Teorija brojeva

Filip Najman

5. predavanje

6.4.2023.

Definicija

Neka je g primitivni korijen modulo n. Lako se vidi da tada brojevi g^l, $l = 0, 1, \ldots, \varphi(n) - 1$ tvore reducirani sustav ostataka modulo n. Stoga za svaki cijeli broj a takav da je $(a, n) = 1$ postoji jedinstveni l takav da je $g^l \equiv a \pmod{n}$. Eksponent l se zove indeks od a u odnosu na g i označava se sa $\operatorname{ind}_g a$ ili $\operatorname{ind} a$.

Teorem

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

Teorem

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

Dokaz: Svojstva 1) – 3) slijede direktno iz definicije, a svojstvo 4) slijedi iz $g^{2\operatorname{ind}(-1)} \equiv (-1)^2 \equiv 1 \pmod{n}$ i $2\operatorname{ind}(-1) < 2\varphi(n)$. □

Teorem

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

Dokaz: Svojstva 1) – 3) slijede direktno iz definicije, a svojstvo 4) slijedi iz $g^{2\operatorname{ind}(-1)} \equiv (-1)^2 \equiv 1 \pmod{n}$ i $2\operatorname{ind}(-1) < 2\varphi(n)$. □

Uočimo da su svojstva indeksa 1) – 3) potpuno analogna svojstvima logaritamske funkcije.

Propozicija

Ako je $(n, p-1) = 1$, *onda kongruencija* $x^n \equiv a \pmod{p}$ *ima jedinstveno rješenje.*

Propozicija

Ako je $(n, p-1) = 1$, *onda kongruencija* $x^n \equiv a \pmod{p}$ *ima jedinstveno rješenje.*

Dokaz: Iz $x^n \equiv a \pmod{p}$, dobivamo

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1},$$

pa jer je $(n, p-1) = 1$, ova kongruencija ima jedinstveno rješenje. □

Zadatak

Odredite najmanji primitvni korijen modulo 11 u sustavu najmanjih nenegativnih ostataka.

Zadatak

Odredite najveći primitvni korijen modulo 13 u sustavu najmanjihu nenegativnih ostataka.

Zadatak

Neka je $a, n, d \in \mathbb{Z}$. Ako je red od a modulo n jednak d, odredite kada postoji x takav da je $ax^2 \equiv 1 \pmod{n}$.

Zadatak

Neka su $a, n \in \mathbb{Z}$. Može li red od a modulo n biti a? Ako može dajte primjer, ako ne može dokažite.

Zadatak

Neka su $a, n \in \mathbb{Z}$. Može li red od a modulo n biti n? Ako može dajte primjer, ako ne može dokažite.

Kvadratni ostatci

Definicija

Neka je $(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je* a *kvadratni ostatak modulo* m. *U protivnom kažemo da je* a *kvadratni neostatak modulo* m.

Primjer

Kvadratni ostatci modulo 5 *su* 1 *i* 4, *a neostatci su* 2 *i* 3.

Teorem

Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.

Dokaz: Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od brojeva

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.

Teorem

Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.

Dokaz: Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od brojeva

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.

Preostaje pokazati da je ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentno modulo p. Pa pretpostavimo da je $k^2 \equiv l^2 \pmod{p}$, gdje je $1 \leq k < l \leq \frac{p-1}{2}$.

Teorem

Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.

Dokaz: Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od brojeva

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.

Preostaje pokazati da je ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentno modulo p. Pa pretpostavimo da je $k^2 \equiv l^2 \pmod{p}$, gdje je $1 \leq k < l \leq \frac{p-1}{2}$.

Tada je $(l-k)(l+k) \equiv 0 \pmod{p}$, pa je $l-k \equiv 0 \pmod{p}$ ili $l+k \equiv 0 \pmod{p}$, što je u suprotnosti s pretpostavkama na k i l, jer je $0 < l-k < p$ i $0 < l+k < p$. □

Zadatak

Odredite sve kvadratne ostatke modulo 11 *i modulo* 13.

Definicija

Neka je p *neparan prost broj. Po definiciji, Legendreov simbol* $\left(\frac{a}{p}\right)$ *je jednak* 1 *ako je* a *kvadratni ostatak modulo* p, -1 *ako je* a *kvadratni neostatak modulo* p, a 0 *ako* $p|a$.

Dakle, broj rješenja kongruencije $x^2 \equiv a \pmod{p}$ je jednak $1 + \left(\frac{a}{p}\right)$.

Teorem (Eulerov kriterij)

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

Dokaz: Ako je $(\frac{a}{p}) = 0$, onda $p|a$, pa je tvrdnja očito zadovoljena. Ako je $(\frac{a}{p}) = 1$, onda postoji $x_0 \in \mathbb{Z}$ takav da je $x_0^2 \equiv a \pmod{p}$.

Teorem (Eulerov kriterij)

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

Dokaz: Ako je $(\frac{a}{p}) = 0$, onda $p|a$, pa je tvrdnja očito zadovoljena. Ako je $(\frac{a}{p}) = 1$, onda postoji $x_0 \in \mathbb{Z}$ takav da je $x_0^2 \equiv a \pmod{p}$.

Sada je iz Malog Fermatovog teorema $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv (\frac{a}{p}) \pmod{p}$.

Neka je $\left(\frac{a}{p}\right) = -1$. Za svaki $i \in \{1, \ldots, p-1\}$ odaberimo $j \in \{1, \ldots, p-1\}$ tako da vrijedi $i \cdot j \equiv a \pmod{p}$ (to je moguće koristeći argumente koje smo prethodni put koristili).

Neka je $\left(\frac{a}{p}\right) = -1$. Za svaki $i \in \{1, \ldots, p-1\}$ odaberimo $j \in \{1, \ldots, p-1\}$ tako da vrijedi $i \cdot j \equiv a \pmod{p}$ (to je moguće koristeći argumente koje smo prethodni put koristili).

Uočimo da je $i \neq j$, budući da kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se raspada na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a \pmod{p}$.

Neka je $\left(\frac{a}{p}\right) = -1$. Za svaki $i \in \{1, \ldots, p-1\}$ odaberimo $j \in \{1, \ldots, p-1\}$ tako da vrijedi $i \cdot j \equiv a \pmod{p}$ (to je moguće koristeći argumente koje smo prethodni put koristili).

Uočimo da je $i \neq j$, budući da kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se raspada na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a \pmod{p}$.

Množenjem ovih $\frac{p-1}{2}$ kongruencija, te koristeći Wilsonov teorem, dobivamo

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

□

Propozicija

1) Ako je $a \equiv b \pmod{p}$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Propozicija

1) *Ako je* $a \equiv b \pmod{p}$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

Propozicija

1) *Ako je* $a \equiv b \pmod{p}$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

3) *Ako je* $(a, p) = 1$, *onda je* $\left(\frac{a^2}{p}\right) = 1$.

Propozicija

1) *Ako je* $a \equiv b \pmod{p}$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

3) *Ako je* $(a, p) = 1$, *onda je* $\left(\frac{a^2}{p}\right) = 1$.

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

Propozicija

1) *Ako je* $a \equiv b \pmod{p}$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

3) *Ako je* $(a, p) = 1$, *onda je* $\left(\frac{a^2}{p}\right) = 1$.

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

Dokaz: 1) Ako je $a \equiv b \pmod{p}$, onda kongruencija $x^2 \equiv a \pmod{p}$ ima rješenja ako i samo ako rješenja ima kongruencija $x^2 \equiv b \pmod{p}$.

2) Iz

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

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

2) Iz

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

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

3) Kongruencija $x^2 \equiv a^2 \pmod{p}$ očito ima rješenje $x = a$.

2) Iz

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

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

3) Kongruencija $x^2 \equiv a^2 \pmod{p}$ očito ima rješenje $x = a$.

4) Prva tvrdnja je specijalni slučaj od 3), dok druga slijedi uvrštavanjem $a = -1$, u Eulerov kriterij. □

Teorem (Gaussova lema)

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

Teorem (Gaussova lema)

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

Dokaz: Neka su $r_1, \ldots, r_n$ ostatci koji su veći od $\frac{p}{2}$, a neka su $s_1, \ldots, s_k$ preostali ostatci.

Teorem (Gaussova lema)

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

Dokaz: Neka su $r_1, \ldots, r_n$ ostatci koji su veći od $\frac{p}{2}$, a neka su $s_1, \ldots, s_k$ preostali ostatci.

Brojevi $r_1, \ldots, r_n, s_1, \ldots, s_k$ su međusobno različiti (po ranije dokazanom Teoremu) i niti jedan od njih nije jednak nuli.

Teorem (Gaussova lema)

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

Dokaz: Neka su $r_1, \ldots, r_n$ ostatci koji su veći od $\frac{p}{2}$, a neka su $s_1, \ldots, s_k$ preostali ostatci.

Brojevi $r_1, \ldots, r_n, s_1, \ldots, s_k$ su međusobno različiti (po ranije dokazanom Teoremu) i niti jedan od njih nije jednak nuli.

Nadalje, $n + k = \frac{p-1}{2}$.

Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$.

Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$.

Pokažimo da niti jedan $p - r_i$ nije jednak nekom s_j.

Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$.

Pokažimo da niti jedan $p - r_i$ nije jednak nekom s_j.

Zaista, ako je $p - r_i = s_j$, onda je $r_i \equiv \alpha a \pmod{p}$, $s_j \equiv \beta a \pmod{p}$ 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 da je $\alpha + \beta \equiv 0 \pmod{p}$, što je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$.

Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$.

Pokažimo da niti jedan $p - r_i$ nije jednak nekom s_j.

Zaista, ako je $p - r_i = s_j$, onda je $r_i \equiv \alpha a \pmod{p}$, $s_j \equiv \beta a \pmod{p}$ 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 da je $\alpha + \beta \equiv 0 \pmod{p}$, što je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$.

Prema tome, brojevi $p - r_1, \ldots, p - r_n, s_1, \ldots, s_k$ su svi međusobno različiti, ima ih $\frac{p-1}{2}$ i elementi su skupa $\{1, \ldots, \frac{p-1}{2}\}$.

Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih, dobivamo

$$(p - r_1) \cdots (p - r_n)\, s_1 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih, dobivamo

$$(p - r_1) \cdots (p - r_n)\, s_1 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$\begin{aligned} 1 \cdot 2 \cdots \frac{p-1}{2} &\equiv (-r_1) \cdots (-r_n)\, s_1 \cdots s_k \equiv (-1)^n\, r_1 \cdots r_n s_1 \cdots s_k \\ &\equiv (-1)^n\, a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \pmod{p}. \end{aligned}$$

Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih, dobivamo

$$(p - r_1) \cdots (p - r_n)\, s_1 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$\begin{aligned} 1 \cdot 2 \cdots \frac{p-1}{2} &\equiv (-r_1) \cdots (-r_n)\, s_1 \cdots s_k \equiv (-1)^n\, r_1 \cdots r_n s_1 \cdots s_k \\ &\equiv (-1)^n\, a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \pmod{p}. \end{aligned}$$

Skratimo li ovu kongruenciju s $\left(\frac{p-1}{2}\right)!$, dobivamo $1 \equiv (-1)^n\, a^{\frac{p-1}{2}} \pmod{p}$, tj. $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$.

Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih, dobivamo

$$(p - r_1) \cdots (p - r_n)\, s_1 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$\begin{aligned} 1 \cdot 2 \cdots \frac{p-1}{2} &\equiv (-r_1) \cdots (-r_n)\, s_1 \cdots s_k \equiv (-1)^n\, r_1 \cdots r_n s_1 \cdots s_k \\ &\equiv (-1)^n\, a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \pmod{p}. \end{aligned}$$

Skratimo li ovu kongruenciju s $\left(\frac{p-1}{2}\right)!$, dobivamo $1 \equiv (-1)^n\, a^{\frac{p-1}{2}} \pmod{p}$, tj. $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$.

Po Eulerovom kriteriju slijedi

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

Teorem

Ako je p neparan prost broj i $(a, 2p) = 1$, onda je $\left(\frac{a}{p}\right) = (-1)^t$, gdje je $t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$. Također vrijedi: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, tj. broj 2 je kvadratni ostatak modulo p ako i samo ako je p oblika $8k \pm 1$.

Teorem

Ako je p neparan prost broj i $(a, 2p) = 1$, onda je $\left(\frac{a}{p}\right) = (-1)^t$, gdje je $t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$. Također vrijedi: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, tj. broj 2 je kvadratni ostatak modulo p ako i samo ako je p oblika $8k \pm 1$.

Dokaz: Koristit ćemo iste oznake kao u dokazu Gaussove leme. Ponovo su r_i i s_i ostatci pri dijeljenju brojeva ja s p, $j = 1, \ldots, \frac{p-1}{2}$.

Kvocijenti pri tom dijeljenju su brojevi $\lfloor \frac{ja}{p} \rfloor$. Pošto je $(a, p) = 1$, onda imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\lfloor \frac{ja}{p} \rfloor + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i,$$

Kvocijenti pri tom dijeljenju su brojevi $\lfloor \frac{ja}{p} \rfloor$. Pošto je $(a, p) = 1$, onda imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\lfloor \frac{ja}{p} \rfloor + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i,$$

te

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_i) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i.$$

Kvocijenti pri tom dijeljenju su brojevi $\lfloor \frac{ja}{p} \rfloor$. Pošto je $(a, p) = 1$, onda imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\lfloor \frac{ja}{p} \rfloor + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i,$$

te

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_i) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i.$$

Oduzimanjem ova dva izraza, dobivamo

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n \Big) + 2 \sum_{i=1}^{n} r_i.$$

Dakle,

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n\Big) + 2\sum_{i=1}^{n} r_i.$$

Dakle,

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n\Big) + 2\sum_{i=1}^{n} r_i.$$

Nadalje je po formuli za sumiranje prvih $\frac{p-1}{2}$ članova

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8},$$

Dakle,

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n\Big) + 2\sum_{i=1}^{n} r_i.$$

Nadalje je po formuli za sumiranje prvih $\frac{p-1}{2}$ članova

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8},$$

pa je

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n \pmod 2.$$

Dakle,

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n\Big) + 2\sum_{i=1}^{n} r_i.$$

Nadalje je po formuli za sumiranje prvih $\frac{p-1}{2}$ članova

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8},$$

pa je

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n \pmod 2.$$

Ako je sada a neparan, tj. $(a, 2p) = 1$, onda odavde dobivamo da je $n \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor \pmod 2$, a ako je $a = 2$, onda dobivamo $n \equiv \frac{p^2-1}{8} \pmod 2$, jer je $\lfloor \frac{2j}{p} \rfloor = 0$ za $j = 1, \ldots, \frac{p-1}{2}$.

Dakle,

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\Big(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n\Big) + 2\sum_{i=1}^{n} r_i.$$

Nadalje je po formuli za sumiranje prvih $\frac{p-1}{2}$ članova

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8},$$

pa je

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor - n \pmod 2.$$

Ako je sada a neparan, tj. $(a, 2p) = 1$, onda odavde dobivamo da je $n \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor \pmod 2$, a ako je $a = 2$, onda dobivamo $n \equiv \frac{p^2-1}{8} \pmod 2$, jer je $\lfloor \frac{2j}{p} \rfloor = 0$ za $j = 1, \ldots, \frac{p-1}{2}$.

Sada tvrdnja ovog Teorema slijedi iz Gaussove leme.

Teorem (Gaussov kvadratni zakon reciprociteta)

Ako su p i q različiti neparni prosti brojevi, onda vrijedi

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

Teorem (Gaussov kvadratni zakon reciprociteta)

Ako su p i q različiti neparni prosti brojevi, onda vrijedi

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

Drugim riječima, ako su p i q oba oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ ima rješenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik $4k+1$, onda ili obje ove kongruencije imaju rješenja ili obje nemaju rješenja.

Teorem (Gaussov kvadratni zakon reciprociteta)

Ako su p i q različiti neparni prosti brojevi, onda vrijedi

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

Drugim riječima, ako su p i q oba oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ ima rješenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik $4k+1$, onda ili obje ove kongruencije imaju rješenja ili obje nemaju rješenja.

Dokaz: Neka je
$\mathcal{S} = \{(x,y) : x,y \in \mathbb{Z}, 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}$. Skup $\mathcal{S}$ ima $\frac{p-1}{2}\cdot\frac{q-1}{2}$ članova.

Podijelimo $\mathcal{S}$ na dva disjunktna podskupa $\mathcal{S}_1$ i $\mathcal{S}_2$ prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$.

Podijelimo $\mathcal{S}$ na dva disjunktna podskupa $\mathcal{S}_1$ i $\mathcal{S}_2$ prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$.

Skup $\mathcal{S}_1$ je, dakle, skup svih parova (x, y) takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $1 \leq y < \frac{qx}{p}$.

Podijelimo $\mathcal{S}$ na dva disjunktna podskupa $\mathcal{S}_1$ i $\mathcal{S}_2$ prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$.

Skup $\mathcal{S}_1$ je, dakle, skup svih parova (x, y) takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $1 \leq y < \frac{qx}{p}$.

Takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$. Slično se $\mathcal{S}_2$ sastoji od svih parova (x, y) takvih da je $1 \leq y \leq \frac{q-1}{2}$ i $1 \leq x < \frac{py}{q}$, a takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$.

Podijelimo $\mathcal{S}$ na dva disjunktna podskupa $\mathcal{S}_1$ i $\mathcal{S}_2$ prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$.

Skup $\mathcal{S}_1$ je, dakle, skup svih parova (x, y) takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $1 \leq y < \frac{qx}{p}$.

Takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$. Slično se $\mathcal{S}_2$ sastoji od svih parova (x, y) takvih da je $1 \leq y \leq \frac{q-1}{2}$ i $1 \leq x < \frac{py}{q}$, a takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$.

Prema tome je

$$\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

Podijelimo $\mathcal{S}$ na dva disjunktna podskupa $\mathcal{S}_1$ i $\mathcal{S}_2$ prema tome da li je $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$.

Skup $\mathcal{S}_1$ je, dakle, skup svih parova (x, y) takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $1 \leq y < \frac{qx}{p}$.

Takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$. Slično se $\mathcal{S}_2$ sastoji od svih parova (x, y) takvih da je $1 \leq y \leq \frac{q-1}{2}$ i $1 \leq x < \frac{py}{q}$, a takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$.

Prema tome je

$$\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

pa je po prethodnom Teoremu

$$\left(\frac{q}{p}\right) = (-1)^t, \text{ gdje } t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor$$

Analogno dobivamo

$$\left(\frac{p}{q}\right) = (-1)^u, \text{ gdje } u = \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor.$$

Analogno dobivamo

$$\left(\frac{p}{q}\right) = (-1)^u, \text{ gdje } u = \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{pj}{q} \rfloor.$$

Slijedi

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