Kongruencije višeg reda

Lalić, Jelena

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:694694

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

Jelena Lalić

Kongruencije višeg reda

Diplomski rad

Osijek, 2016.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

Jelena Lalić

Kongruencije višeg reda

Diplomski rad

Mentor: izv.prof.dr.sc. Ivan Matić

Osijek, 2016.

Sadržaj

1 Uvod

Teorija kongruencija daje nam drukčiji pogled na probleme koji se tiču djeljivosti te nalazi svoju primjenu daleko izvan teorije brojeva. Nepresušan izvor intrigantnih problema vezanih uz kongruencije naveli su mnoge poznate matematičare poput Legendrea, Lagrangea, Eulera i Gaussa da teoriju brojeva svojim rezultatima izdvoje kao zasebnu granu matematike. Jezik kongruencije razvio je Karl Friedrich Gauss 1801. godine u svome djelu "Disquisitiones Arithmeticae".

U ovom radu postepeno ćemo razvijati metodu za rješavanje polinomijalnih kongruencija oblika $f(x) \equiv 0 \pmod{m}$, gdje je f polinom s cjelobrojnim koeficijentima. Od polinomijalnih kongruencija prvo ćemo promatrati one najjednostavnije, linearne kongruencije, a zatim se zaustaviti na kvadratnim kongruencijama i pokazati vezu između vrijednosti Legendreovog simbola i egzistencije rješenja kongruencije oblika $x^2 \equiv a \pmod{p}$, gdje je p neparan prost broj. U zadnjem poglavlju ćemo uvesti pojam primitivnog korijena koji će odigrati važnu ulogu u rješavanju polinomijalnih kongruencija.

2 Djeljivost

Definicija 2.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da a dijeli b ako postoji cijeli broj x takav da je $b = ax$. U tom slučaju pišemo $a \mid b$. Kažemo još da je a dijelitelj od b te da je b višekratnik od a. Ukoliko b nije djeljiv s a pišemo $a \nmid b$.*

Neka su a, b i c cijeli brojevi. Navedimo nekoliko osnovnih svojstava djeljivosti:

(1) Ako je $a \neq 0$, tada $a \mid a$ i $a \mid 0$.

(2) Za svaki a vrijedi $1 \mid a$.

(3) Ako $a \mid b$ i $a \mid c$, tada $a \mid (bx + cy)$ za sve $x, y \in \mathbb{Z}$.

(4) Ako $a \mid b$ i $b \mid c$, tada $a \mid c$.

(5) Ako je $a > 0$, $b > 0$ i $a \mid b$, tada je $a \leq b$.

Jednu od osnovnih tvrdnji iz koje proizlaze mnoga svojstva djeljivosti predstavlja Teorem o dijeljenju s ostatkom.

Teorem 2.1 (**Teorem o dijeljenju s ostatkom**). *Za proizvoljan cijeli broj a i prirodan broj b postoje jedinstveni cijeli brojevi q i r takvi da je $a = bq + r$, gdje je $0 \leq r < b$.*

Dokaz. Promotrimo skup $S = \{a - sb : s \in \mathbb{Z} \text{ takav da je } a - sb \geq 0\}$. Ukoliko je $a < 0$, tada je $a - ab = a(1 - b) \geq 0$, odnosno, $a - ab \in S$. Ako je $a \geq 0$, vrijedi $a = a - 0 \cdot b \geq 0$ te je $a \in S$. Dakle, S je neprazan podskup skupa $\mathbb{N}$ te prema tome ima najmanji element. Označimo ga s $r = a - bq \geq 0$. Dodatno vrijedi $r - b = (a - bq) - b = a - (q + 1)b < 0$, tj. $0 \leq r < b$.
S ciljem dokazivanja jedinstvenosti brojeva q i r pretpostavimo da postoji još jedan par u i v koji zadovoljava iste uvjete, odnosno $a = bu + v$, gdje je $0 \leq v < b$. Pretpostavimo da je $u < q$. Budući su u i q prirodni brojevi, vrijedi $u + 1 \leq q$. Odatle je $r = a - bq \leq a - b(u + 1) = (a - ub) - b = v - b < 0$ što je u kontradikciji s pretpostavkom $r \geq 0$. Sličnu kontradikciju dobivamo za $q < u$. Očito je $u = q$ što dalje implicira $v = r$. □

Definicija 2.2. *Neka su a i b cijeli brojevi. Cijeli broj d nazivamo najveći zajednički djelitelj brojeva a i b i označavamo s (a, b) ukoliko vrijedi:*

1. *$d > 0$*

2. *$d \mid a$ i $d \mid b$*

3. *ako je $e \in \mathbb{Z}$ takav da $e \mid a$ i $e \mid b$, tada $e \mid d$.*

Slično se definira najveći zajednički djelitelj brojeva $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, koji nisu svi jednaki nuli, i označava s $(a_1, a_2, \ldots a_n)$.

Definicija 2.3. *Za cijele brojeve a i b kažemo da su relativno prosti ako je $(a, b) = 1$. Slično, za cijele brojeve $a_1, a_2, \ldots, a_n$ kažemo da su relativno prosti ako je $(a_1, a_2, \ldots, a_n) = 1$. Ukoliko vrijedi $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$, kažemo da su $a_1, a_2, \ldots, a_n$ u parovima relativno prosti.*

Određivanje najvećeg zajedničkog djelitelja dva cijela broja, posebno ukoliko se radi o većim brojevima, zahtjeva metodu koja se pojavljuje u Euklidovim Elementima, a poznata je pod nazivom Euklidov algoritam.
Euklidov algoritam baziran je na teoremu 2.1. Neka su $a, b \in \mathbb{Z}$, $b > 0$. Pretpostavimo da je uzastopnom primjenom teorema 2.1 dobiven sljedeći niz jednakosti:

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b,\\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_ng_{n+1}.
\end{aligned}$$

Neka je $r_n \neq 0$. Budući je $r_1, r_2, \ldots, r_{n+1}$ strogo padajući niz nenegativnih cijelih brojeva, dani niz se završava ostatakom koji je jednak nuli te stavimo $r_{n+1} = 0$. Iz zadnje jednakosti algoritma imamo da r_n dijeli r_{n-1}. Zatim iz predzadnje jednakosti slijedi da r_n dijeli r_{n-2}. Nastavljajući na sličan način dolazimo do zaključka da r_n dijeli brojeve a i b, odnosno r_n je zajednički djelitelj brojeva a i b. Nadalje, ako pretpostavimo da je e bilo koji nenegativan cijeli broj koji dijeli oba broja a i b, tada iz prve jednakosti algoritma slijedi kako e dijeli r_1. Pogledamo li drugu jednakost, vidimo da tada e dijeli i r_2. Nastavljajući dalje dobivamo da e dijeli r_n, točnije, r_n je najveći zajednički djelitelj brojeva a i b.

Primjer 2.1. *Odrediti* $(481, 299)$.

$$\begin{aligned}
481 &= 299 \cdot 1 + 182\\
299 &= 182 \cdot 1 + 117\\
182 &= 117 \cdot 1 + 65\\
117 &= 65 \cdot 1 + 52\\
65 &= 52 \cdot 1 + 13\\
52 &= 13 \cdot 4
\end{aligned}$$

Odatle je $(481, 299) = 13$.

Euklidov algoritam, osim što služi za određivanje najvećeg zajedničog djelitelja brojeva a i b, također daje mogućnost prikazivanja tog istog djelitelja kao linearne kombinacije brojeva

a i b. Sve što treba je ići unazad korak po korak u algoritmu. U prethodnom primjeru bi to izgledalo ovako:

$$\begin{aligned} 13 &= 65 - 52 = 65 - (117 - 65) \\ &= (182 - 117) \cdot 2 - 117 = 182 \cdot 2 - 117 \cdot 3 \\ &= 182 \cdot 2 - (299 - 182) \cdot 3 = (481 - 299) \cdot 5 - 299 \cdot 3 \\ &= 481 \cdot 5 - 299 \cdot 8. \end{aligned}$$

Ne samo da se najmanji zajednički djelitelj dva broja može prikazati u obliku linearne kombinacije ta dva broja, nego je on najmanji prirodan broj takvog oblika.

Teorem 2.2. *Neka $a, b \in \mathbb{Z}$ nisu oba jednaka nuli i neka je $(a, b) = d$. Tada je d najmanji element skupa svih linearnih kombinacija brojeva a i b koje su veće od nule.*

Dokaz. Neka je $T = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$.
Bez smanjenja općenitosti, pretpostavimo da je $a \neq 0$. Ako je $a > 0$, tada je $a = a \cdot 1 + b \cdot 0$ te je $a \in T$. Ukoliko je $a < 0$, tada je $-a = a \cdot (-1) + b \cdot 0$ te je $-a \in T$. Zaključujemo da je skup T neprazan podskup skupa $\mathbb{N}$, stoga ima najmanji element. Označimo ga s $e = au + bv$. Prema teoremu 2.1 postoje $q, r \in \mathbb{Z}$ takvi da je $a = eq + r$, gdje je $0 \leq r < e$. Stoga je $r = a - eq = a - (au + bv)q = a(1 - uq) + b(-vq)$, tj. $r \in T$. Ukoliko je $r \neq 0$ imamo kontradikciju s pretpostavkom da je e najmanji element skupa T pa je $r = 0$ te vrijedi $e \mid a$. Na sličan način se pokaže da $e \mid b$. Kako e dijeli i a i b, prema definiciji 2.2 tada $e \mid d$, odnosno $e \leq d$. S druge strane, iz $e = au + bv$, $d \mid a$ i $d \mid b$, slijedi $d \mid e$, odnosno $d \leq e$. Sada je $r = d$ i time je tvrdnja dokazana. □

Korolar 2.1. *Ako je d najveći zajednički djelitelj brojeva a i b, tada postoje $x, y \in \mathbb{Z}$ takvi da je $d = ax + by$.*

Teorem 2.3. *Neka su a, b i c cijeli brojevi. Ako $a \mid c$ i $b \mid c$ te vrijedi $(a, b) = 1$, onda $ab \mid c$.*

Dokaz. Budući da a i b dijele broj c, postoje $x, y \in \mathbb{Z}$ takvi da je $au = bv = c$. Pretpostavimo da su a i b relativno prosti brojevi te prema korolaru 2.1 postoje $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$. Pomnožimo li obje strane jednakosti s c dobivamo $c = axc + byc = ax(bv) + by(au) = ab(xv + yu)$. Dakle $ab \mid c$. □

Korolar 2.2. *Ako $m_i \mid c$, za $1 \leq i \leq k$, $(m_i, m_j) = 1$ za $i \neq j$, tada $m \mid c$, gdje je $m = \prod_{i=1}^{k} m_i$.*

3 Kongruencije

3.1 Osnovna svojstva

Definicija 3.1. *Neka je n prirodan broj te neka su a i b cijeli brojevi. Ako n dijeli razliku $a-b$ tada kažemo da je a kongruentan b modulo n i pišemo $a \equiv b \pmod{n}$.*

Teorem 3.1. *Neka je n prirodan broj. Biti kongruentan modulo n je relacija ekvivalenije na skupu cijelih brojeva.*

Teorem 3.2. *Cijeli brojevi daju isti ostatak pri dijeljenju prirodnim brojem m ako i samo ako $a \equiv b \pmod{m}$.*

Dokaz. Neka su r i s ostaci pri dijeljenju brojeva a i b modulo m. Prema teoremu 2.1 postoje $t, u \in \mathbb{Z}$ takvi da su $a = mt + r$ i $b = mu + s$, gdje su $0 \leq r < m$ i $0 \leq s < m$. Iz toga je $a - b = m(t-u) + (r-s)$, odnosno $m \mid (a-b)$ ako i samo ako $m \mid (r-s)$. Prema tome $a \equiv b \pmod{m}$ ako i samo ako je $r = s$. □

Teorem 3.3. *Ako je $a_i \equiv b_i \pmod{m}$ za $i = 1, 2 \ldots, n$, tada je*

(1)
$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m} ,$$

(2)
$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m} .$$

Teorem 3.4. *Ako je $a \equiv b \pmod{m}$, tada za svaki prirodni broj c i za svaki prirodni broj n vrijedi:*

(1) $a \pm c \equiv b \pm c \pmod{m}$

(2) $a \cdot c \equiv b \cdot c \pmod{m}$

(3) $a^n \equiv b^n \pmod{m}$.

Iduću tvrdnju lako bismo dokazali pomoću korolara 2.2.

Teorem 3.5. *Ako je $a \equiv b \pmod{m_i}$ za $i = 1, 2, \ldots, k$, gdje su $m_1, m_2, \ldots, m_k$ u parovima relativno prosti, tada je $a \equiv b \pmod{m}$, $m = \prod_{i=1}^{k} m_i$.*

Teorem 3.6. *Ako je $ac \equiv bc \pmod{m}$, tada je $a \equiv b \pmod{\frac{m}{d}}$, gdje je $d = (c, m)$.*

Dokaz. Ako je $ac \equiv bc \pmod{m}$, tada postoji $k \in \mathbb{Z}$ tako da je $ac - bc = km$. Neka je $d = (c, m)$. Tada vrijedi $(a-c)\frac{c}{d} = k\frac{m}{d}$ i $(\frac{c}{d}, \frac{m}{d}) = 1$. Dakle $\frac{m}{d} \mid (a-b)$, tj. $a \equiv b \pmod{\frac{m}{d}}$. □

Korolar 3.1. *Ako je $ac \equiv bc \pmod{m}$ i vrijedi $(c, m) = 1$, tada je $a \equiv b \pmod{m}$.*

3.2 Potpuni sustav ostataka

Definicija 3.2. *Neka je m prirodan broj veći od 1. Skup $S = \{a_1, a_2, \ldots, a_m\}$ naziva se potpuni sustav ostataka modulo m ako za svaki broj b postoji jedinstveni $a_i \in S$ za koji vrijedi $b \equiv a_i \pmod{m}$.*

Drugim riječima, potpuni sustav ostataka modulo m je skup koji se sastoji od m međusobno nekongruentnih cijelih brojeva. Postoji beskonačno potpunih sustava ostataka modulo m. Najpogodniji i najčešće korišten potpuni sustav ostataka modulo m je $\{0, 1, 2, \ldots, m-1\}$.

Primjer 3.1. *Skup $\{0, 1, 2, \ldots, 6\}$ je potpuni sustav ostatak modulo 7, a to su također i skupovi: $\{-3, -2, -1, \ldots, 3\}$, $\{2, 3, 4, \ldots, 8\}$, $\{4, 5, 6, \ldots, 10\}$.*

Teorem 3.7. *Neka je $\{a_1, a_2, \ldots, a_m\}$ potpuni sustav ostataka modulo m, $c \in \mathbb{Z}$ i $(c, m) = 1$. Tada je $\{c \cdot a_1, c \cdot a_2, \ldots, c \cdot a_m\}$ također potpuni sustav ostataka modulo m.*

Dokaz. Pretpostavimo da je $\{a_1, a_2, \ldots, a_m\}$ potpuni sustav ostataka modulo m te neka je $c \cdot a_i \equiv c \cdot a_j \pmod{m}$ za neke $1 \leq i < j \leq m$. Korolar 3.1 tada povlači $a_i \equiv a_j \pmod{m}$, što je u kontradikciji s pretpostavkom. Prema tome je $c \cdot a_i \not\equiv c \cdot a_j \pmod{m}$ za $i \neq j$ te $\{c \cdot a_1, c \cdot a_2, \ldots, c \cdot a_m\}$ čini potpuni sustav ostataka modulo m. □

3.3 Eulerova funkcija

Definicija 3.3. *Za svaki prirodan broj m, $\varphi(m)$ označava broj prirodnih brojeva koji su manji ili jednaki m i koji su relativno prosti s m, dok funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ zovemo Eulerova funkcija.*

Primjer 3.2. *$\varphi(10) = 4$ budući su $1, 3, 7$ i 9 jedini prirodni brojevi manji od 10 i relativno prosti s 10.*

Definicija 3.4. *Neka je m prirodni broj veći od 1. Skup $S = \{a_1, a_2, \ldots, a_r\}$ naziva se reducirani sustav ostataka modulo m ako za svaki broj x, koji je relativno prost s m, postoji jedinstveni $a_i \in S$ za koji vrijedi $x \equiv a_i \pmod{m}$.*

Primijetimo kako je reducirani sustav ostataka modulo m sačinjen od onih $\varphi(m)$ elemenata potpunog sustava ostataka modulo m koji su relativno prosti s m.

Primjer 3.3. *Prema prethodnom primjeru, $\{1, 3, 7, 9\}$ čini reducirani sustav modulo 10. Skupovi $\{3, 9, 21, 27\}$, $\{7, 21, 49, 63\}$ i $\{-9, -7, -3, -1\}$ su također potpuni sustavi ostataka modulo 10.*

Idući teorem može se dokazati na sličan način kao i teorem 3.7.

Teorem 3.8. *Neka je $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ reducirani sustav ostataka modulo m, $c \in \mathbb{Z}$ i $(c, m) = 1$. Tada je $\{c \cdot a_1, c \cdot a_2, \ldots, c \cdot a_{\varphi(m)}\}$ također reducirani sustav ostataka modulo m.*

Teorem 3.9. *Za svaki prirodan broj n je*

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

Dokaz. Definirajmo prvo skup $S_d = \{m \in \mathbb{Z} : 1 \leq m \leq n, (m,n) = d\}$. Tada vrijedi

$$\begin{aligned} (m,n) = d &\iff \text{postoje } x, y \in \mathbb{Z} \text{ takvi da je } xm + yn = d \\ &\iff \text{postoje } x, y \in \mathbb{Z} \text{ takvi da je } x\frac{m}{d} + y\frac{n}{d} = 1 \\ &\iff \left(\frac{m}{d}, \frac{n}{d}\right) = 1. \end{aligned}$$

Po definiciji Eulerove funkcije slijedi $|S_d| = \varphi(\frac{n}{d})$. Iz definicije S_d vidimo da za svaki m, $1 \leq m \leq n$ postoji d za koji vrijedi $(m,n) = d$ pa prema tome svaki broj između 1 i n pripada nekom od skupova S_d, tj. vrijedi

$$\{1, 2, \ldots, n\} = \bigcup_{d|n} S_d.$$

Budući da su za različite djelitelje broja n skupovi S_d međusobno disjunktni, odnosno $d_i \neq d_j \iff S_{d_i} \neq S_{d_j}$, vrijedi sljedeće :

$$n = |\{1, 2, \ldots, n\}| = \left|\bigcup_{d|n} S_d\right| = \sum_{d|n} |S_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d).$$

□

Definicija 3.5. *Funkciju $f : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*

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

zovemo multiplikativna funkcija.

Teorem 3.10. *Eulerova funkcija je multiplikativna.*

Primjer 3.4. *Brojevi 6 i 7 su relativno prosti i vrijedi $\varphi(6) = 2$, $\varphi(7) = 6$. Primjenom muliplikativnosti Eulerove funkcije dobivamo $\varphi(42) = \varphi(6) \cdot \varphi(7) = 2 \cdot 6 = 12$.*

Multiplikativnost je najvažnije svojstvo Eulerove funkcije koje će nam koristiti u kreiranju metode za lakše određivanje vrijednosti funkcije φ posebno u slučaju velikih brojeva.

Teorem 3.11. *Neka je p prost broj i $\alpha \in \mathbb{N}$. Tada je $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Dokaz. Od p^α prirodnih brojeva koji su jednaki ili manji od p^α njih $p^{\alpha-1}$ nisu relativno prosti s p^α. To su sljedeći višekratnici broja p: $p, 2p, \ldots, (p^{\alpha-1}-1)p, p^{\alpha-1}p$. Prema tome je $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. □

Primjer 3.5. *Odredimo koliko je* $\varphi(21^9)$.
$\varphi(21^9) = \varphi((3 \cdot 7)^9) = \varphi(3^9) \cdot \varphi(7^9) = 3^8(3-1)7^8(7-1) = 12 \cdot 21^8$.

Neka je $n > 1$ prirodan broj. Prikažimo n u obliku $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Tada je

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1}(1 - \frac{1}{p_1}) p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) \\
&= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).
\end{aligned}$$

Teorem 3.12 (Eulerov teorem). *Neka je* $a \in \mathbb{Z}$, $m \in \mathbb{N}$. *Ako je* $(a, m) = 1$, *tada je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz. Neka brojevi $a_1, a_2, \dots, a_{\varphi(m)}$ čine reducirani sustav ostataka modulo m. Budući su a i m relativno prosti, prema teoremu 3.8 brojevi $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\varphi(m)}$ također čine reducirani sustav ostataka modulo m. Prema tome, za svaki i, $1 \leq i \leq \varphi(m)$, postoji j, $1 \leq j \leq \varphi(m)$, tako da je $a \cdot a_i \equiv a_j \pmod{m}$. Iz toga je

$$\prod_{i=1}^{\varphi(m)} a \cdot a_i \equiv \prod_{j=1}^{\varphi(m)} a_j \pmod{m},$$

odnosno

$$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} a_i \equiv \prod_{j=1}^{\varphi(m)} a_j \pmod{m}.$$

Budući je $(a_i, m) = 1$ za $1 \leq i \leq \varphi(m)$, prema korolaru 3.1 je $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Korolar 3.2 (Mali Fermatov teorem). *Ako je* p *prost broj i* $(a, p) = 1$, *tada je* $a^{p-1} \equiv 1 \pmod{p}$.

Primjer 3.6. *Neka je* n *prirodan broj. Dokažimo da je* $\varphi(n) = \frac{n}{2}$ *ako i samo ako je* $n = 2^k$ *za* $k \in \mathbb{N}$.
Neka je $n = 2^k$ *za* $k \in \mathbb{N}$. *Tada je broj prirodnih brojeva koji nisu veći od* 2^k *i koji su relativno prosti s* 2^k *jednak broju neparnih brojeva u nizu* $1, 2, \dots, 2^k$. *Takvih brojeva ima* $\frac{n}{2}$. *Obratno, pretpostavimo da je* $\varphi(n) = \frac{n}{2}$. *Tada je* n *paran, odnosno* n *je oblika* $2^k \cdot g$, *gdje je* g *neparan broj. Primjenom multiplikativnosti Eulerove funkcije imamo* $\varphi(n) = 2^{k-1} \cdot \varphi(g)$. *Sada je* $2^{k-1} \cdot \varphi(g) = \frac{2^k \cdot g}{2}$, *iz čega slijedi* $\varphi(g) = g$ *što je istinito samo za* $g = 1$. *Prema tome je* $n = 2^k$.

Primjer 3.7. *Odredimo ostatak pri dijeljenju broja* 2017^{30^2} *brojem* 77.
Kako je $(2017, 77) = 1$ *i* $\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$ *prema Eulerovom teoremu slijedi* $2017^{60} \equiv 1 \pmod{77}$. *Prema tome,* $2017^{30^2} = 2017^{900} \equiv (2017^{60})^{15} \pmod{77}$. *Dakle, traženi ostatak je* 1.

3.4 Linearne kongruencije

Definicija 3.6. *Neka su a i b cijeli brojevi i m prirodni broj. Kongruencija oblika $ax \equiv b \pmod{m}$ se naziva linearna kongruencija.*

Idući teorem govori o egzistenciji i broju rješenja linearnih kongruencija.

Teorem 3.13 (Bachetov teorem). *Neka su a i b cijeli brojevi i m prirodni broj te neka je $(a, m) = 1$. Tada postoji jedinstveno rješenje kongruencije $ax \equiv b \pmod{m}$. Ako je $(a, m) = d$ i $d \mid b$, tada postoji d međusobno nekongruentnih rješenja. Ako $d \nmid b$, ne postoji rješenje.*

Dokaz. Pretpostavimo da $d \mid b$. Tada prema teoremu 2.1 postoji $t \in \mathbb{Z}$ takav da je $b = t \cdot d$. Zbog $(a, m) = d$ postoje $r, s \in \mathbb{Z}$ takvi da je $d = ar + ms$. Sada je $b = td = tar + tms$, odnosno, $a(tr) \equiv b \pmod{m}$ iz čega vidimo da je tr rješenje kongruencije $ax \equiv b \pmod{m}$. Neka za x_0 vrijedi $ax_0 \equiv b \pmod{m}$. Tada je $ax_0 - b = km$ za neki $k \in \mathbb{Z}$. Budući da d dijeli a i m, d dijeli i b. Prema kontrapoziciji, ako $d \nmid b$, ne postoji rješenje.
Ako je x_0 rješenje kongruencije $ax \equiv b \pmod{m}$, također je i $x_0 + k\frac{m}{d}$. Naime,

$$a\left(x_0 + k\frac{m}{d}\right) \equiv ax_0 + km\frac{a}{d} \equiv ax_0 \equiv b \pmod{m}, \quad k = 1, 2, \ldots, d-1.$$

□

Primjer 3.8. *Riješimo linearnu kongruenciju $44x \equiv 8 \pmod{29}$.*
Podijelimo li obje strane s 4, prema korolaru 3.1 dobivamo $11x \equiv 2 \pmod{29}$. Pomnožimo li sada obje strane s 8, prema teoremu 3.6 dobivamo $88x \equiv 16 \pmod{29}$. Budući da je $88 \equiv 1 \pmod{29}$, slijedi da je $x \equiv 16 \pmod{29}$ rješenje dane kongruencije.

Primjer 3.9. *Riješimo linearnu kongruenciju $20x \equiv 16 \pmod{64}$.*
Primijetimo da je $(20, 64) = 4$ i $4 \mid 16$ te iz toga slijedi da kongruencija ima 4 međusobno nekongruentna rješenja. Prema teoremu 3.6 iz dane kongruencije slijedi $5x \equiv 4 \pmod{16}$. Pomnožimo li obje strane s 13 dobivamo $65x \equiv 52 \pmod{16}$. Budući je $65 \equiv 1 \pmod{16}$ i $52 \equiv 4 \pmod{16}$, vrijedi $x \equiv 4 \pmod{16}$, odnosno rješenja su: $x \equiv 4 \pmod{64}$, $x \equiv 20 \pmod{64}$, $x \equiv 36 \pmod{64}$ i $x \equiv 52 \pmod{64}$.

Primjer 3.10. *Riješimo linearnu kongruenciju $22x \equiv 5 \pmod{12}$.*
Budući da je $(22, 12) = 2$ i $2 \nmid 5$, dana kongruencija nema rješenja.

Korolarom 2.1 rekli smo kako jednadžbe oblika $ax + by = d$, gdje su $a, b \in \mathbb{Z}$ i $d = (a, b)$, uvijek imaju rješenja. Jednadžbe takvog oblika nazivamo linearne diofantske jednadžbe s dvije nepoznanice. Idući teorem daje uvijete za egzistenciju rješenja spomenute jednadžbe, a koristi se znanjem iz prethodnog teorema.

Teorem 3.14. *Diofantska jednadžba $ax + by = n$ ima rješenje ako i samo ako $d \mid n$, gdje je $(a, b) = d$. Ako je (x_0, y_0) jedno rješenje, sva rješenja su dana s:*

$$\left(x_0 + k\frac{b}{d},\ y_0 - k\frac{a}{d}\right), \quad k \in \mathbb{Z}.$$

Dokaz. Traženje rješenja jednadžbe $ax + by = n$ je ekvivalentno traženju rješenja kongruencije $ax \equiv n \pmod{b}$ ili $by \equiv n \pmod{a}$. Rješenje obje navedene kongruencije postoji ako i samo ako d dijeli n, gdje je $(a, b) = d$.
Neka je x_0 jedno rješenje kongruencije $ax \equiv n \pmod{b}$. Svako rješenje je dano s $x_0 + k\frac{b}{d}$. Doista, neka je $y_0 = \frac{n-ax_0}{b}$, $y = y_0 - k\frac{a}{d}$, $x = x_0 + k\frac{b}{d}$. Tada je

$$n - ax = n - a\left(x_0 - k\frac{b}{d}\right) = b\left(\frac{n - ax_0}{b} - k\frac{a}{d}\right) = b\left(y_0 - k\frac{a}{d}\right) = by\ .$$

□

Primjer 3.11. *Riješimo jednadžbu $4x + 51y = 9$.*
Rješenje možemo dobiti na dva načina.
Budući je $(4, 51) = 1$, pomoću Euklidovog algoritma možemo dobiti brojeve a i b takve da je $4a + 51b = 1$. Ukoliko cijelu jednadžbu pomnožimo s 9, dobivamo jedno rješenje (x_0, y_0) zadane jednadžbe. Sva ostala rješenja su prema prethodnom teoremu dana s
$(x_0 + 51k, y_0 - 4k), \quad k \in \mathbb{Z}$.
Umjesto da rješavamo jednadžbu $4x + 51y = 9$ možemo riješiti jednu od kongruencija $4x \equiv 9 \pmod{51}$ ili $51y \equiv 9 \pmod{4}$. Bez smanjenja općenitosti, riješimo $4x \equiv 9 \pmod{51}$. Množeći obje strane s 13 dobivamo $52x \equiv 117 \pmod{15}$. Budući da je $52 \equiv 1 \pmod{51}$, slijedi da je $x \equiv 117 \pmod{51}$, odnosno $x = 117 + 51k$ za $k \in \mathbb{Z}$. Uvrstimo li x natrag u početnu jednadžbu, vrijedi da je $51y = 9 - 4(51k + 117)$, odnosno $y = -9 - 4k$ za $k \in \mathbb{Z}$.

Primjer 3.12. *Podijelimo broj 100 u dva dijela. Jedan dio neka je djeljiv brojem 7, a drugi dio neka je djeljiv brojem 11. Odrediti te dijelove.*
Trebamo naći barem jedno rješenje jednadžbe $7x + 11y = 100$. Slično kao u prethodnom primjeru riješit ćemo kongruenciju $7x \equiv 100 \pmod{11}$. Budući da je $100 \equiv 1 \mod 11$, imamo da je $7x \equiv 1 \pmod{11}$. Pomnožimo li obje strane brojem 8, slijedi da je $x \equiv 8 \pmod{11}$, odnosno $x = 11k + 8$ iz čega je $y = 4 - 7k$, $k \in \mathbb{Z}$. Za $k = 0$ vrijedi $100 = 44 + 56$.

Idući rezultat veže se uz kineskog matematičara Sun-Tza, a govori o rješenju sustava linearnih kongruencija.

Teorem 3.15 (Kineski teorem o ostacima). *Neka su $m_1, m_2, \ldots, m_k$ u parovima relativno prosti prirodni brojevi te neka su $a_1, a_2, \ldots a_k$ cijeli brojevi. Tada sustav linearnih kongruencija $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq k$, ima jedinstveno rješenje modulo $m = \prod_{i=1}^{k} m_i$.*

Dokaz. Označimo $M_i = \frac{m}{m_i}$ i $m = \prod_{i=1}^{k} m_i$ te neka su $b_i \in \mathbb{Z}$ takvi da je $M_i b_i \equiv 1 \pmod{m_i}$. Imamo da je $m_j \mid M_i$ i $(m_i, m_j) = 1$ za $i \neq j$. Iz $(m_i, M_i) = 1$ prema teoremu 3.13 slijedi da kongruencija $M_i y \equiv 1 \pmod{m_i}$ ima jedinstveno rješenje b_i za svaki $1 \leq i \leq k$. Dakle, za

svaki i postoji jedinstveni $b_i \in \mathbb{Z}$ takav da je $M_i b_i \equiv 1 \pmod{m_i}$.
Neka je

$$x_0 \equiv \sum_{i=1}^{k} M_i b_i a_i \pmod{m}.$$

Budući da vrijedi $M_i b_i a_i \equiv a_i \pmod{m_i}$ i $M_i \equiv 0 \pmod{m_j}$ za $i \neq j$, slijedi da je
$x_0 \equiv a_i \pmod{m_i}$ za $i = 1, 2, \ldots, k$.
Nadalje, pretpostavimo da je x_0 rješenje danog sustava linearnih kongruencija te pretpostavimo da je x_1 još jedno rješenje različito od x_0. Prema tome vrijedi $x_0 \equiv x_1 \equiv a_i \pmod{m_i}$, odnosno $m_i \mid x_1 - x_0$ za svaki $i = 1, 2, \ldots, k$. Kako je $(m_i, m_j) = 1$ za $i \neq j$, prema korolaru 2.2 slijedi da $m \mid x_1 - x_0$, odnosno $x_1 \equiv x_0 \pmod{m}$ iz čega zaključujemo da, ukoliko rješenje postoji, ono je jedinstvno modulo m. □

Problem naveden u idućem primjeru je jedan od povijesnih problema riješenih metodom iz prethodnog teorema.

Primjer 3.13. *Žena je otišla na tržnicu. Konj je stao u njezinu korpu i zgazio jaja u korpi. Vlasnik konja ponudio je platiti prouzročenu štetu. Pitao je ženu koliko jaja je kupila. Žena nije znala odgovor na to pitanje, ali je znala sljedeće: ukoliko uzima* 2 *po* 2*, ostane jedno na kraju, isto se dogodi i ako uzima po* $3, 4, 5$ *i* 6 *jaja te ako se uzima po* 7 *jaja, ne ostane niti jedno jaje. Koji je najmanji broj jaja koji bi žena mogla imati?*
Odgovor na to pitanje daje rješenje sustava kongruencija

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{6} \\ x &\equiv 0 \pmod{7}. \end{aligned}$$

Uočimo da brojevi $2, 3, 4$ *i* 6 *nisu svi u parovima relativno prosti pa ne možemo Kineski teorem o ostacima primijeniti direktno. Najmanji zajednički višekratnik brojeva* $2, 3, 4$ *i* 6 *je* 12 *te se dani sustav može reducirati na sljedeći sustav kongruencija:*

$$\begin{aligned} x &\equiv 1 \pmod{12} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 0 \pmod{7}. \end{aligned}$$

Sada su brojevi $12, 5$ *i* 7 *u parovima relativno prosti te prema oznakama iz dokaza prethodnog teorema neka je* $m = 12 \cdot 5 \cdot 7 = 420$. *Tada su*

$$\begin{aligned} m_1 = 12 \qquad m_2 = 5 \qquad m_3 = 7 \\ a_1 = 1 \qquad a_2 = 1 \qquad a_3 = 0 \\ M_1 = 35 \qquad M_2 = 84 \qquad M_3 = 60. \end{aligned}$$

Riješimo sljedeće kongruencije za b_1, b_2 *i* b_3*:*

$$\begin{aligned} 35b_1 \equiv 1 \pmod{12} \qquad 84b_2 \equiv 1 \pmod{5} \qquad 60b_3 \equiv 1 \pmod{7} \\ 11b_1 \equiv 1 \pmod{12} \qquad 4b_2 \equiv 1 \pmod{5} \qquad 4b_3 \equiv 1 \pmod{7} \\ b_1 \equiv 11 \pmod{12} \qquad b_2 \equiv 4 \pmod{5} \qquad b_3 \equiv 2 \pmod{7}. \end{aligned}$$

Prema tome je

$$x \equiv \sum_{i=1}^{3} M_i b_i a_i \equiv 35 \cdot 1 \cdot 11 + 84 \cdot 1 \cdot 4 + 60 \cdot 0 \cdot 2 \equiv 721 \equiv 301 \pmod{420}.$$

Dakle, najmanji broj jaja koji bi žena mogla imati je 301.

4 Polinomijalne kongruencije

Definicija 4.1. *Neka je m prirodan broj te neka je f polinom s cjelobrojnim koeficijentima. Tada se kongruencija oblika $f(x) \equiv 0 \pmod{m}$ naziva polinomijalna kongruencija.*

Teorem 4.1. *Neka je $m = \prod_{i=1}^{k} m_i$ te $(m_i, m_j) = 1$ za $1 \leq i < j \leq k$. Tada je svako rješenje polinomijalne kongruencije $f(x) \equiv 0 \pmod{m}$ ujedno i rješenje sustava $f(x) \equiv 0 \pmod{m_i}$ za $i = 1, 2, \ldots, k$. Vrijedi i obratno.*

Dokaz. Pretpostavimo da za neki x_0 vrijedi $f(x_0) \equiv 0 \pmod{m}$.
Budući da $m_i \mid m$, vrijedi $f(x_0) \equiv 0 \pmod{m_i}$ za $i = 1, 2, \ldots, k$. Dakle, svako rješenje kongruencije $f(x) \equiv 0 \pmod{m}$ je ujedno i rješenje sustava $f(x) \equiv 0 \pmod{m_i}$, $1 \leq i < j \leq k$.
Obratno, pretpostavimo da je $f(x_0) \equiv 0 \pmod{m_i}$ za $1 \leq i < j \leq k$. Tada $m_i \mid f(x_0)$ za svaki $i = 1, 2, \ldots, k$. Budući da je $(m_i, m_j) = 1$ za $i \neq j$, slijedi da $m \mid f(x_0)$, odnosno $f(x_0) \equiv 0 \pmod{m}$. □

Prikažimo prirodan broj n u obliku $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, gdje su $k \in \mathbb{N}$, $p_1, p_2, \ldots, p_k \in \mathbb{N}$ različiti prosti brojevi te $\alpha_i \in \mathbb{N}$. Prema prethodnom teoremu vrijedi da je $f(x) \equiv 0 \pmod{n}$ ako i samo ako je $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \ldots, k$.
Neka je x_i rješenje sustava $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \ldots, k$. Prema Kineskom teoremu o ostacima, sustav linearnih kongruencija

$$x \equiv x_i \pmod{p_i^{\alpha_i}}, 1 \leq i \leq k$$

ima jedinstveno rješenje modulo n. Budući da $x \equiv x_i \pmod{p_i^{\alpha_i}}$ povlači
$f(x) \equiv f(x_i) \pmod{p_i^{\alpha_i}}$, x je rješenje polinomijalne kongruencije $f(x) \equiv 0 \pmod{n}$. Upravo smo pokazali ideju dokaza sljedeće tvrdnje.

Teorem 4.2. *Broj rješenja kongruencije $f(x) \equiv 0 \pmod{n}$, gdje je $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, jednak je produktu broja rješenja kongruencija $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \ldots, k$.*

Sva nekongruentna rješenja polinomijalne kongruencije $f(x) \equiv 0 \pmod{m}$ možemo odrediti provjerom zadovoljavaju li elementi nekog potpunog sustava ostataka modulo m danu kongruenciju. Najčešće se kao potpun sustav ostataka modulo m koristi skup $\{0, 1, 2, \ldots, m-1\}$.

Primjer 4.1. *Riješimo kongruenciju $x^3 + 3x - 4 \equiv 0 \pmod{5}$.*
Za svaki od elemenata iz skupa $\{0, 1, 2, 3, 4\}$ provjerit ćemo zadovoljavaju li danu kongruenciju: $f(0) \equiv 1 \pmod{5}$, $f(1) \equiv 0 \pmod{5}$, $f(2) \equiv 0 \pmod{5}$, $f(3) \equiv 2 \pmod{5}$, $f(4) \equiv 2 \pmod{5}$. Dakle, rješenja kongruencije $x^3 + 3x - 4 \equiv 0 \pmod{5}$ su $x \equiv 1 \pmod{5}$ i $x \equiv 2 \pmod{5}$.

Primjetimo kako se u prethodnom teoremu pojavljuje problem kongruencije modulo p^α, gdje je p prost broj. Sljedeći rezultat pokazuje da je rješenje $f(x) \equiv 0 \pmod{p^\alpha}$ generirano rješenjem kongruencije $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.

Teorem 4.3. *Neka je f polinom s cjelobrojnim koeficijentima, p prost broj i $\alpha \in \mathbb{N}$. Ako je $x_{\alpha+1} = x_\alpha + k \cdot p^\alpha$, gdje je x_α rješenje kongruencije $f(x) \equiv 0 \pmod{p^\alpha}$ te k rješenje kongruencije $\frac{f(x_\alpha)}{p^\alpha} + k \cdot f'(x_\alpha) \equiv 0 \pmod{p}$, $0 \leq x_\alpha < p^\alpha$, $0 \leq k < p$ pri čemu f' označava derivaciju funkcije f. Tada je $x_{\alpha+1}$ rješenje kongruencije $f(x) \equiv 0 \pmod{p^{\alpha+1}}$.*

Dokaz. Neka je p prost broj. Ako $p^{\alpha+1} \mid a$, tada $p^\alpha \mid a$. Stoga je svako rješenje kongruencije $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ također rješenje kongruencije $f(x) \equiv 0 \pmod{p^\alpha}$. Preciznije, ako je $f(x_{\alpha+1}) \equiv 0 \pmod{p^{\alpha+1}}$, tada postoji x_α takav da je $f(x_\alpha) \equiv 0 \pmod{p^\alpha}$ i vrijedi $x_{\alpha+1} \equiv x_\alpha \pmod{p^\alpha}$ ili ekvivalentno $x_{\alpha+1} = x_\alpha + k \cdot p^\alpha$, $0 \leq k < p$.
Razvojem u Taylorov red dobivamo $f(x_{\alpha+1}) = f(x_\alpha + k \cdot p^\alpha) = f(x_\alpha) + k \cdot p^\alpha \cdot f'(x_\alpha) + k^2 \cdot N$, gdje je N cijeli broj djeljiv s $p^{\alpha+1}$. Iz toga slijedi da je $f(x_\alpha) + k \cdot p^\alpha \cdot f'(x_\alpha) \equiv 0 \pmod{p^{\alpha+1}}$. Kako je $f(x_\alpha) \equiv 0 \pmod{p^\alpha}$, $\frac{f(x_\alpha)}{p^\alpha} = M$ je cijeli broj. Tada $f(x_\alpha) = M \cdot p^\alpha$ implicira $M \cdot p^\alpha + k \cdot p^\alpha \cdot f'(x_\alpha) \equiv 0 \pmod{p^{\alpha+1}}$. Djeljenjem s p^α slijedi $M + k \cdot f'(x_\alpha) \equiv 0 \pmod{p}$, odnosno $\frac{f(x_\alpha)}{p^\alpha} + k \cdot f'(x_\alpha) \equiv 0 \pmod{p}$. □

Primjer 4.2. *Riješimo kongruenciju $5x^3 - 2x + 1 \equiv 0 \pmod{343}$.*
Budući je $343 = 7^3$, možemo pisati $5x^3 - 2x + 1 \equiv 0 \pmod{7^3}$. Stavimo prvo $f(x) = 5x^3 - 2x + 1$ iz čega slijedi da je $f'(x) = 15x^2 - 2$.
Prethodni teorem nam govori kako je rješenje kongruencije $5x^3 - 2x + 1 \equiv 0 \pmod{7^3}$ generirano rješenjem kongruencije $5x^3 - 2x + 1 \equiv 0 \pmod{7^2}$ dok je ono pak generirano rješenjem kongruencije $5x^3 - 2x + 1 \equiv 0 \pmod{7}$.
Kongruencija $5x^3 - 2x + 1 \equiv 0 \pmod{7}$ ima jedinstveno rješenje modulo 7; $x_1 \equiv 5 \pmod{7}$. Prema teoremu, $x_2 = x_1 + k \cdot 7$ je rješenje kongruencije $5x^3 - 2x + 1 \equiv 0 \pmod{7^2}$. Dakle, da bi smo izračunali koliko je x_2, moramo pronaći k, odnosno riješiti $\frac{f(x_1)}{7} + k \cdot f'(x_1) \equiv 0 \pmod{7}$. Nakon uvrštavanja i računanja dobit ćemo da je $k \equiv 5 \pmod{7}$ te je iz toga $x_2 = 5 + 5 \cdot 7 = 40$. Sada primjenimo sličan postupak za traženje rješenja kongruencije $5x^3 - 2x + 1 \equiv 0 \pmod{7^3}$; $x_3 = x_2 + k \cdot 7^2$, gdje je k rješenje kongruencije $\frac{f(x_2)}{7^2} + k \cdot f'(x_2) \equiv 0 \pmod{7}$. Konačno rješenje je $x_3 = 40 + 1 \cdot 7^2 = 89$.

U idućim razmatranjima bavit ćemo se problemom traženja rješenja polinomijalne kongruencije $f(x) \equiv 0 \pmod{p}$ kada je p prost broj. U 18. st. je Lagrange dao gornju granicu broja rješenja polinomijalne kongruencije $f(x) \equiv 0 \pmod{p}$ te pokazao njenu ovisnost o stupnju polinoma f.

Teorem 4.4 (Lagrangeov teorem). *Neka je p prost broj. Broj nekongruentnih rješenja polinomijalne kongruencije $f(x) \equiv 0 \pmod{p}$ nije veći od stupnja polinoma f.*

Dokaz. Neka je dana kongruencija $f(x) \equiv 0 \pmod{p}$, gdje je p prost broj i označimo s n stupanj polinoma f. Dokaz ćemo provesti indukcijom po n.
Za $n = 1$ promotrimo kongruenciju $ax + b \equiv 0 \pmod{p}$, gdje je $a \not\equiv 0 \pmod{p}$.
Iz $ax \equiv -b \pmod{p}$ i $(a, p) = 1$ prema teoremu 3.13 slijedi da kongruencija ima jedinstveno rješenje. Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja manjeg ili jednakog n. Razmotrimo kongruenciju $f(x) \equiv 0 \pmod{p}$, gdje je f polinom stupnja $n + 1$ te pretpostavimo da postoje $n + 2$ nekongruentna rješenja modulo p. Neka je r jedno rješenje. Slijedi

da je $f(x) = g(x)(x-r)$, g polinom stupnja n. Ako je s neko drugo rješenje kongruencije $f(x) \equiv 0 \pmod{p}$, tada vrijedi $f(s) \equiv g(s)(s-r) \equiv 0 \pmod{p}$. Po pretpostavci je $s - r \not\equiv 0 \pmod{p}$ te vrijedi $(s-r, p) = 1$, p prost. Stoga je $g(s) \equiv 0 \pmod{p}$, odnosno s je rješenje kongruencije $f(x) \equiv 0 \pmod{p}$. Dobili smo da polinomijalna kongruencija stupnja n ima $n+1$ rješenje, što je u kontradikciji s pretpostavkom indukcije. □

Idući teorem daje zanimljiv kriterij za određivanje je li broj prost ili nije.

Teorem 4.5 (**Wilsonov teorem**). *Prirodan broj n je prost ako i samo ako je $(n-1)! \equiv -1 \pmod{n}$.*

Dokaz. Pretpostavimo da je p prost broj. Definirajmo polinom

$$f(x) = x^{p-1} - 1 - (x-1)(x-2)\cdot\ldots\cdot(x-(p-1)) = x^{p-1} - 1 - \prod_{k=1}^{p-1}(x-k).$$

Ako uvrstimo $x = a$ za $a \in \{1, 2, \ldots, p-1\}$ u gornji produkt, jedan od faktora će dati nulu. Prema tome, za $a \in \{1, 2, \ldots, p-1\}$ prema Malom Fermatovom teoremu vrijedi

$$f(a) = a^{p-1} \equiv 1 - 1 = 0 \pmod{p}.$$

Budući da je stupanj polinoma f manji od $p-1$, a kongruencija $f(x) \equiv 0 \pmod{p}$ ima $p-1$ nekongruentnih rješenja modulo p, svaki koeficijent polinoma f je višekratnik broja p te za $x = 0$ imamo

$$f(0) \equiv 0 \pmod{p},$$

odnosno

$$0 \equiv f(0) = -1 - \prod_{k=1}^{p-1}(-k) = -1 - (-1)^{p-1}\prod_{k=1}^{p-1} k.$$

Ako je p neparan prost broj, tada je $(-1)^{p-1} \equiv 1 \pmod{p}$ te ako je $p = 2$, tada je $(-1)^{p-1} \equiv -1 \equiv 1 \pmod{p}$. Dakle, za svaki prost broj je $(p-1)! \equiv -1 \pmod{p}$.
Obratno, ako je n složen broj, tada postoji cijeli broj d, $1 \leq d \leq n$ takav da $d \mid n$. Tada $d \mid (n-1)!$ odnosno $(n-1)! \equiv 0 \pmod{d}$ iz čega slijedi $(n-1) \not\equiv -1 \pmod{n}$. □

Primjer 4.3. *Nađimo ostatak pri dijeljenju broja* $15!$ *sa* 17.
Prema teoremu 4.5 *vrijedi* $16! \equiv -1 \pmod{17}$ *iz čega je* $16 \cdot 15! \equiv -1 \equiv 16 \pmod{17}$. *Budući da su* 16 *i* 17 *relativno prosti, tada je* $15! \equiv 1 \pmod{17}$.

Primjer 4.4. *Neka je p prost broj veći od* 2. *Pokažimo da je* $2 \cdot 4 \cdot 6 \cdots (2p-2) \equiv -1 \pmod{p}$.
Primijetimo da je $2 \cdot 4 \cdot 6 \cdots (2p-2) = (2\cdot 1)(2\cdot 2)(2\cdot 3)\cdots 2\cdot(p-1) = 2^{p-1}\cdot(p-1)!$. *Prema teoremu* 4.5 *imamo da je* $(p-1)! \equiv -1 \pmod{p}$, *dok prema teoremu* 3.2 *vrijedi* $2^{p-1} \equiv 1 \pmod{p}$. *Množenjem ovih kongruencija dobivamo* $2 \cdot 4 \cdot 6 \cdots (2p-2) \equiv -1 \pmod{p}$.

Primjer 4.5. *Riješimo kongruenciju* $x^4 + x + 2 \equiv 0 \pmod{7}$.
Za svaki od elemenata iz skupa $\{0, 1, 2, 3, 4, 5, 6\}$ *provjerit ćemo zadovoljavaju li danu kongruenciju:* $f(0) \equiv f(3) \equiv f(5) \equiv f(6) \equiv 2 \pmod{7}$, $f(1) \equiv 4 \pmod{7}$, $f(2) \equiv 6 \pmod{7}$, $f(4) \equiv 3 \pmod{7}$. *Vidimo da kongruencija* $x^4 + x + 2 \equiv 0 \pmod{7}$ *nema rješenja.*

Primjer 4.6. *Riješimo sustav kongruencija*

$$\begin{aligned} 5x^2+4x-3 &\equiv 0 \pmod 6 \\ 3x^2+10 &\equiv 0 \pmod{17}. \end{aligned}$$

Rješenje prve konguencije je $x \equiv 1,3 \pmod 6$*, a druge* $x \equiv 5,12 \pmod{17}$ *pa rješavamo sljedeće sustave:*

$$\begin{array}{cccc} x \equiv 1 \pmod 6 & x \equiv 1 \pmod 6 & x \equiv 3 \pmod 6 & x \equiv 3 \pmod 6 \\ x \equiv 5 \pmod{17} & x \equiv 12 \pmod{17} & x \equiv 5 \pmod{17} & x \equiv 12 \pmod{17}. \end{array}$$

Primjenom Kineskog teorema o ostacima dobivamo da su rješenja ovih sustava $x \equiv 39 \pmod{102}$*,* $x \equiv 63 \pmod{102}$*,* $x \equiv 73 \pmod{102}$ *i* $x \equiv 97 \pmod{102}$*.*

Primjer 4.7. *Riješimo kongruenciju* $x^3+3x^2-4 \equiv 0 \pmod{175}$*.*
Budući da je $175 = 7 \cdot 5^2$*, rješenje dane kongruencije je ekvivalentno rješenju sustava*

$$\begin{aligned} x^3+3x^2-4 &\equiv 0 \pmod 7 \\ x^3+3x^2-4 &\equiv 0 \pmod{5^2}. \end{aligned}$$

Da bismo riješili prvu kongruenciju, provjerit ćemo koje vrijednosti iz skupa $\{0,1,2,3,4,5,6\}$ *zadovoljavaju kongruenciju. Dobit ćemo da je* $x \equiv 1 \pmod 7$ *i* $x \equiv 5 \pmod 7$*.*
Kako bismo riješili drugu kongruenciju stavimo $f(x) = x^3+3x^2-4$ *iz čega slijedi da je* $f'(x) = 3x^2+6x$*. Kongruencija* $x^3+3x^2-4 \equiv 0 \pmod 5$ *ima dva rješenja modulo* 5*;* $x \equiv 1 \pmod 5$ *i* $x \equiv 3 \pmod 5$*. Računamo li dalje na sličan način kao u primjeru* 4.2*, dobit ćemo da kongruencija* $x^3+3x^2-4 \equiv 0 \pmod{25}$ *ima šest različitih rješenja modulo* 25*;* $x \equiv 1,3,8,13,18,23 \pmod{25}$*.*
Prema tome, za $a_i \in \{1,3,8,13,18,23\}$ *računat ćemo* 12 *sustava linearnih kongruencija*

$$\begin{array}{cc} x \equiv 1 \pmod 7 & x \equiv 5 \pmod 7 \\ x \equiv a_i \pmod{25} & x \equiv a_i \pmod{25}. \end{array}$$

te koristeći Kineski teorem o ostacima dobiti 12 *različitih rješenja modulo* 175*. Rješenja su* $x \equiv 1,8,26,33,43,68,78,103,113,138,148,173 \pmod{175}$*.*

5 Kvadratne kongruencije

U prethodnom poglavlju smo pokazali da rješenje kongruencije $ax^2 + bx + c \equiv 0 \pmod{m}$ ovisi o rješenju kongruencije $ax^2 + bx + c \equiv 0 \pmod{p}$, gdje je p prost broj i $p \mid m$. Neka je p neparan prost broj te $(a, p) = 1$. Tada je i $(4a, p) = 1$. Ako $ax^2 + bx + c \equiv 0 \pmod{p}$ pomnožimo s obje strane s 4, dobivamo $4ax^2 + 4bx + 4c \equiv 0 \pmod{p}$ što možemo zapisati kao $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$. Prema tome, da bi riješili kvadratnu jednadžbu $ax^2 + bx + c = 0$ modulo p, potrebno je naći rješenje kongruencije

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

gdje je y rješenje kongruencije

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

Primjer 5.1. *Riješimo kogruenciju* $5x^2 + 4x + 7 \equiv 0 \pmod{19}$.
Prvo računamo $y^2 \equiv b^2 - 4ac = 16 - 4 \cdot 5 \cdot 7 \equiv 9 \pmod{19}$. *Budući je* $3^2 \equiv 16^2 \equiv 9 \pmod{19}$, *dobivamo da je* $y \equiv 3 \pmod{19}$ *i* $y \equiv 16 \pmod{19}$. *Iz* $y \equiv 3 \pmod{19}$ *slijedi da je* $2ax + b = 10x + 4 \equiv 3 \pmod{19}$ *odakle slijedi* $x \equiv 17 \pmod{19}$. *Slično, iz* $y \equiv 16 \pmod{19}$ *slijedi da je* $2ax + b = 10x + 4 \equiv 16 \pmod{19}$ *odakle vrijedi* $x \equiv 5 \pmod{19}$.

Pred nama su sada dva cilja. Prvi je otkriti koje kongruencije oblika $x^2 \equiv a \pmod{p}$ imaju rješenje za neparan prost broj p, a drugi je pronaći metodu za rješavanje takvih kongruencija.

Definicija 5.1. *Neka su* a *i* p *relativno prosti prirodni brojevi te* $n \in \mathbb{N}$. *Ako kongruencija* $x^n \equiv a \pmod{p}$ *ima rješenja, tada kažemo da je* a *ostatak* n*-tog stupnja modulo* p. *U suprotnom kažemo da je* a *neostatak* n*-tog stupnja modulo* p.

Specijalno, za $n = 2$ kažemo da je a kvadratni ostatak, odnosno kvadratni neostatak.
Broj 0 smatramo trivijalnim kvadratnim ostatakom za svaki prost broj p.

Primjer 5.2. *Prirodni brojevi* $1, 4$ *i* 7 *su kvadratni ostaci modulo* 9, *a brojevi* $2, 3, 5, 6$ *i* 8 *kvadratni neostaci modulo* 9. *Primijetimo da brojevi* 3 *i* 6 *nisu relativno prosti s* 9 *te iz toga odmah možemo zaključiti da su kvadratni ostaci modulo* 9.

Definicija 5.2. *Neka je* p *neparan prost broj i* a *cijeli broj. Legendreov simbol* $\left(\frac{a}{p}\right)$ *definira se na sljedeći način:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \textit{ ako je } a \textit{ kvadratni ostatak modulo } p \\ -1 & , \textit{ ako } a \textit{ nije kvadratni ostatak modulo } p \ . \end{cases}$$

Idući teorem pokazuje kako polovica brojeva između 1 i $p-1$ čini kvadratne ostatke modulo p, dok druga polovica čini kvadratne neostatke.

Teorem 5.1. *Neka je* p *paran prost broj. Tada postoji točno* $\frac{p-1}{2}$ *međusobno nekongruentnih kvadratnih ostataka modulo* p.

Dokaz. Neka je p neparan prost broj.
Želimo odrediti sve a, $1 \leq a \leq p-1$, za koje $x^2 \equiv a \pmod{p}$ ima rješenje.
Budući da vrijedi $x^2 \equiv (p-x)^2 \equiv a \pmod{p}$, kvadrati brojeva iz skupova $\{1, 2, \ldots, \frac{p-1}{2}\}$ i $\{\frac{p-1}{2}+1, \ldots, p-1\}$ su u parovima međusobno kongruentni. Prema tome, dovoljno je ispitati svaki x iz skupa $\{1, 2, \ldots, \frac{p-1}{2}\}$. Kvadrati $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ su svi međusobno nekongruentni modulo p jer bi u suprotnom kongruencija $x^2 \equiv a \pmod{p}$ imala četiri rješenja, što je u kontradikciji s Lagrangeovim teoremom. Dakle, u nizu $1, 2, \ldots, p-1$ postoji $\frac{p-1}{2}$ kvadratnih ostataka modulo p koje čine oni članovi koji su kongruentni s $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ modulo p.
□

Uz činjenice iz prethodnog teorema i dalje je nepraktično određivati je li neki broj kvadratni ostatak modulo p za velike proste brojeve. Jednu od prvih metoda za rješavanje spomenutog problema razvio je Euler 1755. godine.

Lema 5.1. *Neka je p neparan prost broj te $(a, p) = 1$. Tada je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ili $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$*

Dokaz. Prema Malom Fermatovom teoremu, ako je p neparan prost broj i $(a, p) = 1$, tada je $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$. Iz toga slijedi $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ili $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Teorem 5.2 (Eulerov kriterij). *Neka je p neparan prost broj te $(a, p) = 1$. Tada je*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Dokaz. Pretpostavimo da je p neparan prost broj i $(a, p) = 1$ te neka je $1 \leq r \leq p-1$. Kongruencija $rx \equiv a \pmod{p}$ prema teoremu 3.13 ima jedinstveno rješenje. To znači da postoji s, $1 \leq s \leq p-1$ takav da je $rs \equiv a \pmod{p}$. Ukoliko a nije kvadratni ostatak modulo p, mora vrijediti $r \not\equiv s \pmod{p}$ te se elementi skupa $\{1, 2, \ldots, p-1\}$ mogu grupirati u parove $r_i s_i$ tako da je $r_i s_i \equiv a \pmod{p}$ za $i = 1, 2, \ldots, \frac{p-1}{2}$. Prema Wilsonovom teoremu sada vrijedi sljedeće:

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i s_i \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Ako je a kvadratni ostatak modulo p, tada postoji cijeli broj b takav da je $b^2 \equiv a \pmod{p}$. Prema Malom Fermatovom teoremu, $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$.
Vidimo da iz ova dva slučaja slijedi

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

□

Korolar 5.1. *Neka je p neparan prost broj, $(a, p) = 1, (b, p) = 1$ te $a \equiv b \pmod{p}$. Tada je*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Primjer 5.3. *Prema Eulerovom kriteriju odredimo*

$$\left(\frac{3}{19}\right) \equiv 3^{\frac{19-1}{2}} \equiv 3^9 \equiv -1 \pmod{19},$$

$$\left(\frac{6}{19}\right) \equiv 6^{\frac{19-1}{2}} \equiv 6^9 \equiv \quad 1 \pmod{19}.$$

Dakle, kongruencija $x^2 \equiv 3 \pmod{19}$ *nema, dok* $x^2 \equiv 6 \pmod{19}$ *ima rješenja.*

Pokažimo još nekoliko rezultata koji opisuju korisna svojstva Legendreovih simbola.

Teorem 5.3. *Ako je* p *neparan prost broj, tada je*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & , \text{ ako je } p \equiv 1 \pmod{4} \\ -1 & , \text{ ako je } p \equiv 3 \pmod{4}. \end{cases}$$

Dokaz. Ako je $p = 4k + 1$, tada je

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1.$$

Ako je $p = 4k + 3$, tada je

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1.$$

□

Teorem 5.4. *Ako je* p *neparan prost broj i* $p \nmid ab$*, tada je*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Dokaz.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

□

Korolar 5.2. *Neka je* p *neparan prost broj,* $(a, p) = 1$ *te* $n = \prod_{i=1}^{r} p_i^{\alpha_i}$*. Tada je*

$$\left(\frac{n}{p}\right) = \prod_{i=1}^{r} \left(\frac{p_i^{\alpha_i}}{p}\right) = \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i}.$$

Idući teorem daje vrlo efikasnu metodu za određivanje je li neki cijeli broj kvadratni ostatak modulo p.

Teorem 5.5 (Gaussova lema). *Neka je* p *neparan broj i* $(a, p) = 1$*. Promotrimo brojeve* $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ *te njihove najmanje nenegativne ostatke pri dijeljenju s* p*. Označimo sa* s *broj ostataka koji su veći od* $\frac{p}{2}$*. Tada je* $(\frac{a}{p}) = (-1)^s$*.*

Dokaz. Neka S označava skup najmanjih nenegativnih ostataka modulo p elemenata iz skupa $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. Nadalje, neka je s broj elemenata skupa S koji su veći od $\frac{p}{2}$ te označimo $r = \frac{p-1}{2} - s$. Označimo s $a_1, a_2, \ldots, a_r$ elemente iz S koji su manji od $\frac{p}{2}$ i $b_1, b_2, \ldots, b_s$ elemente iz S koji su veći od $\frac{p}{2}$. Brojevi $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s$ su svi međusobno različiti po teoremu 3.7 niti jedan od njih nije nula. Tada su i brojevi $p - b_i$ svi međusobno različiti i $0 < p - b_i < \frac{p}{2}$ za $i = 1, 2, \ldots, s$.
Također, niti jedan $p - b_i$ nije jednak nekom a_j. Zaista, ako je $p - b_i = a_j$, onda je $b_i \equiv \alpha a \pmod{p}$, $a_j \equiv \beta a \pmod{p}$ za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$ pa iz $a(\alpha + \beta) \equiv 0 \pmod{p}$ i $(a, p) = 1$ slijedi $\alpha + \beta \equiv 0 \pmod{p}$ što je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$.
Prema tome, brojevi $p - b_1, p - b_2, \ldots, p - b_s, a_1, a_2, \ldots, a_r$ su svi međusobno različiti, ima ih $\frac{p-1}{2}$ i elementi su skupa $\{1, 2, \ldots, \frac{p-1}{2}\}$. Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih dobivamo

$$(p - b_1) \cdots (p - b_s) \cdot a_1 \cdots a_r = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \left(\prod_{i=1}^{s}(p - b_i)\right)\left(\prod_{j=1}^{r} a_j\right) \equiv (-1)^s \left(\prod_{i=1}^{s} b_i\right)\left(\prod_{j=1}^{r} a_j\right) \\ &\equiv (-1)^s \cdot a \cdot 2a \cdot 3a \cdots (\frac{p-1}{2}) \pmod{p}\end{aligned}$$

Skratimo li s $(\frac{p-1}{2})!$ dobivamo

$$1 \equiv (-1)^s a^{\frac{p-1}{2}} \pmod{p}.$$

Prema Eulerovom kriteriju je

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}.$$

□

Primjer 5.4. *Neka je $p = 23$ i $a = 5$. Prvih $\frac{p-1}{2} = 11$ višekratnika broja 5: $5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55$ kongruentno je redom $5, 10, 15, 20, 2, 7, 12, 17, 22, 4, 9$ modulo 23. Među njima je 5 onih koji su veći od $\frac{23}{2}$. Dakle, $s = 5$ i*

$$\left(\frac{5}{23}\right) = (-1)^5 = -1.$$

Prema tome, kongruencija $x^2 \equiv 5 \pmod{23}$ nema rješenja.

Pomoću idućeg rezultata lakše ćemo odrediti Legendreov simbol za broj 2 i neki neparan prost broj p.

Teorem 5.6. *Neka je p neparan prost broj. Tada je*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , \text{ ako je } p \equiv \pm 1 \pmod{8} \\ -1 & , \text{ ako je } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Dokaz. Neka je s broj elemenata skupa $\{2, 4, 6, \ldots, 2(\frac{p-1}{2})\}$ koji su veći od $\frac{p}{2}$. Primjetimo da je $2k \leq \frac{p}{2}$ ako i samo ako je $k \leq \frac{p}{4}$. Odatle je $s = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$.
Ako je $p = 8k+1$, tada je $s = 4k - \lfloor 2k + \frac{1}{4} \rfloor = 4k - 2k \equiv 0 \pmod 2$.
Ako je $p = 8k+3$, tada je $s = 4k+1 - \lfloor 2k + \frac{3}{4} \rfloor = 4k+1-2k \equiv 1 \pmod 2$.
Ako je $p = 8k+5$, tada je $s = 4k+2 - \lfloor 2k+1+\frac{1}{4} \rfloor = 2k+1 \equiv 1 \pmod 2$.
Ako je $p = 8k+7$, tada je $s = 4k+3 - \lfloor 2k+1+\frac{3}{4} \rfloor = 2k+2 \equiv 0 \pmod 2$. Sada tvrdnja proizilazi iz Gaussove leme. □

Budući da $\frac{p^2-1}{8}$ zadovoljava iste kongruencije kao i s iz dokaza prethodnog teorema, vrijedi sljedeća tvrdnja.

Korolar 5.3. *Ako je p neparan prost broj, tada je*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Idući teorem govori da, ako su p i q različiti prosti brojevi oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod q$ i $x^2 \equiv q \pmod p$ ima rješenje, a druga nema.

Teorem 5.7 (Kvadratni zakon reciprociteta). *Neka su p i q različiti neparni prosti brojevi. Tada vrijedi*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Dokaz. Neka su p i q različiti prosti brojevi te neka su r_k ostaci pri dijeljenju brojeva kq s p za $k = 1, 2, \ldots, \frac{p-1}{2}$. Kvocijenti pri tom dijeljenju su brojevi $\lfloor \frac{kq}{p} \rfloor$, odnosno $kq = p \cdot \lfloor \frac{kq}{p} \rfloor + r_k$. Slično kao u dokazu Gaussove leme, označimo s $a_1, a_2, \ldots, a_r$ one r_k koji su manji od $\frac{p}{2}$, a s $b_1, b_2, \ldots b_s$ one r_k koji su veći od $\frac{p}{2}$. Tamo smo zaključili da su $a_1, a_2, \ldots, a_r, p-b_1, p-b_2, \ldots, p-b_s$ brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Sada je, prema Gaussovoj lemi,

$$\left(\frac{q}{p}\right) = (-1)^s.$$

Označimo

$$a = \sum_{i=1}^{r} a_i \;\; i \;\; b = \sum_{j=1}^{s} b_j \;\; pa \; je \;\; a + b = \sum_{k=1}^{\frac{p-1}{2}} r_k \; .$$

Imamo da je

$$a + sp - b = \sum_{i=1}^{r} a_i + \sum_{j=1}^{s} (p - b_j) = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8}.$$

Sumiranjem jednadžbi $p \cdot \lfloor \frac{kq}{p} \rfloor + r_k = kq$ za $k = 1, 2, \ldots, \frac{p-1}{2}$ dobivamo

$$p \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + a + b = \sum_{k=1}^{\frac{p-1}{2}} (p \left\lfloor \frac{kq}{p} \right\rfloor + rk) = \sum_{k=1}^{\frac{p-1}{2}} kq = \left(\frac{p^2-1}{8}\right) q.$$

Oduzimanjem ova dva izraza dobivamo

$$p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor+2b-sp=\left(\frac{p^2-1}{8}\right)(q-1).$$

Budući da je $p\equiv q\equiv 1 \pmod 2$,

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor\equiv s \pmod 2.$$

Iz toga slijedi da je

$$\left(\frac{q}{p}\right)=(-1)^s=(-1)^u\ ,\ u=\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor.$$

Kada bismo zamijenili uloge brojeva p i q te ponovili gornji postupak, dobili bismo da vrijedi

$$\left(\frac{p}{q}\right)=(-1)^v\ ,\ v=\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor.$$

Zbog toga sada vrijedi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{u+v}.$$

Još nam preostaje dokazati da je

$$u+v=\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right)\ .$$

Na slici 1. je prikazan pravokutnik čiji su vrhovi smješteni u Kartezijev koordinatni sustav. Pogledajmo sve parove cijelih brojeva (i,j) za $1\leq i\leq\frac{p-1}{2}$ i $1\leq j\leq\frac{q-1}{2}$, tj. one točke koje se nalaze unutar pravokutnika. Ako točka (i,j) leži na pravcu l koji je dan jednadžbom $y=\frac{q}{p}x$, tada je $pj=qi$. Budući da su p i q relativno prosti, iz toga slijedi da p dijeli i, što nije moguće jer je $1\leq i\leq\frac{p-1}{2}$ pa možemo zaključiti da svaka točka leži ili iznad ili ispod pravca l. Ukoliko se (i,j) nalazi ispod pravca l, tada je $py<qx$, tj. $j<\frac{qi}{p}$. Dakle, za fiksnu vrijednost i je $1\leq j\leq\lfloor\frac{qi}{p}\rfloor$ kada je (i,j) ispod pravca l. Prema tome, ukupan broj točaka ispod pravca l je dan s

$$\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor\frac{qi}{p}\right\rfloor=u\ .$$

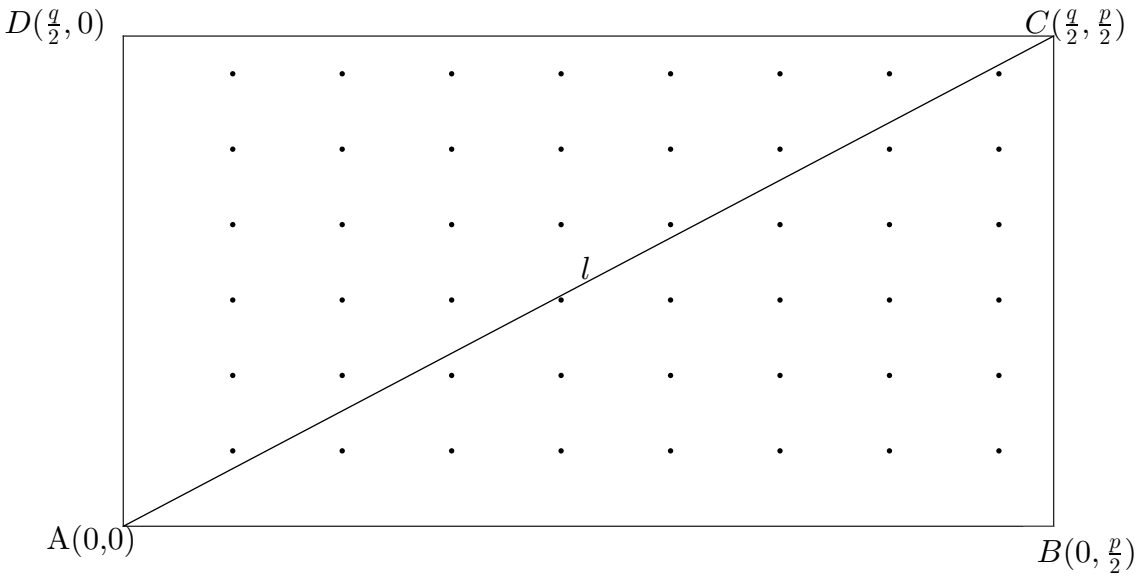
Slično je ukupan broj točaka iznad pravca l jednak

$$\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor=v\ .$$

Kako svaka točka unutar pravokutnika $ABCD$ mora ležati ili ispod ili iznad pravca l vrijedi da je $u+v=(\frac{p-1}{2})\cdot(\frac{q-1}{2})$, odakle slijedi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

□



Slika 1

Primjer 5.5. *Odredimo* $(\frac{7}{227})$.
Primjenom kvadratnog zakona reciprociteta dobivamo

$$\left(\frac{7}{227}\right) = -\left(\frac{227}{7}\right) = -\left(\frac{3}{7}\right) = 1 \ .$$

Postoji mogućnost generalizacije Lagendreova simbola za slučajeve kada je nazivnik složen broj.

Definicija 5.3. *Neka je* $a \neq 0$ *te neka je* m *neparan prirodni broj zapisan u obliku* $m = \prod_{i=1}^{r} {p_i}^{\alpha_i}$. *Tada je Jacobijev simbol definiran s*

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i},$$

gdje su $p_1, p_2, \ldots, p_r$ *prosti brojevi te* $(\frac{a}{p_i})$ *Legendreov simbol.*

Ukoliko je m prost broj, Jacobijev i Legendreov simbol se podudaraju. Za razliku od Legendreovog simbola, Jacobijev simbol $(\frac{a}{m})$ može biti jednak 1, a da to ne povlači da je a kvadratni ostatak modulo m. Na primjer,

$$\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right) \cdot \left(\frac{3}{7}\right) = (-1) \cdot (-1) = 1.$$

No, jednadžba $x^2 \equiv 3 \pmod{35}$ nema rješenja. Da bi a bio kvadratni ostatak modulo m nužno je i dovoljno da svi $(\frac{a}{p_i})$ budu jednaki 1.

6 Primitivni korijeni

Nastavljamo se baviti polinomijalnim kongruencijama višeg reda modulo p za prost broj p. Konkretno, proučavat ćemo kongruencije oblika $x^m \equiv a \pmod{p}$, gdje je p neparan prost broj, $m \geq 1$ te $(a, p) = 1$.
Prisjetimo se, Mali Fermatov teorem kaže nam da ukoliko prost broj p ne dijeli cijeli broj a, tada vrijedi $a^{p-1} \equiv 1 \pmod{p}$. Općenitije, prema Eulerovom teoremu vrijedi
$a^{\varphi(n)} \equiv 1 \pmod{n}$ za svaki prirodni broj n i svaki cijeli broj a koji je relativno prost s n. Dakle, postoji barem jedan k koji zadovoljava kongruenciju $a^k \equiv 1 \pmod{n}$. U ovisnosti o vrijednosti danog broja a, ponekad je moguće pronaći prirodan broj manji od $\varphi(n)$ tako da broj a potenciran tim brojem bude kongruentan 1 modulo n.

Primjer 6.1. *Neka je $n = 15$. Budući je $\varphi(15) = 8$, vrijedi $a^8 \equiv 1 \pmod{15}$ za svaki a relativno prost s 15. Međutim, za brojeve $2, 7, 8$ i 13 vrijedi $2^4 \equiv 7^4 \equiv 8^4 \equiv 13^4 \equiv 1 \pmod{15}$.*

S ciljem ispitivanja ponašanja potencije danog broja a modulo p, definiramo sljedeći pojam.

Definicija 6.1. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj k sa svojstvom da je $a^k \equiv 1 \pmod{n}$ naziva se red od a modulo n i označava s $ord_n(a)$. Još se kaže da a pripada eksponentu k modulo n.*

Primjer 6.2. *Iz prethodnog primjera je $ord_{15}(2) = ord_{15}(7) = ord_{15}(8) = ord_{15}(13) = 4$.*

Teorem 6.1. *Neka je $ord_n(a) = k$. Tada je $a^h \equiv 1 \pmod{n}$ ako i samo ako $k \mid h$.*

Dokaz. Pretpostavimo $(a, n) = 1$, $ord_n(a) = k$ te $a^h \equiv 1 \pmod{n}$. Prema teoremu 2.1 postoje cijeli brojevi q i s takvi da je $h = kq + s$, $0 \leq s < k$. Prema tome vrijedi $a^h = a^{kq+s} = (a^k)^q \cdot a^s$. Budući je $a^k \equiv 1 \pmod{n}$, slijedi da je $a^s \equiv 1 \pmod{n}$ što je, ukoliko je $s \neq 0$, u suprotnosti s pretpostavkom da je $ord_n(a) = k$. Dakle, $s = 0$ te $k \mid h$. Obratno, ukoliko $k \mid h$ tada postoji cijeli broj t takav da je $kt = h$. Budući je $ord_n(a) = k$, vrijedi $a^h \equiv a^{kt} \equiv (a^k)^t \equiv 1 \pmod{n}$. □

Korolar 6.1. *Ako je $ord_n(a) = k$, tada k dijeli $\varphi(n)$.*

Teorem 6.2. *Neka je $ord_n(a) = k$. Tada je $a^r \equiv a^s \pmod{n}$ ako i samo ako $r \equiv s \pmod{k}$.*

Dokaz. Neka je $ord_n(a) = k$. Pretpostavimo da je $a^r \equiv a^s \pmod{n}$ te bez smanjenja općenitosti neka je $r \geq s$. Tada je $a^{r-s} \equiv 1 \pmod{n}$. Prema teoremu 6.1 slijedi da $k \mid r - s$, odnosno $r \equiv s \pmod{k}$.
Obratno, pretpostavimo da je $r \equiv s \pmod{k}$. Tada postoji cijeli broj q takav da je $r = kq + s$ iz čega slijedi

$$a^r = a^{kq+s} = a^{kq}a^s \equiv a^s \pmod{n}.$$

□

Korolar 6.2. *Ukoliko je $ord_n(a) = k$, tada su brojevi $a, a^2, \ldots, a^k$ međusobno nekongruentni modulo n.*

Ukoliko nam je poznat red od a modulo n, tada možemo odrediti red bilo koje potencije broja a modulo n.

Teorem 6.3. *Ako je* $ord_n(a) = k$, *tada je* $ord_n(a^m) = \frac{k}{(m,k)}$.

Dokaz. Neka je $ord_n(a) = k$, $ord_n(a^m) = r$, $(m, k) = d$, $m = bd$, $k = cd$ i $(b, c) = 1$. Tada je $(a^m)^c = (a^{bd})^c = (a^{cd})^b = (a^k)^b \equiv 1 \pmod{n}$. Prema prethodnom teoremu tada $r \mid c$. Budući je $ord_n(a) = k$, $(a^{mr}) = (a^m)^r \equiv 1 \pmod{n}$. Ponovo, prema prethodnom teoremu slijedi da $k \mid mr$. Uvrstimo li $k = cd$ i $m = bd$ imamo da $cd \mid (bd)r$, odnosno $c \mid br$. Kako su c i b relativno prosti, $c \mid r$. Dakle, $c = r$ pa je $ord_n(a^m) = r = c = \frac{k}{d} = \frac{k}{(m,k)}$. □

Primjer 6.3. *Ako znamo da je* $ord_{19}(3) = 18$, *izračunajmo* $ord_{19}(27)$.
$ord_{19}(27) = ord_{19}(3^3) = \frac{18}{(18,3)} = \frac{18}{3} = 6$.

Teorem 6.4. *Ako je* p *prost broj i* d *prirodan broj takav da* $d \mid p-1$, *tada postoji točno* $\varphi(d)$ *međusobno nekongruentnih cijelih brojeva koji pripadaju eksponentu* d *modulo* p.

Dokaz. Označimo s $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d modulo p. Budući da svaki cijeli broj između 1 i $p-1$ pripada eksponentu d za neki djelitelj d od $p-1$, vrijedi

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

S druge strane, prema teoremu 3.9

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

Dovoljno je dokazati da ako je $\psi(d) \neq 0$, onda je $\psi(d) = \varphi(d)$.
Ako bi bilo $\psi(d) = 0 < \varphi(d)$ za neki d, onda bi suma $\sum_{d|p-1} \psi(d)$ bila manja od $p-1$. Stoga je $\psi(d) \neq 0$ za svaki d.
Neka je a broj koji pripada eksponentu d modulo p. Prema korolaru 6.2 brojevi $a, a^2, \ldots, a^d$ su međusobno nekongruentni modulo p. Navedeni brojevi su rješenja $x^d \equiv q \pmod{p}$ te su to, prema Lagrangeovom teoremu, sva rješenja dane kongruencije. Prema tome, svaki cijeli broj b koji pripada eksponentu d modulo p je kongruentan a^k za neki $1 \leq k \leq d$. Iz teorema 6.3 slijedi da je k u tom slučaju nužno relativno prost s d; $(k, d) = \frac{ord_p(a)}{ord_p(a^k)} = \frac{d}{d} = 1$. Dakle, dobili smo da je $\psi(d) = \varphi(d)$ za sve $d \mid p - 1$. □

Teorem 6.5. *Neka je* $ord_n(a) = k$, $ord_n(b) = h$ *te* $(k, h) = 1$. *Tada je* $ord_n(ab) = kh$.

Dokaz. Neka je $(k, h) = 1$ te neka vrijedi $a^k \equiv 1 \pmod{n}$ i $b^h \equiv 1 \pmod{n}$. Iz toga slijedi

$$(ab)^{kh} = (a^k)^h (b^h)^k \equiv 1 \pmod{n}.$$

Neka je $t \in \mathbf{N}$ takav da je $(ab)^t \equiv 1 \pmod{n}$. Tada je

$$b^{kt} \equiv a^{kt} b^{kt} = (ab)^{kt} = ((ab)^t)^k \equiv 1 \pmod{n}.$$

Prema teoremu 6.1 tada $h|kt$. Kako su h i k relativno prosti, slijedi da $h|t$.
Sličnim postupkom dobivamo i $k|t$. Prema tome $kh|t$, odnosno $kh \leq t$. □

Za neke pozitivne brojeve n postoji broj q, $1 < q \leq n-1$, takav da njegove potencije generiraju reducirani sustav ostataka modulo n. Odnosno, za svaki cijeli broj r, $1 < r \leq n-1$, $(r, n) = 1$ postoji cijeli broj k takav da je $q^k = r$. Broj q se u tom slučaju može primjeniti pri određivanju reda nekog elementa iz skupa $\{1, 2, \ldots, n-1\}$ te za određivanje kvadratnih ostataka i kvadratnih neostataka modulo n. Egzistencija takvog broja je vrlo bitna za rješavanje polinomijalnih kongruencija.

Definicija 6.2. *Neka su q i n relativno prosti. Ako je red od q modulo n jednak $\varphi(n)$, onda se q zove primitivni korijen modulo n.*

Primijetimo kako teorem 6.4 povlači da, ukoliko je p prost broj, postoji $\varphi(p-1)$ primitivnih korijena modulo p.
Ako je q primitivni korijen modulo p, $\varphi(p-1)$ primitivnih korijena je dano s $q^{a_1}, q^{a_2}, \ldots, q^{a_{\varphi(p-1)}}$, gdje su $a_1, a_2, \ldots, a_{\varphi(p-1)}$ cijeli brojevi manji od $p-1$ i relativno prosti s $p-1$. Na primjer, želimo li odrediti sve primitivne korijene modulo 11, iskoristit ćemo činjenicu da je 2 primitivni korijen modulo 11 te da je $\varphi(10) = 4$. Četiri broja manja od 10 i relativno prosta s 10 su: $1, 3, 7$ i 9. Kako vrijedi $2^1 \equiv 2$, $2^3 \equiv 8$, $2^7 \equiv 7$ i $2^9 \equiv 6 \pmod{11}$, svi primitivno korijeni modulo 11 su: $2, 6, 7$ i 8.
Njemački matematičar August Leopold Crelle je 1884. godine osmislio metodu za otkrivanje je li neki broj primitivan korijen danog prostog broja koja je vrlo primjenjiva za male proste brojeve. Metoda se temelji na tvrdnji da ukoliko pretpostavimo $1 \leq a, k \leq p-1$ te sa s_k označimo najmanji ostatak pri dijeljenju broja $a \cdot k$ s p, dok s t_k označimo najmanji ostatak pri dijeljenju broja a^k s p, tada vrijedi

$$t_k \equiv s_{t_k - 1} \pmod{p}.$$

Vidimo da tvrdnja proizilazi upravo iz svojstva $a^j \equiv a^{j-1} \cdot a \pmod{p}$.

Primjer 6.4. *Neka je $p = 17$ te $a = 5$. Donju tablicu treba popuniti koristeći višekratnike broja 5.*

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$5k$	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
5^k	1	5															

Tablica 1

Trebamo pronaći čemu je kongruentno 5^2 modulo 17. Kako je $5^2 = 5 \cdot 5$, pogledamo u 7. stupac tablice te vidimo da za $k = 5$ vrijedi $5k \equiv 8 \pmod{17}$. Dakle, $5^2 \equiv 8 \pmod{17}$. Dalje, $5^3 = 5 \cdot 5^2 \equiv 5 \cdot 8 \pmod{17}$. Za $k = 8$ u desetom stupcu tablice je $5 \cdot 8 \equiv 6 \pmod{17}$, Dakle, upisujemo $5^3 \equiv 6 \pmod{17}$ itd. Na kraju dobivamo donju tablicu.
Iz tablice možemo zaključiti kako je broj 5 primitivni korijen broja 17 jer je $ord_{17}(5) = 16 = \varphi(17)$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$5k$	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
5^k	1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1

Tablica 2

Teorem 6.6. *Neka je q primitivni korijen modulo n. Tada brojevi $q, q^2, \ldots, q^{\varphi(n)}$ čine reducirani sustav ostataka modulo n.*

Dokaz. Budući je q primitivni korjen modulo n, $ord_n(q) = \varphi(n)$ što povlači $(q, n) = 1$. Stoga je $(q^i, n) = 1$, za $i = 1, 2, \ldots, \varphi(n)$.
Elementi niza $q, q^2, \ldots, q^{\varphi(n)}$ sačinjeni su od $\varphi(n)$ međusobno nekongruentnih modulo n prirodnih brojeva. U suprotnom, kada bi bilo $q^i \equiv q^j \pmod{n}$ za $1 \leq i < j \leq \varphi(n)$, tada prema teoremu 6.2 slijedi $i \equiv j \pmod{\varphi(n)}$. To je nemoguće, budući da $\varphi(n)$ ne dijeli $j - i$ zbog $0 < j - i < \varphi(n)$. □

Izraz "primitivni korijen" je uveo Euler 1773. godine prilikom objavljivanja pretpostavke J. H. Lamberta iskazane u idućem teoremu.

Teorem 6.7. *Neka je p neparan prost broj, h prirodan broj te neka je q prost broj takav da je q^h dijeli $p - 1$. Tada postoji pozitivan cijeli broj b takav da je $ord_p(b) = q^h$.*

Dokaz. Prema Lagrangeovom teoremu i činjenici da je $p \geq 3$, kongruencija $x^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ ima najviše $\frac{p-1}{q}$ rješenja. Uz to vrijedi sljedeće:

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

Stoga najmanje jedan broj između 1 i $p - 1$, označimo ga s a, nije rješenje navedene kongruencije, odnosno $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$.
Neka je $b = a^{\frac{p-1}{q^h}}$ i pretpostavimo $ord_p(b) = m$. Odatle vrijedi $b^{q^h} \equiv a^{p-1} \pmod{p}$ te prema teoremu 6.1 $m \mid q^h$.
Pretpostavimo $m < q^h$. Kako je q prost broj, m dijeli q^{h-1}, tj. postoji cijeli broj k tako da je $mk = q^{h-1}$. Tada je $a^{\frac{p-1}{q}} = b^{q^{h-1}} = (b^m)^k \equiv 1 \pmod{p}$ što je u kontradikciji s pretpostavkom da a nije rješenje kongruencije $x^{\frac{p-1}{q}} \equiv 1 \pmod{p}$. Dakle, $q^h = m = ord_p(b)$. □

Teorem 6.8. *Neka je p prost broj te q primitivni korijen modulo p. Tada su svi kvadratni ostaci modulo p oblika q^{2k}, dok su svi kvadratni neostaci oblika q^{2k+1} za $0 \leq k \leq \frac{p-1}{2}$.*

Dokaz. Prema Eulerovom kriteriju, ako je $(q, p) = 1$, tada je

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

dok je

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

Obratno, ako je a kvadratni ostatak modulo p, tada je $a = (q^k)^2 = q^{2k}$ te, ako je a kvadratni neostatak modulo p, tada vrijedi $a = (q^2)^k \cdot q = q^{2k+1}$ za $0 \leq k \leq \frac{p-1}{2}$. □

Na primjer, u prethodnom primjeru smo vidjeli kako je broj 5 primitivni korijen modulo 17. Iz toga sada možemo zaključiti da su svi kvadratni ostaci modulo 17 : $5^0, 5^2, 5^4, 5^6, 5^8, 5^{10}, 5^{12}, 5^{14}$ i 5^{16}.

Prema Eulerovom kriteriju kongruencija $x^2 \equiv a \pmod{p}$ ima rješenje ako je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Idući teorem iskazuje uvjete potrebne da bi kongruencija $x^m \equiv a \pmod{p}$ imala rješenje.

Teorem 6.9. *Neka je p neparan prost broj te $(a, p) = 1$. Tada $x^m \equiv a \pmod{p}$ ima rješenje ako i samo ako vrijedi $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, gdje je $d = (m, p-1)$.*

Dokaz. Dovoljno je pokazati nužnost. Pretpostavimo da vrijedi $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, $(a, p) = 1$, $d = (m, p-1)$ te neka je q primitivni korijen modulo p. Tada postoji $s \in \mathbb{Z}$ takav da je $a = q^s$. Slijedi $q^{\frac{s(p-1)}{d}} \equiv a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$. Budući da je q primitivni korijen modulo p mora biti $\frac{s}{d} \in \mathbb{Z}$, tj. $\frac{s}{d} = k$, $k \in \mathbb{Z}$ i $a \equiv q^{kd} \pmod{p}$.
Nadalje, iz $d = (m, p-1)$ slijedi da postoje $u, v \in \mathbb{Z}$ takvi da je $d = um + v(p-1)$. Sada je $a \equiv q^{kd} = q^{kum+kv(p-1)} = q^{kum} q^{(p-1)kv} \equiv q^{(ku)m} \pmod{p}$. Dakle, q^{ku} je rješenje kongruencije $x^m \equiv a \pmod{p}$. □

Primjer 6.5. *Kongruencija $x^8 \equiv 10 \pmod{11}$ nema rješenje zbog*
$10^{\frac{10}{2}} \equiv 10^5 \equiv -1 \not\equiv 1 \pmod{11}$.
Kongruencija $x^3 \equiv 4 \pmod{11}$ ima rješenje zbog $4^{10} \equiv 1 \pmod{11}$.

Za dani m moguće je pronaći sve ostatke m-tog stupnja modulo p, gdje je p prost broj.

Teorem 6.10. *Ako je p neparan prost broj, q primitivni korijen modulo p te $d = (m, p-1)$, tada su svi ostaci m-tog stupnja modulo p dani s $q^d, q^{2d}, \ldots, q^{\frac{d(p-1)}{d}}$.*

Dokaz. Neka je p neparan prost broj, q primitivni korijen modulo p te $d = (m, p-1)$. Prema prethodnom teoremu svaki element skupa $\{q^d, q^{2d}, \ldots, q^{\frac{d(p-1)}{d}}\}$ je ostatak m-tog stupnja modulo p. Također, svi elementi tog skupa su međusobno nekongruentni modulo p jer ako pretpostavimo $q^{id} \equiv q^{jd} \pmod{p}$ za neke $1 \leq i < j \leq \frac{p-1}{d}$ iz korolara 6.1 slijedi $p-1 \mid d(j-i)$ što je nemoguće budući $0 < d(j-i) < p-1$.
Pretpostavimo da je a ostatak m-tog stupnja modulo p. Tada postoji b, $1 \leq b \leq p-1$ takav da je $b^m \equiv a \pmod{p}$. Također, postoji $k \in \mathbb{Z}$, $1 \leq k \leq p-1$, tako da je $b \equiv q^k \pmod{p}$ iz čega slijedi $a \equiv b^m \equiv q^{km} \pmod{p}$.
Neka su $r, s, t, u \in \mathbb{Z}$ takvi da vrijedi $ud = m$, $td = p-1$, $uk = st + r$, gdje je $0 \leq r < t$. Sada je $a \equiv q^{km} \equiv q^{ukd} \equiv q^{(st+r)d} \equiv q^{(p-1)s} q^{rd} \equiv q^{rd} \pmod{p}$ pa je prema tome a element skupa $\{q^d, q^{2d}, \ldots, q^{\frac{d(p-1)}{d}}\}$. □

Primjer 6.6. *Pronađimo sve ostatke šestog stupnja modulo 17.*
Imamo $p-1 = 16$, $m = 6$, $d = (6, 16) = 2$. Dovoljno je pronaći jedan primitivni korijen modulo 17. Iz prethodnih primjera znamo da je 5 primitivni korijen modulo 17 pa neka je $q = 5$. Sada su svi ostaci šestog stupnja $5^2 \equiv 8$, $5^4 \equiv 13$, $5^6 \equiv 2$, $5^8 \equiv 16$, $5^{10} \equiv 9$, $5^{12} \equiv 4$, $5^{14} \equiv 15$, $5^{16} \equiv 1$, tj. kongruencija $x^6 \equiv a \pmod{17}$ ima rješenja samo za $a = 1, 2, 4, 8, 9, 13, 15$ ili 16.

Primijetimo da postoji veza i između primitivnih korijena i kvadratnih neostataka modulo p kada je p neparan prost broj. Ako je q primitivni korijen modulo p, tada je $ord_p(q) = p-1$ te uvijek vrijedi $q^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ jer je $\frac{p-1}{2} < p-1$ te je q kvadratni neostatak modulo p. Idući teorem iskazuje kada vrijedi da je svaki kvadratni neostatak modulo p ujedno i primitivni korijen modulo p.

Teorem 6.11. *Neka je p neparan prost broj. Svaki kvadratni neostatak modulo p je primitivni korijen modulo p onda i samo onda ako je $p = 2^k + 1$ za $k \in \mathbb{N}$.*

Dokaz. Prema teoremu 5.1 postoji $\frac{p-1}{2}$ kvadratnih neostataka modulo p. Također znamo da postoji $\varphi(p-1)$ primitivnih korijena modulo p. Da bi svaki kvadratni neostatak bio primitivni korijen modulo p mora vrijediti $\varphi(p-1) = \frac{p-1}{2}$. Prema primjeru 3.6, $\varphi(n) = \frac{n}{2}$ ako i samo ako je $n = 2^k$. Slijedi da je tada p oblika $2^k + 1$, $k \in \mathbb{N}$. □

Definicija i teorem koji slijede daju nam dovoljno potrebnog znanja za rješavanje brojnih polinomijalnih kongruencija višeg reda.

Definicija 6.3. *Neka je p neparan prost broj i q primitivni korijen modulo p. Za svaki cijeli broj n takav da je $(n,p) = 1$ postoji jedinstveni $r \in \{1, 2, \ldots, p-1\}$ takav da je $q^r \equiv n \pmod{p}$. Eksponent r nazivamo indeks od n u odnosu na q i označavamo s $I_q(n)$ ili kraće s $I(n)$.*

Teorem 6.12. *Neka je p neparan prost broj, q primitivni korijen modulo p, $r, k \in \mathbb{N}$ te m i n cijeli brojevi takvi da je $(m,p) = (n,p) = 1$. Tada vrijede sljedeće tvrdnje:*

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

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

(3) $I(1) = 0$ *i* $I(q) = 1$

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

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

Dokaz. Budući je q primitivni korijen modulo p, vrijedi $ord_p(q) = p-1$. Neka je $r = I(m)$ i $s = I(n)$, odnosno $q^r \equiv m \pmod{p}$ i $q^s \equiv n \pmod{p}$.

(1)

$$\begin{aligned} m \equiv n \pmod{p} &\iff q^r \equiv q^s \pmod{p} \\ &\iff r \equiv s \pmod{p-1} \\ &\iff I(m) \equiv I(n) \pmod{p-1}. \end{aligned}$$

(2) Budući da je $q^r \equiv m \pmod{p}$, prema (1) slijedi da je $I(q^r) \equiv I(m) \equiv r \pmod{p-1}$.

(3) $1 \equiv q^0 \pmod{p}$ i $q \equiv q^1 \pmod{p}$ te je stoga $I(1) = 0$ i $I(q) = 1$.

(4) $q^{r+s} = q^r q^s \equiv mn \pmod{p}$ iz čega je $I(mn) \equiv r + s \equiv I(m) + I(n) \pmod{p-1}$.

(5) Kako je $n^k \equiv (q^s)^k \pmod{p}$, tada je $I(n^k) \equiv ks \equiv k \cdot I(n) \pmod{p-1}$.

□

Primjer 6.7. *Riješimo kongruenciju* $3x \equiv 11 \pmod{17}$.
Iskoristimo činjenicu da je 3 *primitivni korijen modulo* 17 *te svojstva iz prethodnog teorema. Sada imamo:*

$$\begin{aligned} 3x &\equiv 11 \pmod{17} \\ I(3x) &\equiv I(11) \pmod{16} \\ I(3) + I(x) &\equiv I(11) \pmod{16} \\ 1 + I(x) &\equiv 7 \pmod{16} \\ I(x) &\equiv 6 \pmod{16} \\ x &\equiv 15 \pmod{17}. \end{aligned}$$

Primjer 6.8. *Izračunajmo ostatak pri dijeljenju broja* $3^{24} \cdot 5^{13}$ *brojem* 17. *Neka je* $q = 3$ *kao u i prethodnom primjeru.*

$$\begin{aligned} x &\equiv 3^{24} \cdot 5^{13} \pmod{17} \\ I(x) &\equiv 24 \cdot I(3) + 13 \cdot I(5) \pmod{16} \\ I(x) &\equiv 24 \cdot 1 + 13 \cdot 5 \pmod{16} \\ I(x) &\equiv 89 \pmod{16} \\ I(x) &\equiv 9 \pmod{16} \\ x &\equiv 14 \pmod{17}. \end{aligned}$$

Primjer 6.9. *Riješimo kongruenciju* $3x^4 \equiv 5 \pmod{11}$.
Kao u primjeru 6.4 *napravit ćemo tablicu za* $p = 11$.

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

Tablica 3

Iz tablice vidimo da je 7 *primitivni korijen modulo* 11. *Imamo:*

$$\begin{aligned}
3x^4 &\equiv 5 \pmod{11} \\
I(3) + 4 \cdot I(x) &\equiv I(5) \pmod{10} \\
4 + 4 \cdot I(x) &\equiv 2 \pmod{10} \\
4 \cdot I(x) &\equiv 8 \pmod{10} \\
I(x) &\equiv 2 \pmod{10} \;\; ; \;\; I(x) \equiv 7 \pmod{10} \\
x &\equiv 5 \pmod{11} \;\; ; \;\; x \equiv 6 \pmod{11}.
\end{aligned}$$

Literatura

[1] A. Dujella, *Uvod u teoriju brojeva*, Skripta, PMF-Matematički odjel, Sveučilište u Zagrebu

[2] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, 2015.

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

Sažetak

U ovom radu upoznat ćemo se s metodama određivanja uvijeta za egzistenciju rješenja polinomijalnih kongruencija te pronalaženja istih. Glavni dio rada podijeljen je u pet poglavlja, od kojih prva dva daju dovoljno temeljnog znanja o djeljivosti i kongruencijama te njihovim svojstvima. Također su promatrane linearne kongruencije kao i rješavanje sustava linearnih kongruencija koristeći Kineski teorem o ostacima. U četvrtom poglavlju posebna pažnja je usmjerena na kvadratne kongruencije. Definiran je pojam Legendreovog simbola te su predstavljeni rezultati koji vode lakšem određivanju njegove vrijednosti. Svi teorijski rezultati u radu primjenjeni su na konkretnim primjerima. U posljednjem poglavlju ćemo preko definicije reda prirodnog broja a modulo n doći do pojma primitivnog korijena modulo n. Pokazat ćemo kako odrediti je li neki prirodni broj primitivan korijen modulo n. Spomenuti pojam bit će ključan u rješavanju polinomijalnih kongruencija.

Ključne riječi: polinomijalna kongruencija, modulo, Legendreov simbol, Jacobijev simbol, primitvni korijen

High order congruences

Summary

In this paper we will introduce the methods of determining the conditions for the existence of solutions of polynomial congruence and technique to obtain such solutions. The main part of this paper is divided into five chapters, of which the first two provide enough basic knowledge about the divisibility and congruence and their properties. We study a linear congruence and solving systems of linear congruences using the Chinese theorem of residues. In the fourth chapter, special attention is focused on quadratic congruence. We define Legendre symbol and presents the results which lead to easier determine its value. All theoretical results in the work were applied to particular examples. In the last chapter we introduce the concept of the order of integer modulo n and then we define primitive roots modulo n and show how to determine whether an integer is primitive modulo n or not. The mentioned term will be a key to solving polynomial congruence.

Key words: polynomial congruence, modulo, Legendre symbol, Jacobi symbol, primitive root

Životopis

Rođena sam 20. listopada 1990. godine u Rijeci. Osnovnoškolsko obrazovanje završila sam u Dalju, nakon čega se upisujem u opću gimnaziju u Zagrebu. Odličan uspjeh u gimnaziji mi omogućuje izravan upis na preddiplomski studij matematike na Odjelu za matematiku u Osijeku 2009. godine te se 2013. godine prebacujem na sveučilišni nastavnički studij matematike i informatike.