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

Slaven Viljevac

Kongruencije višeg reda

Završni rad

Osijek, 2016.

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

Slaven Viljevac

Kongruencije višeg reda

Završni rad

voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2016.

Sažetak. U ovom završnom radu objasnit ćemo što su to kongruencije višeg reda. Objasnit ćemo što su polinomijalne kongruencije, te kako se rješavaju. Nadalje obradit ćemo kvadratne kongruencije i primitivne korjene, te ćemo pokazati kako se pronalaze primitivni korijeni i navesti ćemo njihova svojstva.

Ključne riječi: Prosti brojevi, biti kongruentan, primitivan korijen.

Abstract. This work will explain the congruences of the higher degree. It will also explain and clarify the polynomial congruences, as well as show ways of solving them. Along with an analysis of quadratic congruences and primitive roots, ways of discovering primitive roots and their properties will also be explained.

Key words: Prime numbers, congruent, primitive root.

Sadržaj

1 Uvod

Cilj ovog završnog rada je proučiti kongruencije višeg reda i opisati njihova svojstva. Za početak ćemo definirati i obraditi polinomijalne kongruencije, te nadalje kvadratne kongruencije i primitivne korijene. Obradit ćemo njihova svojstva što ćemo ilustrirati primjerima kako bismo ih lakše razumjeli.

1.1 Dodatni teoremi i definicije

U ovom poglavlju nabrojat ćemo rezultate koje ćemo kasnije koristiti ili se na njih pozivati prilikom dokazivanja narednih teorema.

Teorem 1.1. *Neka su a,b i c cijeli brojevi. Ako $a|c$ i $b|c$ te ako su a i b realtivno prosti, tada $ab|c$.*

Korolar 1.2. *Ako $m_i|c$, za $1 \leq i < n$, $(m_i, m_j) = 1$ za $i \neq j$ i $m = \prod_{i=1}^{n} m_i$, tada $m|c$.*

Teorem 1.3. *Neka $m = \prod_{i=1}^{k} m_i$ i $(m_i, m_j) = 1$ za $1 \leq i < j \leq k$, tada je svako rješenje $f(x) \equiv 0 \pmod{m_i}$ ujedno i rješenje sustava $f(x) \equiv 0 \pmod{m_i}$ za $i = 1, 2, \ldots, k$ i obratno.*

Teorem 1.4. *(Bachetov teorem) Ako su a i b cijeli brojevi, te m prirodan broj koji je relativno prost s a, tada postoji jedinstveno rješenje kongruencije $f(x) \equiv b \pmod{m}$. Ako je $(a, m) = d$ i $d|b$ tada postoji d nekongruentnih rješenja. Ako $d \nmid b$ tada nema rješenja.*

Teorem 1.5. *(Euler-Fermatov Teorem) Ako je $(a, m) = 1$, tada je $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

2 Polinomijalne kongruencije

Promatramo kongruencije oblika $f(x) \equiv 0 \pmod{m}$ gdje je $f(x)$ polinom sa cijelobrojnim koeficijentima. Te kongruencije nazivaju se polinomijalne.

Primjer 2.1. *Polinom* $f(x) = x^2 + x + 1$ *ima točno dva nekongruentna rješenja modulo* 7, *i to* $x \equiv 2 \pmod{7}$ *i* $x \equiv 4 \pmod{7}$.

Teorem 2.2. *Neka je* $m = \prod_{i=1}^{n} m_i$ *i* $(m_i, m_j) = 1$ *za* $1 \leq i < j \leq k$ *tada je svako rješenje* $f(x) \equiv 0 \pmod{m}$ *ujedno i rješenje sustava* $f(x) \equiv 0 \pmod{m_i}$ *za* $i = 0, 1, \ldots, k$. *Vrijedi i obrat.*

Dokaz. Pretpostavimo $f(x_0) \equiv 0 \pmod{m}$. Kako $m_i | m$, $f(x) \equiv 0 \pmod{m_i}$, za $i = 0, 1, \ldots, k$. Tada je svako rješenje $f(x_0) \equiv \pmod{m}$ rješenje sustava $f(x) \equiv 0 \pmod{m_i}$, za $i = 0, 1, \ldots, k$. Obrat, pretpostavimo da je $f(x_0) \equiv 0 \pmod{m_i}$ za $i = 0, 1, \ldots, k$. Tada, $m_i | f(x_0)$ za $i = 0, 1, \ldots, k$. Kako je $(m_i, m_j) = 1$, za $i \neq j$ prema Teoremu 1.1 i Korolaru 1.2 $m | f(x_0)$. Slijedi , $f(x_0) \equiv 0 \pmod{m}$. □

Ako $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ ima n_i rješenja za $i = 1, 2, \ldots, k$, po principu produkta, $f(x) \equiv 0 \pmod{m}$, gdje je $n = \prod_{i=1}^{n} p_i^{\alpha_i}$, ima najviše $\prod_{i=1}^{k} n_i$ rješenja. Prema Teoremu 1.3. kako bi rješili polinomijalnu jednadžbu $f(x) \equiv 0 \pmod{n}$, gdje je $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ pri čemu je $\alpha_i \geq 1$ za $i = 1, 2, \ldots, k$ prvo rješavamo jednadžbe $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ za $i = 1, 2, \ldots, k$. Zatim koristimo Kineski teorem o ostatcima ili namještanjem pokušavamo doći do rješenja modulo n. U oba slučaja trebamo tehniku za rješavanje polinomijalne kongruencije oblika $f(x) \equiv 0 \pmod{p^{\alpha}}$ za prost broj p i prirodan broj α veću od 1. Sljedeći rezultat pokazuje da je rješenje $f(x) \equiv 0 \pmod{p^{\alpha}}$ generirano rješenjima $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.

Teorem 2.3. *Neka je* $f(x)$ *polinom s cjelobrojnim koeficijentima,* p *prost broj i* $\alpha \geq 1$ *cijeli broj. Ako je* $x_{\alpha+1} = x_\alpha + kp^\alpha$, *gdje je* x_α *rješenje* $f(x) \equiv 0 \pmod{p^\alpha}$ *i* k *rješenje kongruencije* $(f(x_\alpha)/p^\alpha) + k \cdot f'(x_\alpha) \equiv 0 \pmod{p}$, *gdje* $0 \leq x_\alpha < p^\alpha$, $0 \leq k < p$ *pri čemu* $f'(x)$ *označava derivaciju funkcije* $f(x)$, *tada je* $x_{\alpha+1}$ *rješenje od* $f(x) \equiv 0 \pmod{p^{\alpha+1}}$.

Dokaz. Neka je p prost broj, ako $p^{\alpha+1} | a$ tada $p^\alpha | a$. Stoga je svako rješenje $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ također rješenje od $f(x) \equiv 0 \pmod{p^\alpha}$. Da budemo precizniji, ako je $f(x_{\alpha+1}) \equiv 0 \pmod{p^{\alpha+1}}$ tada postoji x_α takav da je $f(x_\alpha) \equiv 0 \pmod{p^\alpha}$ za $x_{\alpha+1} \equiv x_\alpha \pmod{p^\alpha}$ ili ekvivalentno $x_{\alpha+1} = x_\alpha + kp^\alpha$. Razvojem u Taylorov red dobivamo $f(x_{\alpha+1}) = f(x_\alpha + kp^\alpha) = f(x_\alpha) + kp^\alpha f'(x_\alpha) + k^2 N$ gdje je N cijeli broj djeljiv s $p^{\alpha+1}$. Tada je $f(x_\alpha) + kp^\alpha f'(x_\alpha) \equiv 0 \pmod{p^{\alpha+1}}$. Kako $f(x_\alpha) \equiv 0 \pmod{p^\alpha}$, $f(x_\alpha)/p^\alpha = M$ je cijeli broj. Tada $f(x_\alpha) = Mp^\alpha$ implicira $Mp^\alpha + kp^\alpha f'(x_\alpha) \equiv 0 \pmod{p^{\alpha+1}}$. Dijeljenjem sa p^α slijedi $M + kf'(x_\alpha) \equiv 0 \pmod{p}$. □

Primjer 2.4. *Riješimo kongruneciju* $27x \equiv 312 \pmod{17^3}$. *Stavimo prvo* $f(x) = 27x - 312$, *slijedi* $f'(x) = 27$. *Svako rješenje* $27x \equiv 312 \pmod{17^2}$ *je oblika* $x_1 = x_0 + k \cdot 17$ *gdje je* $27x_0 \equiv 312 \pmod{17}$ *i* $f(x_0)/17 + 27k \equiv 0 \pmod{17}$. *Jedno rješenje od* $27x_0 \equiv 312 \pmod{17}$ *je dano s* $x_0 \equiv 4 \pmod{17}$. *Sada je* $f(4) = 27 \cdot 4 - 312 = -204$, *dobivamo* $-204/17 + 27k \equiv -12 + 27k \equiv 0 \pmod{17}$ *što implicira* $k \equiv 8 \pmod{17}$. *Slijedeće rješenje* $27x \equiv 312 \pmod{17^2}$ *je dano s* $x_1 = x_0 + k \cdot 17 = 4 + 8 \cdot 17 = 140$. *Rješenje* $27x \equiv 312 \pmod{17^3}$ *je dano s* $x_2 = x_1 + r \cdot 17^2$ *gdje* $f(140)/17^2 + 27r \equiv 3468/12^2 + 27r \equiv 12 + 27r \equiv 0$ (*mod* 17) *implicira* $r \equiv 9 \pmod{17}$. *Slijedi* $x_2 = x_1 + r \cdot 17^2 = 140 + 9 \cdot 17^2 = 2741$ *je rješenje od* $27x \equiv 312 \pmod{17^3}$.

Nakon što smo iskazali i dokazali Teorem 2.1. i Teorem 2.2. možemo se posvetiti metodama za rješavanje polinomijalnih kongruencija oblika $f(x) \equiv 0 \pmod{p}$ gdje je p prost broj. Još je Lagrange krajem 18. stoljeća postavio granicu što se tiče broja rješenja polinomijalnih jednadžbi kao funkciju stupnja polinoma. Također ustvrdio je da polinomijalna jednadžba može imati najviše p nekongruentnih rješenja modulo p. Prema Malom Fermatovom teoremu, jednadžba $x^p - x \equiv 0 \pmod{p}$ ima točno p rješenja. Stoga je Lagrangeov teorem najbolje moguće rješenje.

Teorem 2.5. *(Lagrangeov teorem) Broj nekongruentnih rješenja polinomijalne jednadžbe* $f(x) \equiv 0 \pmod{p}$ *nikad nije veći od stupnja od* $f(x)$.

Dokaz. Neka je $f(x) \equiv 0 \pmod{p}$, gdje je p prost, i n je stupanj od $f(x)$. Induktivno za $n = 1$, uzmimo u obzir kongruencije oblika $ax + b \equiv 0 \pmod{p}$, gdje je $a \not\equiv 0 \pmod{p}$ takav da $ax \equiv -b \pmod{p}$. Kako $(a, p) = 1$, Teorem 1.4. povlači da jednadžba ima točno jedno rješenje. Pretpostavimo da Teorem 1.4. vrijedi za sve polinome stupnja manjeg ili jednako n. Neka je $f(x) \equiv 0 \pmod{p}$, za prost broj p i $deg(f(x)) = n + 1$. Pretpostavimo dalje kako $f(x)$ ima $n + 2$ nekongruentna rješenja modulo p, te neka je r jedno od njih. Slijedi $f(x) = g(x)(x - r)$, gdje je $deg(g(x)) = n$. Ako je s neko drugo rješenje od $f(x) \equiv 0 \pmod{p}$, tada $f(s) = g(s)(s - r) \equiv 0 \pmod{p}$. Sada je $s - r \equiv 0 \pmod{p}$, a kako je $nzd(s-r, p) = 1$ i p prost, slijedi $g(s) \equiv 0 \pmod{p}$ i s je rjeenje od $g(x) \equiv 0 \pmod{p}$. Tada polinomijalna jednadžba $g(x) \equiv 0 \pmod{p}$ stupnja n ima $n+1$ rješenje, što je u kontradikciji s pretpostavkom. □

Ako je $n > 4$ složen broj, tada n dijeli $(n - 1)!$ ili ekvivalentno $(n - 1)! \equiv 0 \pmod{n}$. 1770. u svom djelu *Meditationes Algebraicae*, Edward Waring je napomenuo da je jedan od njegovih studenata, John Wilson, došao do pretpostavke da ako je p prost broj, tada p dijeli $(p-1)!+1$, ali se dokaz činio težak zbog nedostatka zapisa prostih brijeva. Wilson na kraju napušta matematiku kako bi studirao pravo, te postaje sudac, a kasnije ga proglašavaju vitezom. Leibniz je također već 1683. dao pretpostavku rješenja ali to nije uspio dokazati. Nakon što mu je Waring poslao kopiju svoje *Meditationes Algebriacae*, Lagrange je prvi dao dokaz i njegov obrat 1771. Gauss je navodno do suštine dokaza došao u pet minuta dok je pješačio kući. Njegov klasičan protuudarac Waringovom komentaru je bio da dokaz treba biti izvučen iz pojmova, a ne iz zapisa.
Kako je

$$\sin\left(\frac{(n-1)!+1}{n}\right)\pi = 0$$

ako i samo ako je n prost. Wilsonov teorem daje zanimljiv, ali ne baš praktičan kriterij za određivanje je li broj prost ili ne, sljedeći dokaz je prema ruskom matematičaru Pafnuti Čebiševu predložen kao zakon velikih brojeva. Primjetimo, ranije je otvoreno pitanje da li je $n! + 1$ prost za beskonačno mnogo vrijednosti od n. Slijedeći rezultat pokazuje da je $n! + 1$ složen za beskonačno mnogo vrijednosti od n.

Teorem 2.6. *(Wilsonov teorem) Prirodan broj n je prost ako i samo ako je* $(n - 1)! \equiv -1 \pmod{n}$.

Dokaz. Pretpostavimo p je prost broj. Prema Malom Fermatovom teoremu rješenja od $g(x) = x^p - 1 \equiv 0 \pmod{p}$, su upravo $1, 2, \ldots, p - 1$. Promotrimo $h(x) = (x - 1)(x - 2) \ldots (x - (p - 1)) \equiv 0 \pmod{p}$, čija su rješenja $1, 2, \ldots, p - 1$. kako su $g(x)$ i $h(x)$ stupnja $p - 1$ i istog vodećeg koeficijenta, $f(x) = g(x) - h(x) \equiv 0 \pmod{p}$ je kongruencija stupnja

najviše $p-2$ koja ima $p-1$ nekongruentnih rješenja, što je u kontradikciji s Lagrangeovim teoremom. Stoga je svaki koeficijent od $f(x)$ je višekratnik od p takav da je $deg(f(x)) = 0$. No kako $f(x)$ nema konstantan član, $x \equiv 0 \pmod{p}$ također zadovoljava $f(x) \equiv 0 \pmod{p}$. Dakle $0 \equiv f(0) = g(0) - h(0) = -1 - (-1)^{p-1}(p-1)! \pmod{p}$. Ako je p neparan i prost, tada $(-1)^{p-1} \equiv 1 \pmod{p}$, a ako $p = 2$, tada $(-1)^{p-1} \equiv -1 \equiv 1 \pmod{2}$. Stoga za svaki prost broj p imamo $(p-1)! \equiv -1 \pmod{p}$. Obrat, ako je n složen, tada postoji cijeli broj d, $1 < d < n$ takav da $d|n$. Stavimo $d|(n-1)!$ i $(n-1)! \equiv 0 \pmod{d}$, što implicira $(n-1)! \not\equiv -1 \pmod{n}$. □

Neka je $f(x,y) = \frac{1}{2}(y-1)[|A^2-1| - (A^2-1)] + 2$, gdje je $A = x(y+1) - (y!+1)$, a x i y su prirodni brojevi. Ako je p neparan i prost, $x_0 = [(p-1)!+1]/p$, te $y_0 = p-1$, tada

$$A = \frac{1}{2}[(p-1)!+1][p-1+1] - [(p-1)!+1] = 0$$

imamo

$$f(x_0, y_0) = \frac{(p-1)-1}{2}[|1| - |-1|] + 2 = p.$$

$f(x,y)$ je primjer prosto generirane funkcije.

3 Kvadratne kongruencije

U prethodnom poglavlju pokazali smo da rješenje $ax^2+bx+c \equiv 0 \pmod{m}$ ovisi o rješenju $ax^2 + bx + c \equiv 0 \pmod{p}$, gdje je p prost i $p|m$. Ako je p neparan i prost i $(a, p) = 1$, tada $(4a, p) = 1$. Ako $ax^2 + bx + c \equiv 0 \pmod{p}$ pomnožimo s obje strane sa $4a$, dobivamo $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$ ili $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$. Da bi riješili kvadratnu jednadžbu $ax^2 + bx + c \equiv 0$ modulo a za prost broj p, moramo riješiti

$$(2ax + b) \equiv y \pmod{p}$$

gdje je y rješenje od

$$y^2 \equiv (b^2 - 4ac) \pmod{p}$$

Za $nzd(2a, p) = 1$, prva jednadžba uvijek ima rješenje.

Primjer 3.1. *Neka je* $6x^2 + 31x + 27 \equiv 0 \pmod{29}$. *Prvo riješimo* $y^2 = b^2 - 4ac = 961 - 648 = 313 \equiv 23 \pmod{29}$. *Kako je* $9^2 \equiv 20^2 \equiv 23 \pmod{29}$ *dobivamo rješenja* $y \equiv 9 \pmod{29}$ *i* $y \equiv 20 \pmod{29}$. *Ako je* $y \equiv 9 \pmod{29}$ *tada* $2ax + b = 12x + 31 \equiv 9 \pmod{29}$ *iz čega slijedi* $x \equiv 3 \pmod{29}$. *Ako je* $y \equiv 20 \pmod{29}$ *tada* $2ax + b = 12x + 31 \equiv 20 \pmod{29}$ *iz čega slijedi* $x \equiv 16 \pmod{29}$. *Dakle, rješenja od* $6x^2 + 31x + 27 \equiv 0 \pmod{29}$ *su* $x \equiv 3 \pmod{29}$ *i* $x \equiv 16 \pmod{29}$.

Teorem 3.2. *(Gausova lema) Ako je* p *neparan i prost i* $nzd(a, p) = 1$, *tada je* $(\frac{a}{b}) = (-1)^s$, *gdje* s *označava broj elemenata* $\{a, 2a, 3a, \ldots, \frac{1}{2}(p-1)a\}$ *većih od* $p/2$.

4 Primitivni korijeni

U ovom dijelu opisat ćemo opći postupak za rješavanje polinomijalnih kongruencija višeg reda modulo a gdje je a prost broj. Krenut ćemo od kongruencije oblika $x^m \equiv a \pmod{p}$, gdje je p neparan i prost, $a > 2$, $(a, p) = 1$. Ako je $x^m \equiv a \pmod{p}$ rješiva, reći ćemo da je a m-ta ostatak m-te potencije. Ako je n pozitivan cijeli broj i $(a, n) = 1$, najmanji pozitivan cijeli broj k takav da je $a^k \equiv 1 \pmod{n}$, naziva se red od a modulo n. i označavamo sa $ord_n(a)$. Za svaki prirodan broj n vrijedi $a^{\varphi(n)} \equiv 1$. Prema Euler-Fermatovom Teoremu $ord_n(a)$ je dobro definiran i uvijek je manji od $\varphi(n)$.

Teorem 4.1. *Ako $ord_n(a) = k$, tada je $a^h \equiv 1 \pmod{n}$ ako i samo ako k dijeli h.*

Dokaz. Pretpostavimo da $(a, n) = 1$, $ord_n(a) = k$, te $a^h \equiv 1 \pmod{n}$. Prema teoremu o dijeljenju s ostatkom, postoje cijeli brojevi q i s, takvi da $h = kq + s$, gdje je $0 \leq s < k$. Tada $a^h = a^{kq+s} = (a^k)^q a^s$. Iz $a^k \equiv 1 \pmod{n}$ slijedi $a^s \equiv 1 \pmod{n}$, pa za $s \neq 0$ dolazimo do kontradikcije s činjenicom da je k najmanje pozitivan cijeli broj sa svojstvom da $a^k \equiv 1 \pmod{n}$. Dakle $s = 0$ i k dijeli h. Obrat, ako $k|h$, tada postoji cijeli broj t takav da je $kt = h$. Kako je $ord_n(a) = k$, tada $a^h \equiv a^{kt} \equiv (a^k)^t \equiv 1 \pmod{n}$. □

Ako znamo red od a modulo n, tada uz malo truda možemo odrediti bilo koju potenciju od a modulo n, kako je i prikazano u sljedećem rezultatu.

Teorem 4.2. *Ako je $ord_n(a) = k$, tada je $ord_n(a^m) = k/(m, k)$.*

Dokaz. Neka su $ord_n(a) = k$, $ord_n(a^m) = r$, $d = (m, k)$, $m = bd$, $k = cd$ i $(b, c) = 1$. Tada je $(a^m)^c = (a^{bd})^c = (a^{cd})^b = (a^k)^b \equiv 1 \pmod{n}$. Tada prema Teoremu 4.1. $r|c$. Kako $ord_n(a) = k$, $(a^{mr}) = (a^m)^r \equiv 1 \pmod{n}$ iz Teorema 4.1. $k|mr$. Budući da cd dijeli $(bd)r$, tada c dijeli br. Kako su b i c relativno prosti, c dijeli r. Tada je c jednak r. Dakle $ord_n(a^m) = r = c = k/d = k/(m, k)$. □

Posljedica Teorema 4.1. jest da red svakog elementa modulo prost broj p dijeli $p - 1$. U nastavku, iz Teorema 4.2. slijedi da ako je d djelitelj od $p - 1$, tada postoji točno $\varphi(d)$ nekongruentnih cjelih brojeva modulo p koji su reda d.

Sljedeći korolari proizlaze direktno iz prethodna dva teorema i definicije redu elementa, pa ćemo ih samo iskazati.

Korolar 4.3. *Ako je $ord_n(a) = k$, tada k dijeli $\varphi(n)$.*

Korolar 4.4. *Ako je $ord_n(a) = k$, tada je $a^r \equiv a^s \pmod{n}$, ako i samo ako je $r \equiv s \pmod{k}$.*

Korolar 4.5. *Ako je $k > 0$ i $ord_n(a) = hk$, tada je $ord_n(a^h) = k$.*

Korolar 4.6. *Ako su $ord_n(a) = k$, $ord_n(b) = h$ i $(h, k) = 1$, tada je $ord_n(ab) = hk$.*

Red elementa koristimo kako bismo uspostavili sljedeći test prostosti, kojeg je u 18. stoljeću razvio francuski matematičar J.F.T. Pepin. Definirajmo još i Fermatove brojeve. Fermatovi brojevi su brojevi oblika $F_n = 2^{2^n} + 1$, gdje je n nenegativan cijeli broj. Prvih nekoliko Fermatovih brojeva su:

$$3, 5, 17, 257, 65537, 4294967297, \ldots$$

Teorem 4.7. *(Pepinov test prostosti) Za $n \geq 1$, n-ti Fermatov broj F_n je prost ako i samo ako je $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

Dokaz. Ako je F_n prost za $n \geq 1$ i $F_n \equiv 2 \pmod 3$. Tada prema kvadratnom zakonu reciprociteta imamo

$$\left(\frac{3}{F_n}\right)\left(\frac{F_n}{3}\right) = \left(\frac{3}{F_n}\right)\left(\frac{2}{3}\right) = \left(\frac{3}{F_n}\right)(-1) = 1.$$

Sljedi

$$\left(\frac{3}{F_n}\right) = -1.$$

Prema Eulerovom kriteriju je $3^{(F_n)/2} \equiv -1 \pmod{F_n}$.
Obratno, pretpostavimo da je $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ako je p bilo koji prost djelitelj broja F_n, tada $3^{(F_n-1)/2} \equiv -1 \pmod p$. Kvadriramo obje strane kongruencije i dobijemo $3^{F_n-1} \equiv 1 \pmod p$. Ako je m reda 3 modulo p, prema Teoremu 4.1. m dijeli $F_n - 1$, pa m dijeli 2^{2^n}. Prema tome $m = 2^r$, za $0 \leq r \leq 2^n$. Ako je $r = 2^n - s$, gdje je $s > 0$, tada je $3^{(F_n-1)/2} = 3^{2^{2^n-1}} = 3^{2^{r+s+1}} = (3^{2^r})^{2^{s-1}} = 1$, što je kontradikcija s pretpostavkom $3^{(F_n-1)/2} \equiv -1 \pmod p$. Red za $s = 0$ i 3 je 2^{2^n} modulo p. Prema Teoremu 4.1. 2^{2^n} dijeli $p - 1$. Stoga $2^{2^n} \leq p - 1$ iz čega slijedi da je $F_n \leq p$. Dakle ako je p prost djelitelj od F_n, tada je $F_n = p$. Pa je F_n prost. □

Za neke pozitivne cijele brojeve n, postoji q, $1 < q \leq n - 1$, takav da potencije od q generiraju reducirani sustav ostataka modulo n. Tada za svaki cijeli broj r, $1 \leq r \leq n - 1$, $(r, n) = 1$, postoji pozitivan cijeli broj k, takav da $q^k = r$. U tom slučaju q se može koristiti za određivanje reda elementa u $\mathbb{Z}_n^\times = \{1, 2, 3, \ldots, n-1\}$ i za određivanje kvadratnog ostatka i kvadratnog neostatka od n. Postojanje takvog broja krucijalno za postojanje rješenja polinomijalne kongruencije višeg reda. Za pozitivan cijeli broj q kažemo da je primitivan korijen od n ako je $ord_n(q) = \varphi(n)$. Sada ćemo pokazati da prosti korijeni od n generiraju reducirani sustav ostataka modulo n.

Teorem 4.8. *Ako je q primitivan korijen od n, tada q, q^2,…,$q^{\varphi(n)}$ čine reducirani sustav ostataka modulo n.*

Dokaz. Kako je q primitivan korijen od n, $ord_n(q) = \varphi(n)$, iz čega slijedi $(q, n) = 1$. Stoga je i $(q^i, n) = 1$ za $i = 1, 2, \ldots, \varphi(n)$. Elementi $q, q^2, \ldots, q^{\varphi(n)}$ od $\varphi(n)$ čine sustav međusobno nekongruentnih pozitivnih cijelih brojeva. Ako je $q^i \equiv q^j \pmod n$, za $1 \leq i < j \leq \varphi(n)$, tada je prema Korolaru 4.4. $i \equiv j \pmod{\varphi(n)}$. Prema tome $\varphi(n)$ dijeli $j - i$, što nije moguće, jer $0 < j - i < \varphi(n)$. Stoga $q^i \not\equiv q^j \pmod{\varphi(n)}$, za $1 \leq i < j \leq \varphi(n)$ i $q, q^2, \ldots, q^{\varphi(n)}$ čine sustav reduciranih ostataka modulo n.

Teorem 4.9. *(Lambertov teorem) Ako je p neparan i prost, h pozitivan cijeli broj i q prost, takav da q^h dijeli $p - 1$, tada postoji pozitivan cijeli broj b, takav da vrijedi $ord_p(b) = q^h$.*

Dokaz. Prema Lagrangeovom teoremu i činjenice da $p > 2$, jednadžba $x^{(p-1)/q} \equiv 1 \pmod p$ ima najviše $(p - 1)/q$ rješenja za

$$\frac{p-1}{q} \leq \frac{p-1}{2} \leq p - 2.$$

Tada barem jedan a, $1 \leq a \leq p-1$, takav da je $(a,p) = 1$ i a nije rješenje. Stoga $a^{(p-1)/q^h} \not\equiv 1 \pmod{p}$. Neka je $b = a^{(p-1)/q^h}$ i pretpostavimo da je $ord_p(b) = m$. Kako je $b^{q^h} \equiv a^{p-1} \pmod{p}$, prema Teoremu 4.1. slijedi m dijeli q^h. Pretpostavimo $m < q^h$. Kako je q prost i m dijeli $q^h - 1$, tada postoji cijeli broj k takav da $mk = q^{h-1}$. Prema tome $a^{(p-1)/q} = b^{q^{h-1}} = (b^m)^k \equiv 1 \pmod{p}$, što je kontradikcija s pretpostavkom. Stoga je $q^h = m = ord_p(b)$. □

U svome radu na raspisu broja $1/p$ u decimalni oblik, pri čemu je p neparan i prost, J.H. Lambert je uspostavio Teorem 4.9. i tvrdio je da postoje primitivni korijeni broja p za svaki prost broj p. Euler je uveo pojam 'primitivan korijen' 1773. kada je pokušao uspostaviti Lambertovu pretpostavku. Euler je dokazao da postoji točno $\varphi(p-1)$ primitivnih korijena broja p. Gauss je pokazao da ako je $m = 2^\alpha 5^\beta$ tada je period decimalnog proširenja za m/p^n red 10 modulo p^n. Također je pokazao da postoje primitivni korijeni modulo n, za $n = 2, 4, p, p^k, 2p^k$, gdje je p neparan i prost, a k pozitivan cijeli broj. Dokazao je da ako je q primitivan korijen neparnog prostog broja p, tada su $q^p - p, q^p - qp$ i barem jedan od q i $q+p$ primitivan korijen od p^2; ako je r primitivan korijen od p^2, tada je r primitivan korijen od p^k, za $k > 1$; a ako je s primitivan korijen od p^k, i s neparan, tada je s primitivan korijen od $2p^k$; te ako je s paran, tada je $s + p^k$ primitivan korijen od $2p^k$. U nastavku, dokazao je da ako su m i n relativno prosti pozitivni cijeli brojevi, oba veći od 3, tada ne postoje primitivni korijeni od mn. Za pozitivne cijele brojeve $n > 2$, ne postoje primitivni korijeni od 2^n, kako je i pokazano u sljedećem teoremu.

Teorem 4.10. *Ne postoje primitivni korijeni broja 2^n, za $n > 2$.*

Dokaz. Indukcijom ćemo pokazati da ako je $(a, 2^n) = 1$, za $n > 2$, tada je $ord_{2^n}(a) = 2^{n-2}$. Prema tome a ne može biti primitivan korijen od 2^n. Za $n = 3$ i $(a, 2^3) = 1$, $a \equiv 1, 3, 5, 7 \pmod{8}$. U nastavku $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$. Stoga ako je $(a, 2^3) = 1$, tada je $ord_8(a) = 2 = 2^{3-2}$. Neka je $k > 3$, pretpostavimo da ako je $(m, 1^k) = 1$, za neki cijeli prost broj m je $ord_{2^k}(m) = 2^{k-2}$. Tada je $m^{2^{k-2}} \equiv 1 \pmod{2^k}$ za $m^s \not\equiv 1 \pmod{2^k}$ za $1 \leq s < 2^{k-2}$. Neka je b takav da $(b, 2^{k+1}) = 1$. Tada iz $(b, 1^k) = 1$ i pretpostavke indukcije slijedi $ord_{2^k}(b) = 2^{k-2}$. Stoga postoji cijeli broj r takav da je $b^{2^{k-2}} = 1 + r \cdot 2^k$. U nastavku imamo $b^{2^{k-1}} = (b^{2^{k-2}})^2 = (1 + 2r \cdot 2^k + r^2 \cdot 2^{2k}) \equiv 1 \pmod{2^{k+1}}$. Pretpostavimo da postoji cijeli broj s takav da je $b^s \equiv 1 \pmod{2^{k+1}}$ za $1 \leq s < 2^k - 1$. Imamo $b^s = 1 + t \cdot 2^{k+1} = 1 + 2t \cdot 2^k$ iz čega slijedi da je $b^s \equiv 1 \pmod{2^k}$, što je kontradikcija. Stoga iz $(b, 2^{k+1}) = 1$ slijedi da je $ord_{2^{k+1}}(b) = 2^{k-1}$, pa teorem vrijedi. □

Pronalaženje primitivnih korijena nije nimalo lako. 1844. A.L. Crell je smislio učinkovitu shemu za određivanje koji su brojevi primitivni korijeni. Taj postupak je učinkovit za male proste brojeve. Postupak koristi svojstvo da je s_i najmanji ostatak od $a \cdot i$ modulo p, za $1 \leq a \leq p-1$ i t_j najmanji ostatak od a^j za $1 \leq i, j \leq p-1$, tada $t_k \equiv s_{t_{k-1}} \pmod{p}$ za $1 \leq k \leq p-1$. Crellov algoritam proizlazi iz $a^{j-1} \cdot a \equiv a^j \pmod{p}$, za $1 \leq a \leq p-1$.

Tablica 1

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$2k$	0	2	4	6	8	10	12	1	3	5	7	9	11
2^k	0	2	4	8	3	6	12	11	9	5	10	7	1

Primjer 4.11. *Neka su* $p = 13$ *i* $a = 2$. *Sada generiramo potencije broja* 2 *koristeći produkte broja* 2, *kako je i prikazano u Tablici 1. Specijalno, pretpostavimo da su redci od* k *i* $2k$ *potpuni i popunjeni na sljedeći način.* $2^0 = 1$, $2^1 = 2$ *i* $2^2 = 4$ *u donjem redu. Kako bi odredili* 2^3 *modulo* 13 *idemo u stupac* 4 *(budući da je* $2^2 \equiv 4 \pmod{13}$*), da bi pronašli* $2^3 \equiv 2 \cdot 4 \pmod{13}$. *Prema tome* $2^3 \equiv 8 \pmod{13}$. *Dalje, da bi odredili* 2^4 *modulo* 13 *idemo u stupac* 8. *Imamo* $2^4 \equiv 2 \cdot 8 \equiv 3 \pmod{13}$. *Za* 2^5 *modulo* 13 *idemo u stupac* 3, *pa imamo* $2 \cdot 3 \equiv 6 \pmod{13}$. *Postupak ponavljamo. Najmanja vrijednost od* k, $1 \leq k \leq 12$ *za koju je* $2^k \equiv 1 \pmod{13}$ *je* 12. *Stoga je* 2 *primitivan korijen modulo* 13.

Teorem 4.12. *Ako je* p *prost broj, tada postoji* $\varphi(p-1)$ *primitivnih korijena modulo* p.

Dokaz. Ako je $p - 1 = \prod_{i=1}^{r} p_i^{\alpha_i}$, gdje je $\alpha_i \geq 1$, za $i = 1, 2, \ldots, r$, kanonski oblik od $p - 1$, prema Teoremu 4.9. postoje cijeli brojevi n_i za koje je $ord_p(n_i) = p_i$, za $1 \leq i \leq r$. Generalizacijom Korolara 4.6., ako je $m = \prod_{i=1}^{r} n_i$ tada je $ord_p(m) = \prod_{i=1}^{r} p_i^{\alpha_i} = p - 1$ i m je traženi primitivan korijen. Iz Teorema 4.2, ako je q primitivan korijen od p i $(r, p-1) = 1$, tada je q^r primitivan korijen od p. Prema tome, postoji $\varphi(p-1)$ primitivnih korijena od p. □

Ako je q primitivan korijen od p, tada su $\varphi(p-1)$ nekongrunetnih korijena od p dani s $q^{\alpha_1}, q^{\alpha_2}, \ldots, q^{\alpha_{\varphi(p-1)}}$, gdje su $\alpha_1, \alpha_2, \ldots, \alpha_{\varphi(p-1)}$, $\varphi(p-1)$ cijelih brojeva manjih od $p - 1$ i relativno prostih sa $p - 1$.

Primjer 4.13. *Odredimo sve primitivne korjene od* 13. *Koristimo činjenicu da je* 2 *primitivan korjen od* 13 *i* $\varphi(12) = 4$. *Četiri cijela broja manja od* 12 *i relativno prosta s* 12 *su* $1, 3, 5$ *i* 7. *Dalje imamo* $2^1 \equiv 2$, $2^3 \equiv 8$, $2^5 \equiv 6$, $2^7 \equiv 11 \pmod{13}$. *Stoga su* $2, 8, 6, 11$ *primitivni korijeni od* 13.

Ako je $(q, m) = 1$, tada je q primitivan korijen od m ako i samo ako je $q^{\varphi(m)/p} \not\equiv 1 \pmod{m}$, za sve proste djelitelje od $\varphi(m)$. Općenito, ako primitivan korijen od m postoji, tada postoji $\varphi(\varphi(m))$ nekongruentnih primitivnih korijena od m.

Teorem 4.14. *Ako je* q *primitivan korijen prostog broja* p, *tada su kvadratni ostatci od* p *dani s* q^{2k}, *a kvadratni neostatci sa* q^{2k-1}, *za* $0 \leq k \leq (p-1)/2$.

Dokaz. Koristeći Eulerov kriterij, ako je $(a, p) = 1$, tada je

$$(q^{2k})^{(p-1)/2} = (q^{p-1})^k \equiv 1 \pmod{p}$$

i

$$(q^{2k-1})^{(p-1)/2} = (q^{p-1})^k \cdot (q^{(p-1)/2})^{-1} \equiv (q^{(p-1)/2})^{-1} \equiv -1 \pmod{p}.$$

Obrat, ako je a kvadratni ostatak od p, tada $a = (q^k)^2 = q^{2k}$ i ako je a kvadratni neostatak od p, tada je $a = (q^2)^5 \cdot q = q^{2k+1}$, za $0 \leq k \leq (p-1)/2$. □

Sljedeći rezultat je generalizacija Eulerovog kriterija za m-tu potenciju ostatka prostog broja. Dokaz će nam omogućiti da odredimo kada polinomijalna kongruencija oblika $x^m \equiv a \pmod{p}$ ima rješenje.

Teorem 4.15. *Neka je* p *neparan i prost, te neka je* $(a, p) = 1$, *tada je* $x^m \equiv a \pmod{p}$ *rješiva ako i samo ako je* $a^{(p-1)/d} \equiv 1 \pmod{p}$, *gdje je* $d = (m, p-1)$.

Dokaz. Dovoljno je pokazati nužnost. Pretpostavimo da je $a^{(p-1)/d} \equiv 1 \pmod{p}$, pri čemu su $(a,p) = 1$, $d = (m, p-1)$ i q primitivan korijen od p. Tada postoji cijeli broj s, takav da je $a = q^s$. Stoga je $q^{s(p-1)/d} \equiv a^{(p-1)/d} \equiv 1 \pmod{p}$. Kako je q primitivan korjen od p, tada je $ord_p(q) = p-1$. Tada je $s/d = k$ cijeli broj i $a \equiv q^{kd} \pmod{p}$. Kako je $d = (m, p-1)$, postoje cijeli brojevi u i v takvi da je $d = um + v(p-1)$. Tada je $a = q^{kd} = q^{kum+kv(p-1)} = q^{kum} q^{(p-1)kv} = q^{(ku)m} \cdot 1 = q^{(ku)m}$. Slijedi da je q^{ku} rješenje od $x^m \equiv a \pmod{p}$. □

Na primjer jednadžba $x^5 \equiv 9 \pmod{31}$ nema rješenja jer $9^{30/5} \equiv 9^6 \equiv -23 \not\equiv 1 \pmod{31}$. Jednadžba $x^{13} \equiv 26 \pmod{87}$ ima rješenje, budući da je $(13, 86) = 1$ i $26^{86/1} = 26^8 6 \equiv 67 \pmod{87}$.
Ako za m uzmemo neku vrijednost, tada možemo pronaći sve m-te potencije ostatka modulo prost broj, kako je opisano u sljedećem rezultatu.

Teorem 4.16. *Ako su p neparan prost broj, q je primitivan korijen od p i $d = (m, p-1)$, tada je m-ta potencija ostatka od p dana s $q^d, q^{2d}, \ldots, q^{d(p-1)/d}$.*

Dokaz. Neka je p neparan i prost, q primitivan korijen od p i $d = (m, p-1)$. Prema dokazu Teorema 4.15. svaki element iz skupa $q^d, q^{2d}, \ldots, q^{d(p-1)/d}$ je m-ta potencija ostatka od p. U nastavku oni su nekongruentni modulo p, ako je $q^{id} \equiv q^{jd} \pmod{p}$, za neke $1 \leq i < j \leq (p-1)/d$, prema Korolaru 4.4. $p-1$ dijeli $d(j-i)$ što nije moguće budući da je $0 < d(j-i) < p-1$. Pretpostavimo da je a ostatak m-te potencije modulo p. Stoga postoji b, takav da $1 \leq b \leq p-1$, za koji je $b^m \equiv a \pmod{p}$. Postoji k takav da $1 \leq k \leq p-1$, za koji je $b \equiv q^k \pmod{p}$, prema tome $a \equiv b^m \equiv q^{kd} \pmod{p}$. Neka su r, s, t, u takvi da je $ud = m$, $rd = p-1$, $uk = st + r$, za $0 \leq r < t$. Tada je $a \equiv q^{mk} \equiv q^{ukd} \equiv q^{(st+r)d} \equiv q^{(p-1)s} q^{rd} \equiv q^{rd} \pmod{p}$. Tada je a iz skupa $q^d, q^{2d}, \ldots, q^{d(p-1)/d}$. □

Postoji veza između primitivnih korijena i kvadratnih neostataka neparnih prostih brojeva. Posebno ako je p neparan prost broj i a kvadratni neostatak od p, tada postoji b, $1 \leq b \leq p-1$, takav da $b^2 \equiv a \pmod{p}$. Prema tome $a^{(p-1)/2} \equiv b^{((p-1)/2)^2} \equiv b^{p-1} \equiv 1 \pmod{p}$. Dakle, za neparan prost broj p, svaki primitivan korijen od p je kvadratni neostatak od p.

Teorem 4.17. *Neka je p neparan prost broj. Tada je svaki kvadratni neostatak od p je primitivan korijen od p, ako i samo ako je $p = 2^k + 1$, za pozitivan cijeli broj k.*

Dokaz. Postoji $(p-1)/2$ kvadratnih neostataka od p i $\varphi(p-1)$ primitivnih korijena od p. Svaki kvadratni neostatak od p je primitivan korijen od p ako i samo ako je $\varphi(p-1) = (p-1)/2$, ali $\varphi(n) = n/2$ ako i samo ako je $n = 2^k$. Pa je $p = 2^k + 1$. □

Gauss je uveo metodu za rješavanje polinomijalnih kongruencija višeg reda modulo prost broj. Posebno, ako je p neparan prost broj i q primitivan korijen od p i pišemo $r = I_q(n) \pmod{p}$ ako i samo ako je $n \equiv q^r \pmod{p}$, za $0 \leq r < p-1$. Uočimo da je $q^{I_q(n)} \equiv n \pmod{p}$. Ako su p i q poznati iz konteksta, pišemo samo $I(n)$ za označavanje indeksa od n po bazi q modulo p. Sljedeći rezultat nam pruža dovoljno, kako bismo mogli riješiti polinomijalne kongruencije višeg reda poput ostalih problema u modularnoj aritmetici.

Teorem 4.18. *Ako je p neparan i prost, q primitivan korijen od p, m i n cijeli brojevi, za koje je $(m,p) = (n,p) = 1$ i r i k prirodni brojevi, tada je*

(a) $m \equiv n \pmod{p}$ *ako i samo ako je* $I(m) \equiv I(n) \pmod{p-1}$,

(b) $I(q^r) \equiv r \pmod{p-1}$,

(c) $I(1) = 0$ *i* $I(q) = 1$,

(d) $I(mn) \equiv I(m) + I(n) \pmod{p-1}$,

(e) $I(n^k) \equiv k \cdot I(n) \pmod{p-1}$.

Dokaz. Budući da je q primitivan korijen modulo p, $ord_p(q) = p-1$. Neka je $r = I(m)$ i $s = I(n)$; prema tome je $q^r \equiv m \pmod{p}$ i $q^s \equiv n \pmod{p}$.

(a) $m \equiv n \pmod{p}$ ako i samo ako je $q^r \equiv q^s \pmod{p}$ ako i samo ako je $r \equiv s \pmod{p-1}$ ako i samo ako je $I(m) \equiv I(n) \pmod{p-1}$. □

(b) Kako je $I(q^r) \equiv m \pmod{p}$, prema (a) je $I(q^r) \equiv I(m) \equiv r \pmod{p-1}$. □

(c) $1 \equiv q^0 \pmod{p}$ i $q \equiv q^1 \pmod{p}$. Tada je $I(1) = 0$ i $I(q) = 1$. □

(d) $q^{r+s} = q^r q^s \equiv mn \pmod{p}$. Prema (a), imamo $I(mn) \equiv r + s \equiv I(m) + I(n) \pmod{p-1}$. □

(e) $q^{st} \equiv n^t \pmod{p}$. Prema (a), imamo $I(n^t) \equiv ts \equiv t \cdot I(n) \pmod{p-1}$ □

Tablica indeksa (Tablica 2) za primitivne korjene 2 modulo 13 se dobiva iz Tablice 1, na način da se ispusti drugi redak i prepisivanjem trećeg retka u uzlaznom poretku i izmjenjujući treći redak s prvim.

Tablica 2

k	1	2	3	4	5	6	7	8	9	10	11	12
$I(k)$	12	1	4	2	9	5	11	3	8	10	7	6

Primjer 4.19. *Iskoristimo indekse i činjenicu da je* 2 *primitivan korijen od* 13 *i Tablicu 2 da bi riješili kongruenciju* $5x \equiv 4 \pmod{13}$.

$$I(5x) \equiv I(4) \pmod{12},$$

$$I(5) + I(x) \equiv I(4) \pmod{12},$$

$$9 + I(x) \equiv 2 \pmod{12},$$

$$I(x) \equiv 5 \pmod{12},$$

$$x \equiv 6 \pmod{13}.$$

5 Literatura

[1] B. Jadrijević, Uvod u teoriju brojeva, Odjel za matematiku, Sveučilište u Splitu, 2014.

[2] I. Matić, Uvod u teoriju brojeva, Odjel za matematiku, Sveučilište u Osijeku, 2013.

[3] J. J. Tattersall, Elementary number theory in nine chapters, Cambridge University Press The Edinburgh Building, Cambridge CB2 2RU, UK, 2005.