m_1 relativno prosti brojevi, koristeći Lemu [3, Lemma 2.3.] dobivamo da $d_1 \mid s$.
Budući da $s \mid d_1$ i $d_1 \mid s$, zaključujemo da je $s = d_1 = d/v = d/(d, m)$ čime smo dokazali teorem. □

Iz prethodnog teorema dobivamo sljedeći korolar.

Korolar 4 ([3, Corollary 8.2.])**.** *Neka je* $n \in \mathbb{N}$, $n \geq 2$. *Ako je* a *primitivni korijen modulo* n, *onda je* a^m *primitivni korijen modulo* n *onda i samo onda ako su* m *i* $\varphi(n)$ *relativno prosti brojevi.*

Dokaz. Označimo sa d red od a^m modulo n. Budući da je a primitivni korijen modulo n, $\varphi(n)$ je red od a modulo n. Iz Teorema 6 slijedi

$$D = \frac{\varphi(n)}{(m, \varphi(n))}.$$

Stoga je $d = \varphi(n)$ i d je primitivni korijen modulo n ako i samo ako vrijedi da je $(m, \varphi(n)) = 1$. □

Prethodno nas dovodi do sljedećeg teorema.

Teorem 7 ([3, Theorem 8.5.]). *Ukoliko postoji primitivni korijen modulo n, tada u reduciranome sustavu ostataka modulo n imamo točno $\varphi(\varphi(n))$ primitivnih korijena modulo n.*

Dokaz. Neka je a primitivni korijen modulo n. Tada iz Teorema 5 slijedi da cijeli brojevi $a, a^2, \ldots, a^{\varphi(n)}$ čine reducirani sustav ostataka modulo n. Koristeći Korolar 4 slijedi da je a^m primitivni korijen modulo n onda i samo onda ako je $(m, \varphi(n)) = 1$. U nizu $1, 2, \ldots, \varphi(n)$ postoji točno $\varphi(\varphi(n))$ brojeva za koje vrijedi da su relativno prosti s $\varphi(n)$. Stoga možemo zaključiti kako skup $\{a, a^2, \ldots, a^{\varphi(n)}\}$ sadrži točno $\varphi(\varphi(n))$ primitivnih korijena modulo n. □

U sljedećem primjeru ilustriramo prethodno navedeni teorem.

Primjer 8. *Neka je $n = 13$. Vrlo lako se pokaže kako je 2 primitivni korijen modulo 13. Budući da 13 ima primitivni korijen, prema Teoremu 7 znamo da 13 ima $\varphi(\varphi(13)) = \varphi(12) = 4$ primitivna korijena. Jednostavnim izračunom slijedi da su $2, 6, 7,$ i 11 primitivni korijeni modulo 13.*

2.1 Primitivni korijeni prostih brojeva

U ovom ćemo poglavlju pokazati kako za svaki prost broj p postoji primitivni korijen modulo p. Da bismo ovo pokazali, promatrat ćemo polinimijalne kongruencije. Za početak, neka nam $f(x)$ predstavlja polinom s cjelobrojnim koeficijentima. Ako vrijedi $f(c) \equiv 0 \pmod{n}$, tada za $c \in \mathbb{Z}$ kažemo da je *korijen polinoma f modulo n.*

Primjer 9. *Pretpostavimo da nam je dan polinom $f(x) = x^2 + x + 1$. Taj polinom ima 2 korijena modulo 7, a to su $x \equiv 2 \pmod{7}$ i $x \equiv 4 \pmod{7}$.*

Sljedeći nam teorem govori koliko najviše rješenja ima polinomijalna kongruencija.

Teorem 8 (Lagrangeov teorem). *Pretpostavimo da je dan prost broj p i neka je $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ polinom stupnja n s cjelobrojnim koeficijentima sa svojstvom da vodeći koeficijent danog polinoma nije djeljiv s p, to jest $p \nmid a_n$. Tada vrijedi da kongruencija $f(x) \equiv 0 \pmod{p}$ može imati najviše n rješenja modulo p.*

Dokaz. Kako bismo dokazali navedeni teorem, koristit ćemo princip matematičke indukcije. U bazi, za $n = 1$, dan nam je polinom $f(x) = a_1 x + a_0$ i uvjet $p \nmid a_1$. Korijen od $f(x)$ modulo p je rješenje linearne kongruencije $a_1 x \equiv a_0 \pmod{p}$. Kako je $(a_1, p) = 1$ i koristeći [3, Theorem 3.7.], ova linearna kongruencija ima točno jedno rješenje, odnosno postoji točno jedan korijen modulo p. Dakle, za $n = 1$ vrijedi tvrdnja.
Nadalje, pretpostavimo kako navedeno vrijedi za polinom stupnja $n - 1$ i neka nam je dan polinom g čiji vodeći koeficijent nije djeljiv s brojem p, stupnja $n - 1$. Vrijedi da tada kongruencija $g(x) \equiv 0 \pmod{p}$ sadrži najviše $n - 1$ rješenja modulo p.
Nadalje, neka je dan polinom f stupnja n, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ i neka

$p \nmid a_1$. Pretpostavimo sada kako polinom f sadrži točno $n+1$ korijena modulo p. Ti korijeni neka su $c_0, c_1, \ldots, c_n$, $c_i \neq c_j$, odnosno neka svaki c_k, $k = 0, 1, \ldots, n$ zadovoljava $f(c_k) \equiv 0 \pmod{p}$. Tada imamo

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + xc_0^{n-2} + c_0^{n-1}) + \\ &\quad a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + xc_0^{n-3} + c_0^{n-2}) + \cdots + \\ &\quad a_1(x - c_0) \\ &= (x - c_0)g(x), \end{aligned}$$

gdje je g polinom s vodećim koeficijentom a_n i stupnja $n-1$. Pokažimo sada da su $c_1, c_2, \ldots c_n$ svi korijeni polinoma g modulo p. Neka je dan $k \in \mathbb{N}$ za koji vrijedi $1 \leq k \leq n$. S obzirom da je $f(c_k) \equiv f(c_0) \equiv 0 \pmod{p}$, imamo

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod{p}.$$

Iz [3, Corollary 2.2.] znamo da je $g(c_k) \equiv 0 \pmod{p}$ jer $c_k - c_0 \not\equiv 0 \pmod{p}$. Dakle, korijen polinoma g modulo p je c_k. Iz ovoga slijedi da polinom g, stupnja jednakog $n-1$ i vodećim koeficijentom koji nije djeljiv s p, ima najviše n korijena modulo p, a što je pak u kontradikciji s pretpostavkom. Stoga, možemo zaključiti kako polinom f može imati najviše n korijena modulo p. □

U sljedećem ćemo primjeru pomoću Lagrangeovog teorema pronaći rješenja dane kongruencije.

Primjer 10. *Neka je dana sljedeća kongruencija:*

$$x^3 + 2x - 3 \equiv 0 \pmod{5}.$$

Za početak provjerimo jesu li zadovoljene sve pretpostavke Lagrangeovog teorema:

- $p = 5$ *je prost broj,*
- $f(x) = x^3 + 2x - 3$ *je polinom stupnja* 3 *s cjelobrojnim koeficijentima,*
- *vodeći koeficijent danog polinoma nije djeljiv s* p*, odnosno* $5 \nmid 1$.

Budući da su zadovoljene pretpostavke, Lagrangeov teorem kaže kako ova kongruencija može imati najviše 3 *rješenja modulo* 5*. Sva moguća rješenja su:* $x \equiv 0, 1, 2, 3, 4 \pmod{5}$*. Sada provjeravamo za svako moguće rješenje zadovoljava li danu kongruenciju:*

$$\begin{aligned} x &\equiv 0 \pmod{5} \Rightarrow f(x) \equiv -3 \pmod{5} \\ x &\equiv 1 \pmod{5} \Rightarrow f(x) \equiv 0 \pmod{5} \\ x &\equiv 2 \pmod{5} \Rightarrow f(x) \equiv 9 \pmod{5} \\ x &\equiv 3 \pmod{5} \Rightarrow f(x) \equiv 0 \pmod{5} \\ x &\equiv 4 \pmod{5} \Rightarrow f(x) \equiv 4 \pmod{5}. \end{aligned}$$

Stoga su 1 *i* 3 *rješenja kongruencije* $x^3 + 2x - 3 \equiv 0 \pmod{5}$.

Lagrangeov teorem koristimo kako bismo dokazali sljedeći teorem.

Teorem 9 ([3, Theorem 8.6.]). *Neka je dan prost broj p te neka je d djelitelj od $p-1$. Tada polinom x^d-1 ima točno d nekongruentnih korijena modulo p.*

Dokaz. Neka je $p-1=de$. Tada

$$\begin{aligned} x^{p-1}-1 &= (x^d-1)(x^{d(e-1)}+x^{d(e-2)}+\cdots+x^e+1) \\ &= (x^d-1)g(x). \end{aligned}$$

Koristeći Mali Fermatov teorem slijedi kako $x^{p-1}-1$ ima $p-1$ korijena modulo p. Nadalje, iz [3, Corollary 2.2.], znamo da je svaki korijen od $x^{p-1}-1$ modulo p ili korijen od x^d-1 modulo p ili korijen od $g(x)$ modulo p.
Lagrangeov teorem kaže nam kako $g(x)$ ima najviše $d(e-1)=p-d-1$ korijena modulo p. Budući da svaki korijen od $x^{p-1}-1$ modulo p koji nije korijen od $g(x)$ modulo p mora biti korijen od x^d-1 modulo p, znamo da polinom x^d-1 ima najmanje $(p-1)-(p-d-1)=d$ korijena modulo p. S druge strane, Lagrangeov teorem kaže nam kako polinom x^d-1 ima najviše d korijena modulo p. Posljedično, x^d-1 ima točno d korijena modulo p. □

Prethodni teorem koristan je za dokazivanje sljedećeg teorema koji nam govori koliko cijelih brojeva ima određeni red modulo p.

Teorem 10 ([3, Theorem 8.7.]). *Ako je dan prost broj p te ako je d pozitivan djelitelj od $p-1$, onda je broj međusobno nekongruentnih cijelih brojeva reda d po modulu p jednak $\varphi(d)$.*

Sljedeća tvrdnja koju navodimo direktna je posljedica prethodnog teorema.

Korolar 5 ([3, Corollary 8.3.]). *Svaki prost broj p ima primitivni korijen. Preciznije, za svaki prost broj p postoji točno $\varphi(p-1)$ međusobno nekongruentnih primitivnih korijena modulo p.*

Dokaz. Neka je dan prost broj p. Prema Teoremu 10 znamo kako postoji $\varphi(p-1)$ brojeva reda $p-1$ modulo p. Budući da je svaki od njih, po definiciji, primitivni korijen, slijedi da p ima $\varphi(p-1)$ primitivnih korijena. □

Primjer 11. *U ovom primjeru odredit ćemo sve međusobno nekongruentne primitivne korijene modulo* 13. *Prema Korolaru 5 postoji točno $\varphi(13-1)=\varphi(12)=4$ međusobno nekongruentna primitivna korijena modulo* 13. *Sljedeće ćemo ispitati koji su potencijalni kandidati iz skupa $\{2,3,\ldots,12\}$ za primitivne korijene modulo* 13. *Kako su upravo* 2 *i* 3 *jedini prosti djelitelji od $p-1=12$, tada će $a\in\{2,3,\ldots,12\}$ biti primitivan korijen modulo* 13 *onda i samo onda ako je*

$$a^{(p-1)/2}=a^6\not\equiv 1 \pmod{13},\ a^{(p-1)/3}=a^4\not\equiv 1 \pmod{13}.$$

Redom provjeravamo za $a\in\{2,3,\ldots,12\}$:

- $a = 2$*:*

$$2^6 = 64 \not\equiv 1 \pmod{13},\ 2^4 = 16 \not\equiv 1 \pmod{13}$$

odakle slijedi da je 2 *primitivni korijen modulo* 13*.*

- $a = 3$

$$3^6 = 64 \equiv 1 \pmod{13},\ 3^4 = 81 \not\equiv 1 \pmod{13}$$

iz čega slijedi da 3 *nije primitivni korijen modulo* 13*, a iz toga možemo zaključiti da nije ni* $3^2 = 9$*.*

- $a = 4$

$$4^6 = 4096 \equiv 1 \pmod{13},\ 4^4 = 256 \not\equiv 1 \pmod{13}$$

odakle imamo 4 *nije primitivni korijen modulo* 13*.*

- $a = 5$

$$5^6 = 15625 \not\equiv 1 \pmod{13},\ 5^4 = 625 \equiv 1 \pmod{13}$$

iz čega slijedi da 5 *nije primitivni korijen modulo* 13*.*

- $a = 6$

$$6^6 = 46656 \not\equiv 1 \pmod{13},\ 6^4 = 1296 \not\equiv 1 \pmod{13}$$

iz čega je 6 *primitivni korijen modulo* 13*.*

- $a = 7$

$$7^6 = 117649 \not\equiv 1 \pmod{13},\ 7^4 = 2401 \not\equiv 1 \pmod{13}$$

zaključujemo da je 7 *primitivni korijen modulo* 13*.*

- $a = 8$

$$8^6 = 262144 \not\equiv 1 \pmod{13},\ 8^4 = 4096 \equiv 1 \pmod{13}$$

iz čega slijedi da 8 *nije primitivni korijen modulo* 13*.*

- $a = 10$

$$10^6 = 1000000 \equiv 1 \pmod{13},\ 10^4 = 10000 \not\equiv 1 \pmod{13}$$

odakle dobivamo da 10 *nije primitivni korijen modulo* 13*.*

- $a = 11$

$$11^6 = 1771561 \not\equiv 1 \pmod{13},\ 11^4 = 14641 \not\equiv 1 \pmod{13}$$

iz čega slijedi da je 11 *primitivni korijen modulo* 13*.*

Dakle, budući da znamo da postoje 4 *međusobno nekongruentna primitivna korijena modulo* 11*, to su* $2, 6, 7, 11$*.*

2.2 Egzistencija primitivnih korijena

U prethodnom smo poglavlju pokazali kako za svaki prost broj p postoji primitivni korijen modulo p. U ovome ćemo se poglavlju baviti traženjem svih prirodnih brojeva koji imaju primitivne korijene. Prvo ćemo pokazati kako postoji primitivni korijen modulo p^2, pri čemu je p neparan prost broj. Nakon toga ćemo to pokazati i na nešto općenitijoj razini, odnosno, za svaki prirodan broj k pokazat ćemo kako postoji primitivni korijen modulo p^k.

Teorem 11 ([3, Theorem 8.8.]). *Ako je dan neparan prost broj p s primitivnim korijenom r, onda je ili r ili $r+p$ primitivni korijen modulo p^2.*

Dokaz. Za početak, označimo s d red od r modulo p. Kako je r primitivni korijen modulo p, vrijedi

$$d = \varphi(p) = p - 1.$$

Nadalje, pretpostavimo kako je n red od r modulo p^2. Vrijedi

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

Jasno je da tada vrijedi i

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

Kako je $p-1$ red od r modulo p, iz Teorema 4 slijedi

$$p - 1 = d \mid n.$$

S druge strane, kako je n red od r modulo p^2, prema Korolaru 3 vrijedi

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

Budući da $n \mid p(p-1)$ i $p-1 \mid n$, vrijedi da je $n = p-1$ ili $n = p(p-1)$. Ukoliko vrijedi da je $n = p(p-1)$, onda će r biti primitivni korijen modulo p^2 jer je $n = \varphi(p^2)$.

S druge strane, ako je $n = p-1$, tada je

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

Označimo sada $s = r + p$. Tada, budući da je $s \equiv r \pmod{p}$, možemo zaključiti kako također vrijedi da je s primitivni korijen modulo p. Stoga je red od s modulo p^2 jednak ili $p-1$ ili $p(p-1)$. Pokazat ćemo kako red od s modulo p^2 nije jednak $p-1$. Prema binomnom teoremu imamo sljedeće:

$$\begin{aligned} s^{p-1} &= (r+p)^{p-1} \\ &= r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \cdots + p^{p-1} \\ &\equiv r^{p-1} + (p-1)p \cdot r^{p-2} \pmod{p^2}. \end{aligned}$$

Iz (1) slijedi:

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

Iz zadnje kongruencije možemo zaključiti da

$$s^{p-1} \not\equiv 1 \pmod{p^2}.$$

Kako bismo to dokazali, primijetimo da ako je $s^{p-1} \equiv 1 \pmod{p^2}$, onda je $pr^{p-2} \equiv 0 \pmod{p^2}$. Prethodna kongruencija implicira da je $r^{p-2} \equiv 0 \pmod{p}$, a to nije moguće budući da $p \nmid r$ jer vrijedi da je r primitivni korijen modulo p. Time smo pokazali da $p-1$ nije red od s modulo p^2, stoga jedino što nam je preostalo je da $p(p-1)$ bude red od s modulo p^2, to jest da $\varphi(p^2)$ bude red od s modulo p^2. Stoga zaključujemo kako je primitivni korijen od p^2 jednak $s = r + p$.

□

Primjer 12. *Neka je dan prost broj $p = 5$. Prvo odredimo primitivni korijen modulo 5. Redom ćemo ispitati za prirodne brojeve veće od 1. Budući da je*

$$2^2 \equiv 4 \pmod{5},$$

slijedi kako je 2 primitivni korijen modulo 5 jer $3^d \not\equiv 1 \pmod{5}$ za svaki djelitelj od $\varphi(5) = 4$ koji je manji od 4. Iz dokaza Teorema 11 slijedi da je $r = 2$ također primitivni korijen modulo $p^2 = 5^2 = 25$ jer red od 2 modulo 5 poprima samo jednu od sljedeće navedenih dviju vrijednosti: ili $p - 1 = 4$ ili $\varphi(p^2) = 5^2 - 5 = 20$. No, kako je

$$2^4 \equiv 16 \not\equiv 1 \pmod{5^2},$$

zaključujemo da je

$$2^{20} \equiv 1 \pmod{5^2},$$

odnosno $r = 2$ je primitivni korijen modulo 5^2.

Sada ćemo pokazati kako prethodni teorem vrijedi i u općenitijim slučajevima, odnosno za proizvoljne potencije prostih brojeva.

Teorem 12 ([3, Theorem 8.9.])**.** *Neka je dan neparan prost broj p. Tada za svaki prirodan broj k postoji primitivni korijen p^k. Preciznije, ukoliko je r primitivan korijen modulo p^2, tada za sve prirodne brojeve k vrijedi da je r primitivan korijen modulo p^k.*

Dokaz. Iz Teorema 11 znamo da ukoliko s r označimo primitivni korijen modulo p, slijedi da je tada on i primitivni korijen modulo p^2. To znači da

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

Koristeći matematičku indukciju, pokazat ćemo

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}, \tag{3}$$

za svaki $k \in \mathbb{N}$. U bazi indukcije, za $k = 2$, navedena tvrdnja vrijedi zbog (2). Pretpostavimo kako tvrdnja $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ vrijedi za neki prirodni broj $k > 1$. Nadalje, budući da su n i p relativno prosti brojevi, to jest $(n, p) = 1$, slijedi i da je $(n, p^{k-1}) = 1$ pa prema Eulerovom teoremu vrijedi

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

Stoga, možemo zaključiti kako postoji prirodan broj d za kojega vrijedi

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

te zbog pretpostavke naše indukcije vrijedi da $p \nmid d$. Kada potenciramo s potencijom p obje strane prethodne jednakosti, dobivamo sljedeće

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

Budući da $p \nmid d$, slijedi

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

Stoga, možemo zaključiti da (3) vrijedi za sve prirodne brojeve $k > 1$.
Sada možemo pokazati kako je r primitivni korijen modulo p^k. Označimo s n red od r modulo p^k. Iz Propozicije 2, znamo da vrijedi $n \mid \varphi(p^k) = pk - 1(p - 1)$. S druge strane, kako je

$$r^n \equiv 1 \pmod{p^k},$$

znamo također i da je

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

Budući da smo rekli da je r primitivni korijen modulo p, odnosno kako je $\varphi(p) = p-1$ red od r modulo p, prema Teoremu 4, znamo da $p - 1 = \varphi(p) \mid n$. Kako $(p-1) \mid n$ i $n \mid p^{k-1}(p-1)$, znamo da je $n = p^t(p-1)$, gdje je $t \in \mathbb{Z}$ takav da je $0 \leq t \leq k-1$. Ako je $n = p^t(p-1)$ za $t \leq 2$, tada je

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

a navedeno je u suprotnosti s (3). Stoga je $n = p^{k-1}(p-1) = \varphi(p^k)$ iz čega možemo zaključiti da je r primitivni korijen modulo p^k.

□

Primjer 13. *Iz Primjera 12 znamo kako je $r = 2$ primitivni korijen modulo 5 i 5^2. Stoga, Teorem 12 kaže nam kako je $r = 2$ također primitivni korijen modulo 5^k i to vrijedi za svaki $k \in \mathbb{N}$.*

Sljedeće ćemo provjeriti imamo li primitivne korijene modulo 2^k za $k \in \mathbb{N}$. Iz prethodnih teorema vidimo kako postoje primitivni korijeni modulo 2 i $2^2 = 4$ i to su, redom, 1 i 3. Za potencije veće od 2 situacija se mijenja kao što pokazuje sljedeći teorem.

Teorem 13 ([3, Theorem 8.10.]). *Ako je dan neparan prirodan broj a i ako je $k > 2$ cijeli broj, onda vrijedi*

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

Dokaz. Ovaj ćemo teorem dokazati koristeći matematičku indukciju. Ako je a neparan prirodan broj, tada a možemo zapisati kao $a = 2b + 1$, gdje je $b \in \mathbb{Z}$. Stoga,

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1.$$

Kako je ili b ili $b+1$ paran broj, znamo da $8 \mid 4b(b+1)$, odakle slijedi

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

Prethodna kongruencija vrijedi za $k = 3$ i to je baza naše indukcije.
Da bismo završili ovu matematičku indukciju, pretpostavimo da vrijedi

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

To znači da postoji $d \in \mathbb{N}$ za koji vrijedi

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

Ako bismo kvadrirali obje strane prethodne jednakosti, dobili bismo

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

Iz prethodne jednakosti imamo da vrijedi

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

čime smo riješili matematičku induckiju pa samim time i teorem.

□

Iz prethodnog teorema zaključujemo kako nemamo potencije od 2, izuzev 2 i 4, a koje imaju primitivni korijen, no uvijek postoji prirodni broj koji ima red 2^{k-2} modulo 2^k, a taj red nam predstavlja najveći mogući red manji od $\varphi(2^k) = 2^{k-1}$.

Teorem 14 ([3, Theorem 8.11.]). *Ako je $k \geq 3$ prirodni broj, onda je $\varphi(2^k)/2 = 2^{k-2}$ red od 5 modulo 2^k.*

Dokaz. Označimo sa r red od 5 modulo 2^k. Prethodni teorem govori nam da je

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

za $k \geq 3$. Iz Propozicije 2 vidimo kako $r \mid 2^{k-2}$. Ukoliko bismo pokazali da $r \nmid 2^{k-3}$, mogli bismo zaključiti da vrijedi

$$r = 2^{k-2}.$$

Da bismo pokazali da $r \nmid 2^{k-3}$, koristit ćemo princip matematičke indukcije za $k \geq 3$ i pokazati da je

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

U bazi indukcije, za $k = 3$, očito vrijedi da je

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

Nadalje, pretpostavit ćemo kako vrijedi

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

To znači kako postoji $d \in \mathbb{N}$ takav da je

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

Ako bismo kvadrirali obje strane prethodne jednakosti, dobili bismo

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

iz čega nam 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

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

za svaki $k \geq 3$, odnosno da je red od 5 modulo 2^k jednak $\varphi(2^k)/2$. □

Sada smo pokazali da sve potencije neparnih prostih brojeva imaju primitivne korijene, dok su jedine potencije broja 2, koje imaju primitivne korijene, 2 i 4. Sljedeće utvrđujemo koji prirodni brojevi imaju primitivne korijene. Pokazat ćemo da su jedini prirodni brojevi koji posjeduju primitivne korijene upravo $2p^t$, gdje je $t \in \mathbb{N}$ i p neparan prost broj.
Prvo ćemo suziti skup prirodnih brojeva koje treba razmotriti sljedećim rezultatom.

Teorem 15 ([3, Theorem 8.12.]). *Neka je $n \in \mathbb{N}$ takav da $n \neq p^k$ i $n \neq 2p^k$, za neki prost broj p. Tada ne postoji primitivni korijen modulo n.*

Dokaz. Pretpostavimo kako nam je dan neki prirodni broj n. Pretpostavimo da, koristeći Osnovni teorem aritmetike, n možemo prikazati kao

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

pri čemu su $p_1, \dots p_m$ prosti brojevi koji su međusobno različiti i neka su $t_1, \dots t_m$ prirodni brojevi.
Neka je r primitivni korijen modulo n. To znači da su r i n relativno prosti brojevi i da je $\varphi(n)$ red od r modulo n. Kako vrijedi $(r, n) = 1$, slijedi da su r i p^t relativno prosti brojevi za $t = 1, \dots, m$, to jest vrijedi $(r, p^t) = 1$. Iz Eulerovog teorema, znamo da je

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

Pretpostavimo da je U najmanji zajednički višekratnik brojeva $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \dots, \varphi(p_m^{t_m})$. Budući da $\varphi(p_i^{t_i}) \mid U$, vrijedi

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

za $i = 1, 2, \dots, m$. Iz prethodno navedene kongruencije i Propozicije 2, vidimo da vrijedi

$$\varphi(n) \leq U.$$

Kako je Eulerova funkcija multiplikativna, imamo

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

Iz prethodnog zapisa od $\varphi(n)$ i $\varphi(n) \leq U$, slijedi

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

a to znači kako je umnožak prirodnih brojeva manji ili jednak od njihovog najmanjeg zajedničkog višekratnika. Prethodno je moguće samo ukoliko su brojevi $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \dots, \varphi(p_m^{t_m})$ u parovima relativno prosti.
Znamo da je $\varphi(p^t) = p^{t-1}(p-1)$ tako da $\varphi(p^t)$ je paran ako je p neparan ili ako je $p = 2$ i $t \geq 2$. Dakle, brojevi $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \dots, \varphi(p_m^{t_m})$ nisu u parovima relativno prosti osim ako je $m = 1$ i n je potencija prostog broja ili $m = 2$ i $n = 2p^t$, pri čemu je p neparan prost broj i t neki prirodni broj, ali navedeno je u kontradikciji s pretpostavkama teorema pa možemo zaključiti kako ne postoji primitivni korijen modulo n.

□

Sada smo ograničili razmatranje na prirodne brojeve oblika $n = 2p^t$, za neki neparan prost broj p i neki prirodan broj t. Sljedeće ćemo pokazati da svi takvi prirodni brojevi imaju primitivne korijene.

Teorem 16 ([3, Theorem 8.13.]). *Ako je dan neparan prost broj p i neki prirodan broj t, onda postoji primitivni korijen modulo $2p^t$. Međutim, ukoliko je r primitivni korijen modulo p^t i ukoliko je*

1. *r neki neparan broj, onda je r primitivni korijen modulo $2p^t$*
2. *r neki paran broj, onda je $r + p^t$ primitivni korijen modulo $2p^t$.*

Dokaz. Ako bismo sa r označili primitivni korijen modulo p^t, onda imamo kako vrijedi

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

i niti jedan pozitivan eksponent manji od $\varphi(p^t)$ nema to svojstvo. Budući da je $(2, p^t) = 1$ i zbog multiplikativnosti Eulerove funkcije je $\varphi(2p^t) = \varphi(2)\varphi(p^t) = \varphi(p^t)$, slijedi

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

Razlikujemo dva slučaja:

1. Ukoliko pretpostavimo da je broj r neparan, onda iz kongruencija

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

   slijedi $r^{\varphi(2p^t)} \equiv 1 \pmod{2p^t}$, odnosno vrijedi kako je $\varphi(2p^t)$ najmanja potencija broja r koja je kongruentna 1 modulo $2p^t$. Ukoliko bismo pronašli da postoji neka manja potencija, onda bismo i za nju mogli zaključiti da je kongruentna 1 modulo p^t. To bi bilo u suprotnosti s našom pretpostavkom kako je r primitivni korijen modulo p^t. Stoga, u slučaju kad je r neparan broj, r je primitivni korijen modulo $2p^t$.

2. Ukoliko pretpostavimo da je broj r paran, onda bi $r + p^t$ bio neparan broj. Stoga,

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

   Budući da je $r + p^t \equiv r \pmod{p^t}$, slijedi da je

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

   Prema tome, možemo zaključiti da je $(r + p^t)^{\varphi(2p^t)} \equiv 1 \pmod{2p^t}$, odnosno kako je $\varphi(2p^t)$ najmanja potenacija od $r + p^t$ koja je kongruentna 1 modulo $2p^t$. Ukoliko bismo našli neku manju potenciju, ona bi također bila kongruentna 1 modulo p^t, a to bi bilo u kontradikciji s našom pretpostavkom kako je r primitivni korijen modulo p^t. Zaključujemo da ukoliko je r paran broj, $r + p^t$ je primitivni korijen modulo $2p^t$.

□

Primjer 14. *U Primjeru 13 pokazali smo da je* 2 *primitivni korijen modulo* 5^k*, i to vrijedi za svaki* $k \in \mathbb{N}$*. Kako je* 2 *paran broj, prethodni teorem kaže da je* $r + p^t = 2 + 5^t$ *primitivni korijen modulo* $2 \cdot 5^t$*, za svaki* $t \in \mathbb{N}$*. Na primjer,* 7 *je primitivni korijen modulo* 10*.*

Sada, prema Korolaru 5 i Teoremima 12, 15, 16, možemo zaključiti koji prirodni brojevi imaju primitivni korijen.

Teorem 17 ([3, Theorem 8.14.])**.** *Prirodni broj* n *ima primitivni korijen onda i samo onda ukoliko je*

$$n = 2, 4, p^t \text{ ili } 2p^t,$$

gdje je p *neki neparan prost broj i* t *prirodan broj.*

3 Primjena primitivnih korijena

U ovom poglavlju vidjet ćemo kakva je korisnost primitivnih korijena, odnosno pogledat ćemo u kojim sve slučajevima možemo primijeniti primitivne korijene.

3.1 Indeksi

U ovom potpoglavlju demonstrirat ćemo kako se primitivni korijeni mogu koristiti za izvođenje modularne aritmetike.
Označimo s r primitivni korijen modulo n, za neki $n \in \mathbb{N}$. Iz Teorema 17 n je oblika $n = 2, 4, p^t$ ili $2p^t$. Prema Teoremu 5, znamo da brojevi

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

čine reducirani sustav ostataka modulo n. Iz ovoga vidimo da ako je a broj koji je relativno prost sa n, onda postoji jedinstven prirodan broj x, $1 \leq x \leq \varphi(n)$ koji zadovoljava

$$r^x \equiv a \pmod{n}.$$

To nas dovodi do sljedeće definicije.

Definicija 5. *Neka je dan neki prirodan broj n i neka je r primitivni korijen modulo n. Ukoliko je a prirodni broj za koji vrijedi $(a, n) = 1$, tada jedinstveni pirodni broj x takav da je $1 \leq x \leq \varphi(n)$ i $r^x \equiv a \pmod{n}$ nazivamo indeks od a u odnosu na r modulo n i označavamo ga kao $ind_r a$.*

U skladu s prethodnom definicijom vrijedi

$$a \equiv r^{ind_r a} \pmod{n}.$$

Iz Definicije 5 znamo da ukoliko su $a, b \in \mathbb{N}$ relativno prosti s brojem n i ako je $a \equiv b \pmod{n}$, onda je $ind_r a = ind_r b$.

Primjer 15. *Neka je dan broj $n = 5$. Vidjeli smo kako je 2 primitivni korijen modulo 5 i znamo $2^1 \equiv 2 \pmod{5}, 2^2 \equiv 4 \pmod{5}, 2^3 \equiv 3 \pmod{5}, 2^4 \equiv 1 \pmod{5}$. Dakle, po modulu 5 imamo*

$$ind_2\ 1 = 4,\ ind_2\ 2 = 1,$$
$$ind_2\ 3 = 3,\ ind_2\ 4 = 2.$$

S drugačijim primitivnim korijenom modulo 5, dobivamo drugačiji skup indeksa. Na primjer, ako uzmemo primitivni korijen 3 modulo 5, dobivamo sljedeći skup indeksa:

$$ind_3\ 1 = 4,\ ind_3\ 2 = 3,$$
$$ind_3\ 3 = 1,\ ind_3\ 4 = 2.$$

U sljedećem teoremu navest ćemo neka svojstva indeksa. Ova svojstva su slična svojstvima logaritama, ali umjesto jednakosti, ovdje imamo kongruencije modulo $\varphi(n)$.

Teorem 18 ([3, Theorem 8.15.]). *Neka je dan prirodni broj n, neka je r primitivni korijen modulo n i neka su a, b prirodni brojevi za koje vrijedi da su relativno prosti s brojem n. Tada vrijedi:*

(i) $ind_r 1 \equiv 0 \pmod{\varphi(n)}$,

(ii) $ind_r(ab) \equiv ind_r a + ind_r b \pmod{\varphi(n)}$,

(iii) $ind_r a^k \equiv k \cdot ind_r a \pmod{\varphi(n)}$, $k \in \mathbb{N}$.

Dokaz. (i) Iz Eulerovog teorema znamo kako vrijedi $r^{\varphi(n)} \equiv 1 \pmod{n}$. Budući da je r primitivni korijen modulo n, to znači da ne može postojati manja pozitivna potencija od r za koju vrijedi da je kongruentna 1 modulo n. Dakle,

$$ind_r 1 = \varphi(n) \equiv 0 \pmod{\varphi(n)}.$$

(ii) Kako bismo dokazali ovo svojstvo, znamo kako iz Definicije 5 slijedi

$$r^{ind_r(ab)} \equiv ab \pmod{n}$$

i

$$r^{ind_r a + ind_r b} \equiv r^{ind_r a} \cdot r^{ind_r b} \equiv ab \pmod{n}.$$

Iz prethodne dvije kongruencije slijedi

$$r^{ind_r(ab)} \equiv r^{ind_r a + ind_r b} \pmod{n}.$$

Koristeći Teorem 4, zaključujemo da je

$$ind_r(ab) \equiv ind_r a + ind_r b \pmod{\varphi(n)}.$$

(iii) Za dokazivanje ovog svojstva, primijetimo prvo kako, prema Definiciji 5, imamo

$$r^{ind_r a^k} \equiv a^k \pmod{n}$$

i

$$r^{k \cdot ind_r a} \equiv (r^{ind_r a})^k \equiv a^k \pmod{n}.$$

Dakle, iz prethodnih dviju kongruencija imamo

$$r^{ind_r a^k} \equiv r^{k \cdot ind_r a} \pmod{n}.$$

Koristeći Teorem 4 ovo nas odmah dovodi do kongruencije koju smo željeli dokazati, odnosno vrijedi

$$ind_r a^k \equiv k \cdot ind_r a \pmod{\varphi(n)}.$$

□

Primjer 16. *Iz prethodnih primjera vidjeli smo kako je* $ind_2 2 = 1$ *i* $ind_2 3 = 3$ *modulo* 5. *Kako je* $\varphi(5) = 4$, *dio (ii) Teorema 18 kaže nam kako je*

$$ind_2(2 \cdot 3) = ind_2\ 2 + ind_2\ 3 = 1 + 3 \equiv 0 \pmod 4.$$

Za provjeru, ako se vratimo u Primjer 15, vidimo kako je prethodna kongruencija točna.

Primjer 17. *U Primjeru 15 smo vidjeli da je* $ind_3\ 2 = 3$. *Stoga, koristeći (iii) dio Teorema 18, slijedi nam*

$$ind_3\ 2^5 = 5 \cdot ind_3\ 2 = 5 \cdot 3 = 15 \equiv 3 \pmod 4.$$

3.1.1 Rješavanje nekih konguencija pomoću indekasa

Koristeći indekse, možemo lako riješiti polinomijalne kongruencije oblika

$$ax^m \equiv b \pmod n,$$

$a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$, uz pretpostavku kako postoji primitivni korijen modulo n. Iz Teorema 18 imamo

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

To znači da se kongruencija $ax^n \equiv b \pmod m$ svodi na rješavanje kongruencije

$$m \cdot ind_r x \equiv ind_r b - ind_r a \pmod{\varphi(n)}.$$

Za ovu kongruenciju postoji rješenje onda i samo onda kad $(m, \varphi(n))$ dijeli $ind_r b - ind_r a$. Ukoliko je kongruencija rješiva, onda je broj rješenja navedene kongruencije jednak $(m, \varphi(n))$.

Primjer 18. *Primjenom indeksa riješit ćemo kongruenciju* $6x^{12} \equiv 11 \pmod{17}$. *Lako se pokaže kako je* 3 *primitivni korijen modulo* 17. *U sljedećoj tablici dani su indeksi prirodnih brojeva u odnosu na* 3 *modulo* 17.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Iz tablice vidimo da je $ind_3\ 11 = 7$ *te, budući da je* $\varphi(17) = 16$, *slijedi*

$$ind_3(6x^{12}) \equiv ind_3\ 11 = 7 \pmod{16}.$$

Koristeći dijelove (ii) i (iii) Teorema 18, dobivamo

$$ind_3(6x^{12}) \equiv ind_3 6 + ind_3(x^{12}) \equiv 15 + 12 \cdot ind_3 x \pmod{16}.$$

Stoga je

$$15 + 12 \cdot ind_3 x \equiv 7 \pmod{16}$$

ili

$$12 \cdot ind_3 x \equiv 8 \pmod{16}.$$

Budući da je $(12, 16) = 4$ *i* $4 \mid 8$*, slijedi kako postoji točno* 4 *međusobno nekongruentna rješenja modulo* 16 *za koja vrijedi*

$$3 \cdot ind_3 x \equiv 2 \pmod{4},$$

to jest

$$-ind_3 x \equiv 2 \pmod{4}.$$

Prethodno nam pak znači kako je

$$ind_3 x \equiv 2, 6, 10, 14 \pmod{16}.$$

Prema Definiciji 5 slijedi da su

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

sva rješenja naše kongruencije.

Pretpostavimo kako je $(a, n) = 1$. Koristeći indekse možemo riješiti i neke eksponencijalne kongruencije oblika

$$a^x \equiv b \pmod{n}.$$

Ukoliko je r primitivni korijen modulo n, onda vidimo kako je prethodna kongruencija ekvivalentna kongruenciji

$$x \cdot ind_r a \equiv ind_r b \pmod{\varphi(n)}.$$

Primjer 19. *Želimo pronaći sva rješenja kongruencije* $7^x \equiv 6 \pmod{17}$*. Kada uzmemo indekse u odnosu na* 3 *modulo* 17*, iz tablice u prethodnom primjeru imamo da je*

$$ind_3(7^x) \equiv ind_3 6 = 15 \pmod{16}.$$

Iz dijela (iii) Teorema 18, dobivamo

$$ind_3(7^x) \equiv x \cdot ind_3 7 \equiv 11x \pmod{16}.$$

Dakle,

$$11x \equiv 15 \pmod{16}.$$

Budući da je 3 *red od* 11 *modulo* 16*, množimo obje strane gornje linearne kongruencije sa* 3 *i dobivamo*

$$x \equiv 3 \cdot 15 = 45 \equiv 13 \pmod{16}.$$

Stoga je rješenje početne kongruencije upravo dano s

$$x \equiv 13 \pmod{16}.$$

3.2 Testovi prostosti

Koristeći dosad obrađene teme kao što su redovi cijelih brojeva i primitivni korijeni, možemo proizvesti korisne testove prostosti. Ove testove možemo definirati kao algoritme s kojima provjeravamo je li neki broj prost. Da bismo provjerili je li neki broj n prost, najjednostavnije je uzastopno dijeliti dani broj n prostim brojevima koji su manji od $\sqrt{n}$. U sljedećem teoremu navodimo još jedan test prostosti.

Teorem 19 (Lucasov test prostosti)**.** *Ako je $n \in \mathbb{N}$ i ako postoji $x \in \mathbb{Z}$ za kojeg vrijedi*

$$x^{n-1} \equiv 1 \pmod{n}$$

i

$$x^{(n-1)/q} \not\equiv 1 \pmod{n}$$

za svaki prost djelitelj q od $n-1$, onda je dani broj n prost.

Dokaz. Kako je $x^{n-1} \equiv 1 \pmod{n}$, Propozicija 2 kaže nam kako red od x modulo n dijeli $n-1$. Označimo red od x modulo n sa d. Pokažimo kako je $d = n-1$. Za početak, pretpostavit ćemo da vrijedi suprotno, odnosno da $d \neq n-1$. Kako vrijedi da $d|n-1$, to znači da mora postojati cijeli broj k za koji je $n-1 = k \cdot d$ i budući da smo pretpostavili da $d \neq n-1$, znamo da je $k \geq 2$. Neka je q prost djelitelj broja k. Tada

$$x^{(n-1)/q} = x^{kd/q} = (x^d)^{(k/q)} \equiv 1 \pmod{n}.$$

Međutim, prethodno je u kontradikciji s pretpostavkama teorema tako da mora vrijediti $d = n-1$.
Budući da je $d \leq \varphi(n)$ i $\varphi(n) \leq n-1$, imamo da je $\varphi(n) = n-1$. Stoga, možemo zaključiti da je n prost broj. □

Navedeni teorem ilustrirat ćemo primjerom.

Primjer 20. *Neka je $n = 1009$. Tada je $11^{1008} \equiv 1 \pmod{1009}$. Prosti djelitelji broja 1008 su $2, 3$ i 7. Lako se pokaže da je $11^{1008/2} = 11^{504} \equiv -1 \pmod{1009}$, $11^{1008/3} = 11^{336} \equiv 374 \pmod{1009}$ i $11^{1008/7} = 11^{144} \equiv 935 \pmod{1009}$. Dakle, prema prethodnom teoremu zaključujemo kako je 1009 prost broj.*

Sljedeći korolar posljedica je Teorema 19 i daje nam nešto učinkovitiji test prostosti.

Korolar 6 ([3, Corollary 8.4.])**.** *Ako je dan neki neparan prirodan broj n i ako imamo prirodan broj x za koji vrijedi*

$$x^{(n-1)/2} \equiv -1 \pmod{n}$$

i

$$x^{(n-1)/q} \not\equiv 1 \pmod{n}$$

za svaki neparan prost djelitelj q od $n-1$, tada je n prost broj.

Dokaz. Kako je $x^{(n-1)/2} \equiv -1 \pmod{n}$, imamo da je

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

Kako su sada ispunjene hipoteze Teorema 19, slijedi da je n prost broj. □

Primjer 21. *Uzmimo* $n = 2003$. *Neparni prosti djelitelji od* $n - 1 = 2022$ *su* 7, 11 *i* 13. *Za prirodan broj* x *provjerit ćemo uvjete iz Korolara 6. Za* $x = 2$ *imamo*

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

a to znači kako $x = 2$ *ne prolazi Lucasov test.*
Za $x = 3$ *imamo*

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

to jest $x = 3$ *također nije prošao test.*
Kako 2 *ne prolazi test, slijedi da ni* $2^2 = 4$ *neće proći dani test.*
Za $x = 5$

$$\begin{aligned} 5^{2002} &= 5^{1001} \equiv -1 \pmod{2003},\ 5^{2002/7} = 5^{286} \equiv 874 \pmod{2003}, \\ 5^{2002/11} &= 5^{183} \equiv 886 \pmod{2003},\ 5^{2002/13} = 5^{154} \equiv 663 \pmod{2003}. \end{aligned}$$

Dakle, prema Korolaru 6 slijedi da je $n = 2003$ *prost broj.*

4 Univerzalni eksponentni

Neka je n neki prirodni broj i neka je dan kanonski rastav broja n

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

Ako je $a \in \mathbb{N}$ i ako je $(a, n) = 1$, tada prema Eulerovom teoremu slijedi

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

gdje je p^t jedan od članova iz kanonskog rastava broja n.
Kao i u Teoremu 15, označimo s U najmanji zajednički višekratnik od $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \ldots, \varphi(p_m^{t_m})$.
Budući da vrijedi da

$$\varphi(p_j^{t_j}) \mid U,$$

za svaki $j = 1, 2, \ldots, m$, prema Propoziciji 2 slijedi

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

za svaki $j = 1, 2, \ldots, m$. Stoga, iz [3, Corollary 3.2.], slijedi

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

To nas dovodi do sljedeće definicije.

Definicija 6. *Univerzalni eksponent prirodnog broja n je prirodni broj U za koji je*

$$a^U \equiv 1 \pmod{n},$$

za svaki $a \in \mathbb{N}$ za koji je $(a, n) = 1$.

Primjer 22. *U ovom primjeru pronaći ćemo univerzalni eksponent broja* 300. *Kako je kanonski rastav od* 300 *dan sa* $300 = 2^2 \cdot 3 \cdot 5^2$, *slijedi da je najmanji zajednički višekratnik* $U = [\varphi(2^2), \varphi(3), \varphi(5^2)] = [2, 2, 20] = 20$. *Dakle, univerzalni eksponent od* 300 *je* 20.

Iz Eulerovog teorema znamo da je $\varphi(n)$ univerzalni eksponent. Kao što smo prethodno spomenuli, $U = [\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \ldots, \varphi(p_m^{t_m})]$ je također univerzalni eksponent od $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$. Sada nas zanima kako odrediti najmanji pozitivni univerzalni eksponent broja n.

Definicija 7. *Najmanji univerzalni eksponent prirodnog broja n nazivamo minimalni univerzalni eksponent od n i označavamo s $\lambda(n)$.*

Sljedeće ćemo pronaći formulu za minimalni univerzalni eksponent $\lambda(n)$ koja se temelji na kanonskom rastavu broja n.
Prvo, primijetimo da ako postoji primitivni korijen modulo n, onda je $\lambda(n) = \varphi(n)$. Budući da potencije neparnih prostih brojeva imaju primitivne korijene, znamo da je

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

za neki neparan prost broj p i neki prirodni broj t.
Slično, znamo da je $\lambda(2) = \varphi(2) = 1$ i $\lambda(4) = \varphi(4) = 2$, budući da 2 i 4 imaju primitivne korijene. S druge strane, ako je $t \geq 3$, tada prema Teoremu 13 znamo

$$a^{2^{t-2}} = 1 \pmod{2^t}$$

i red od a modulo t je 2^{t-2}, stoga možemo zaključiti da je $\lambda(2^t) = 2^{t-2}$ ako je $t \geq 3$.
Pronašli smo $\lambda(n)$ kada je $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$. U nastavku ćemo tražiti $\lambda(n)$ za proizvoljne prirodne brojeve n.

Teorem 20 ([3, Theorem 8.20.]). *Neka je dan neki prirodni broj n te neka je*

$$n = 2^{t_0} {p_1}^{t_1} {p_2}^{t_2} \cdots {p_m}^{t_m}$$

kanonski rastav broja n. Tada je minimalni univerzalni eksponent od n dan sa

$$\lambda(n) = \left[\lambda(2^{t_0}), \varphi({p_1}^{t_1}), \ldots, \varphi({p_m}^{t_m})\right].$$

Štoviše, postoji $a \in \mathbb{Z}$ takav da je red od a modulo n jednak $\lambda(n)$, najveći mogući red cijelog broja modulo n.

Dokaz. Pretpostavimo da je dan neki cijeli broj a za koji vrijedi da je relativno prost s brojem n, to jest $(a, n) = 1$. Označimo:

$$M = \left[\lambda(2^{t_0}), \varphi({p_1}^{t_1}), \ldots, \varphi({p_m}^{t_m})\right].$$

Budući da je M djeljiv sa svim brojevima $\lambda(2^{t_0}), \varphi({p_1}^{t_1}) = \lambda({p_1}^{t_1}), \varphi({p_2}^{t_2}) = \lambda({p_2}^{t_2}), \ldots,$ $\varphi({p_m}^{t_m}) = \lambda({p_m}^{t_m})$ i kako vrijedi $a^{\lambda(p^t)} \equiv 1 \pmod{p^t}$ za svaki prost broj p iz faktorizacije od n, vidimo da je

$$a^M \equiv 1 \pmod{p^t},$$

gdje je p^t broj iz faktorizacije od n.
Posljedično, prema [3, Corollary 3.2.] možemo zaključiti da je

$$a^M \equiv 1 \pmod{n}.$$

Posljednja kongruencija potvrđuje da je M univerzalni eksponent. Još moramo pokazati da je M najmanji univerzalni eksponent. Kako bismo to učinili, pronađimo $a \in \mathbb{Z}$ takav da za prirodni broj $k < M$ ne vrijedi $a^k \equiv 1 \pmod{n}$. Imajući ovo na umu, neka je r_i primitivni korijen modulo ${p_i}^{t_i}$.
Promatramo sustav kongruencija:

$$\begin{aligned}
x &\equiv 3 \pmod{2^{t_0}} \\
x &\equiv r_1 \pmod{{p_1}^{t_1}} \\
x &\equiv r_2 \pmod{{p_2}^{t_2}} \\
&\vdots \\
x &\equiv r_m \pmod{{p_m}^{t_m}}.
\end{aligned}$$

Koristeći Kineski teorem o ostacima, dobivamo rješenje a prethodnog sustava kongruencija koje je jedinstveno modulo $n = 2^{t_0}{p_1}^{t_1}{p_2}^{t_2}\cdots{p_n}^{t_m}$. Pokazat ćemo da je M red od a modulo n. Kako bismo dokazali ovu tvrdnju, pretpostavimo kako za neki prirodni broj N vrijedi

$$a^N \equiv 1 \pmod{n}.$$

Nadalje, ako je p^t djelitelj od n, pri čemu je p prost broj, tada imamo

$$a^N \equiv 1 \pmod{p^t},$$

tako da slijedi da red od a modulo p^t dijeli N.
Ali, budući da a zadovoljava svaku od $m+1$ kongruencija sustava, slijedi kako je red od a modulo p^t jednak $\lambda(p^t)$, za svaki p^t iz faktorizacije broja n. Stoga, iz [3, Corollary 3.2.], slijedi

$$M = \left[\lambda(2^{t_0}), \varphi({p_1}^{t_1}), \ldots, \varphi({p_m}^{t_m})\right] \mid N.$$

Kako je $a^M \equiv 1 \pmod{n}$ te kako vrijedi $M \mid N$ kad je $a^N \equiv 1 \pmod{n}$, možemo zaključiti da je M red od a modulo n. Ovo pokazuje kako je $M = \lambda(n)$ i istovremeno daje $a \in \mathbb{Z}$ za koji vrijedi da je $\lambda(n)$ red od a modulo n. □

Primjer 23. *Neka je* $n = 2^6 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 37 \cdot 73$. *Tada imamo*

$$\begin{aligned}
\lambda(n) &= \left[\lambda(2^6), \varphi(3^2), \varphi(5), \varphi(17), \varphi(19), \varphi(37), (73)\right] \\
&= \left[2^4, 2\cdot 3, 2^2, 2^4, 2\cdot 3^2, 2^3\cdot 3^2\right] \\
&= 2^4 \cdot 3^2 \\
&= 144.
\end{aligned}$$

Dakle, kad god imamo neki $a \in \mathbb{N}$ *za koji je* $(a, n) = 1$, $n = 2^6 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 37 \cdot 73$, *znamo da je* $a^{144} \equiv 1 \pmod{n = 2^6 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 37 \cdot 73}$.

4.1 Carmichaelovi brojevi

U ovom potpoglavlju uvest ćemo definiciju Carmichaelovih brojeva i dokazati neke teoreme vezane za Carmichaelove brojeve.

Definicija 8. *Složen broj* n *koji zadovoljava* $c^{n-1} \equiv 1 \pmod{n}$ *za svaki* $c \in \mathbb{N}$ *za koji je* $(c, n) = 1$ *nazivamo Carmichaelov broj.*

Primjer 24. *Najmanji Carmichaelov broj je* 561. *Faktorizacija navedenog broja je* $561 = 3 \cdot 11 \cdot 17$. *Kako bismo pokazali da je* 561 *Charmichaelov broj, moramo imati na umu da ako vrijedi* $(c, 561) = 1$, *onda vrijedi i* $(c, 3) = (c, 11) = (c, 17) = 1$. *Stoga, prema Malom Fermatovom teoremu vrijedi:*

$$\begin{aligned}
c^2 &\equiv 1 \pmod{3} \\
c^{10} &\equiv 1 \pmod{11} \\
c^{16} &\equiv 1 \pmod{17}.
\end{aligned}$$

Posljedično vrijedi

$$\begin{aligned} c^{560} &\equiv (c^2)^{280} \equiv 1 \pmod 3 \\ c^{560} &\equiv (c^{10})^{56} \equiv 1 \pmod{11} \\ c^{560} &\equiv (c^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Stoga je $c^{560} \equiv 1 \pmod{561}$ *za svaki* c *za koji je* $(c, n) = 1$.

Teorem 21 ([3, Theorem 5.5.]). *Ako je dan* $n \in \mathbb{N}$, $n = q_1 q_2 \cdots q_k$, *pri čemu su* q_i, $i = 1, 2, \ldots, k$ *različiti prosti brojevi koji zadovoljavaju* $q_i - 1 \mid n - 1$, *za* $i = 1, 2, \ldots, k$, *tada je* n *Carmichaelov broj.*

Dokaz. Pretpostavimo da je dan prirodan broj c za koji je $(c, n) = 1$. Vrijedi da je $(c, q_i) = 1$ za svaki $i = 1, 2, \ldots, k$ i, stoga, koristeći Mali Fermatov teorem slijedi $c^{q_i - 1} \equiv 1 \pmod{q_i}$ za $i = 1, 2, \ldots, k$. Budući da $q_i - 1 \mid n - 1$, za $i = 1, 2, \ldots, k$, postoje cijeli brojevi t_i takvi da je $t_i(q_i - 1) = n - 1$. Stoga, za svaki i znamo da vrijedi $c^{n-1} = c^{q_i - 1} t_i \equiv 1 \pmod{q_i}$. Dakle, iz [3, Corollary 3.2.] slijedi $c^{n-1} \equiv 1 \pmod n$ i zaključujemo kako je n Carmichaelov broj. □

Navedeni teorem potkrijepit ćemo sljedećim primjerom.

Primjer 25. *Pokazat ćemo da je* $6601 = 7 \cdot 23 \cdot 41$ *Carmichaelov broj. Budući da su svi brojevi u navedenoj faktorizaciji različiti prosti brojevi i budući da vrijedi* $6 = 7 - 1 \mid 6600$, $22 = 23 - 1 \mid 6600$ *i* $40 = 41 - 1 \mid 6600$, *zaključujemo da je* 6600 *Carmichaelov broj.*

Vrijedi i obrat Teorema 21 kojeg navodimo u sljedećem teoremu.

Teorem 22 ([3, Theorem 8.21.]). *Ako je* $n > 2$ *Carmichaelov broj, tada za* $n = q_1 q_2 \cdots q_k$, *gdje su* q_i, $i = 1, 2, \ldots, k$ *različiti prosti brojevi, vrijedi* $q_i - 1 \mid n - 1$, *za* $i = 1, 2, \ldots, k$.

Dokaz. Ako je n Carmichaelov broj, tada je

$$c^{n-1} \equiv 1 \pmod n$$

za sve prirodne brojeve c za koje je $(c, n) = 1$. Teorem 20 kaže nam da postoji $a \in \mathbb{Z}$ takav da je red od a modulo n jednak $\lambda(n)$, gdje je $\lambda(n)$ minimalni univerzalni eksponent te kako je $a^{n-1} \equiv 1 \pmod n$, prema Propoziciji 2 slijedi

$$\lambda(n) \mid n - 1.$$

Sada slijedi da n mora biti neparan broj jer kada bi n bio paran, tada bi $n - 1$ bio neparan broj, a budući da je $\lambda(n)$ paran (jer je $n > 2$), došli bismo do kontradikcije s $\lambda(n) \mid n - 1$. Sljedeće pokazujemo da n mora biti umnožak različitih prostih brojeva. Pretpostavimo da u faktorizaciji broja n postoji član p^t, $t \geq 2$. Tada je

$$\lambda(p^t) = \varphi(p^t) = p^{t-1}(p - 1) \mid \lambda(n) = n - 1.$$

Iz prethodnoga slijedi da $p \mid n-1$ što je nemoguće jer $p \mid n$. Dakle, n mora biti umnožak različitih neparnih prostih brojeva, odnosno

$$n = q_1 q_2 \cdots q_k.$$

Stoga, zaključujemo

$$\lambda(q_i) = \varphi(q_i) = q_i - 1 \mid \lambda(n) = n - 1.$$

□

Sada lako možemo dokazati i više o Charmichaelovim brojevima.

Teorem 23 ([3, Theorem 8.22.])**.** *Carmichaelov broj mora sadržavati najmanje tri različita neparna prosta faktora.*

Dokaz. Pretpostavimo da je n Carmichaelov broj. Znamo da tada n nema samo jedan prost faktor u svojoj faktorizaciji jer je n broj koji je složen i n je umnožak prostih brojeva koji su različiti. Stoga pretpostavimo kako je $n = pq$, pri čemu su p i q neparni prosti brojevi za koje vrijedi $p > q$. Slijedi da je

$$n - 1 = pq - 1 = (p-1)q + (q-1) \equiv q - 1 \not\equiv 0 \pmod{p-1},$$

odakle imamo da $p - 1 \nmid n - 1$. Dakle, zaključujemo kako n ne može biti Carmichaelov broj ako ima samo dva različita prosta faktora. □

Literatura

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

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

[3] K.H. Rosen, *Elementary Number Theory and Its Applications. Fourth edition.*, Addison-Wesley, Reading, MA, 2000.

[4] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, New York, 2008.

Sažetak

U ovom radu definirali smo pojam primitivnih korijena te naveli važne tvrdnje vezane za primitivne korijene. Naveli smo neke od najvažnijih teorema teorije brojeva kao što su Eulerov teorem, Mali Fermatov teorem, Lagrangeov teorem, Lucasov test prostosti. Pokazali smo kako svaki prost broj ima primitivni korijen. Upoznali smo se s nekim primjenama primitivnih korijena poput indekasa i testova prostosti. Upoznali smo se s univerzalnim eksponentima i Carmichaelovim brojevima.

Ključne riječi: primitivni korijeni, Lagrangeov teorem, prosti brojevi, indeksi, univerzalni eksponent, Carmichaelov broj

Primitive roots

Summary

In this paper, we defined the concept of primitive roots and stated important claims related to primitive roots. We have listed some of the most important theorems of number theory such as Euler's theorem, Little Fermat's theorem, Lagrange's theorem, Lucas' primality test. We have shown that every prime number has a primitive root. We were introduced to some applications of primitive roots such as indices and primality tests. We were introduced to universal exponents and Carmichael numbers.

Key words: Primitive Roots, Lagrange's Theorem, Prime Numbers, Index Arithmetic, Universal Exponents, Carmichael number

Životopis

Moje ime je Ana Rezo. Rođena sam 2. travnja 1999. godine u Požegi. Pohađala sam Osnovnu školu Zdenka Turkovića u Kutjevu u razdoblju od 2005. do 2013. godine. Po završetku osnovne škole upisala sam Opću gimnaziju u Požegi koju sam završila 2017. godine. Tijekom cijelog svog školovanja aktivno sam sudjelovala na natjecanjima iz matematike što je rezultiralo upisivanjem Preddiplomskog studija matematike na Odjelu za matematiku u Osijeku. Naziv sveučilište prvostupnice matematike stječem 2020. godine završnim radom pod nazivom "Kvadratni ostatci i primjene" pod mentorstvom doc. dr. sc. Ivana Solde. Te godine upisujem Diplomski studij matematike, smjer Financijska matematika i statisika također na Odjelu za matematiku u Osijeku. U posljednjem semestru diplomskog studija obavila sam stručnu praksu u OTP invest d.o.o. Društvu za upravljanje fondovima u Zagrebu u odjelu Front office. Trenutno radim u OTP invest d.o.o. Društvu za upravljanje fondovima u Zagrebu kao pripravnik u Front office-u.