Teorija brojeva

Filip Najman

4. predavanje

30.3.2023.

Teorem

Za svaki prirodan broj $n > 1$ *vrijedi* $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$.

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Teorem

Za svaki prirodan broj $n > 1$ *vrijedi* $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$.

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Jedini brojevi u nizu $1, 2, \ldots, p_i^{\alpha_i}$ koji nisu relativno prosti s $p_i^{\alpha_i}$ su brojevi $p_i, 2p_i, \ldots, p_i^{\alpha_i - 1} \cdot p_i$.

Teorem

Za svaki prirodan broj $n > 1$ *vrijedi* $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$.

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Jedini brojevi u nizu $1, 2, \ldots, p_i^{\alpha_i}$ koji nisu relativno prosti s $p_i^{\alpha_i}$ su brojevi $p_i, 2p_i, \ldots, p_i^{\alpha_i - 1} \cdot p_i$.

Stoga je $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}(1 - \frac{1}{p_i})$.

Teorem

Za svaki prirodan broj $n > 1$ *vrijedi* $\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$.

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Jedini brojevi u nizu $1, 2, \ldots, p_i^{\alpha_i}$ koji nisu relativno prosti s $p_i^{\alpha_i}$ su brojevi $p_i, 2p_i, \ldots, p_i^{\alpha_i - 1} \cdot p_i$.

Stoga je $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}(1 - \frac{1}{p_i})$.

Zbog multiplikativnosti od φ, imamo

$$\begin{aligned}
\varphi(n) &= \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) \\
&= n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right).
\end{aligned}$$

$\square$

Teorem

Vrijedi

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

Teorem

Vrijedi

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

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Teorem

Vrijedi

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

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Zbog multiplikativnosti od φ, imamo:

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})). \qquad (1)$$

Naime, množenjem faktora na desnoj strani od (1) dobivamo sumu faktora oblika $\varphi(p_1^{\beta_1}) \cdots \varphi(p_k^{\beta_k}) = \varphi(p_1^{\beta_1} \cdots p_k^{\beta_k})$, gdje je $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$, a to je upravo lijeva strana od (1).

Teorem

Vrijedi

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

Dokaz: Neka je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Zbog multiplikativnosti od φ, imamo:

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})). \tag{1}$$

Naime, množenjem faktora na desnoj strani od (1) dobivamo sumu faktora oblika $\varphi(p_1^{\beta_1}) \cdots \varphi(p_k^{\beta_k}) = \varphi(p_1^{\beta_1} \cdots p_k^{\beta_k})$, gdje je $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$, a to je upravo lijeva strana od (1). Sada

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} \left(1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})\right)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} = n.$$

Teorem (Wilson)

Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.

Teorem (Wilson)

Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.

Dokaz: Za $p = 2$ i $p = 3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$.

Teorem (Wilson)

Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.

Dokaz: Za $p = 2$ i $p = 3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$.

Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \pmod{p}$.

Teorem (Wilson)

Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.

Dokaz: Za $p=2$ i $p=3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$.

Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \pmod{p}$.

Primjetimo da za svaki i postoji točno jedan j modulo p koji to zadovoljava, pošto jednadžba $i \cdot x \equiv 1 \pmod{p}$ ima točno jedno rješenje.

Teorem (Wilson)

Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.

Dokaz: Za $p = 2$ i $p = 3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$.

Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \pmod{p}$.

Primjetimo da za svaki i postoji točno jedan j modulo p koji to zadovoljava, pošto jednadžba $i \cdot x \equiv 1 \pmod{p}$ ima točno jedno rješenje.

Očito je $i \neq j$ jer bi inače broj $(i-1)(i+1)$ bio djeljiv sa p, a to je nemoguće zbog $0 < i - 1 < i + 1 < p$.

Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućh $\frac{p-3}{2}$ kongruencija, dobit ćemo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

pa je

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

$\square$

Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućh $\frac{p-3}{2}$ kongruencija, dobit ćemo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

pa je

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

$\square$

Očito je da vrijedi i obrat Wilsonovog teorema. Zaista, neka vrijedi

$$(p-1)! \equiv -1 \pmod{p}$$

i pretpostavimo da p nije prost. Tada p ima djelitelj d, $1 < d < p$, i d dijeli $(p-1)!$.

Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućh $\frac{p-3}{2}$ kongruencija, dobit ćemo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

pa je

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

$\square$

Očito je da vrijedi i obrat Wilsonovog teorema. Zaista, neka vrijedi

$$(p-1)! \equiv -1 \pmod{p}$$

i pretpostavimo da p nije prost. Tada p ima djelitelj d, $1 < d < p$, i d dijeli $(p-1)!$.

No, tada d mora dijeliti i -1, što je kontradikcija.

Teorem

Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ *ima rješenja ako i samo ako je* $p = 2$ *ili* $p \equiv 1 \pmod{4}$.

Teorem

Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.

Dokaz: Ako je $p = 2$, onda je $x = 1$ jedno rješenje.

Teorem

Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.

Dokaz: Ako je $p = 2$, onda je $x = 1$ jedno rješenje.

Ako je $p \equiv 1 \pmod{4}$, onda iz Wilsonovog teorema imamo:

$$[1 \cdot 2 \cdots \frac{p-1}{2}] \cdot [(p-1)(p-2) \cdots (p - \frac{p-1}{2})]$$

$$\equiv [\left(\frac{p-1}{2}\right)!] \cdot [(-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!] \equiv [\left(\frac{p-1}{2}\right)!]^2 \equiv -1 \pmod{p},$$

pa je $x = \frac{p-1}{2})!$ jedno rješenje.

Teorem

Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.

Dokaz: Ako je $p = 2$, onda je $x = 1$ jedno rješenje.

Ako je $p \equiv 1 \pmod{4}$, onda iz Wilsonovog teorema imamo:

$$[1 \cdot 2 \cdots \frac{p-1}{2}] \cdot [(p-1)(p-2) \cdots (p - \frac{p-1}{2})]$$

$$\equiv [\left(\frac{p-1}{2}\right)!] \cdot [(-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!] \equiv [\left(\frac{p-1}{2}\right)!]^2 \equiv -1 \pmod{p},$$

pa je $x = \frac{p-1}{2})!$ jedno rješenje.

Neka je $p \equiv 3 \pmod{4}$. Pretpostavimo da postoji $x \in \mathbb{Z}$ takav da je $x^2 \equiv -1 \pmod{p}$.

Teorem

Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.

Dokaz: Ako je $p = 2$, onda je $x = 1$ jedno rješenje.

Ako je $p \equiv 1 \pmod{4}$, onda iz Wilsonovog teorema imamo:

$$[1 \cdot 2 \cdots \frac{p-1}{2}] \cdot [(p-1)(p-2) \cdots (p - \frac{p-1}{2})]$$

$$\equiv [\left(\frac{p-1}{2}\right)!] \cdot [(-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!] \equiv [\left(\frac{p-1}{2}\right)!]^2 \equiv -1 \pmod{p},$$

pa je $x = \frac{p-1}{2})!$ jedno rješenje.

Neka je $p \equiv 3 \pmod{4}$. Pretpostavimo da postoji $x \in \mathbb{Z}$ takav da je $x^2 \equiv -1 \pmod{p}$.

Tada je $x^{p-1} \equiv (-1)^{(\frac{p-1}{2})} \equiv -1 \pmod{p}$, što je u suprotnosti s Malim Fermatovim teoremom. $\square$

Teorem (Lagrange)

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n. Pretpostavimo da je p prost broj, te da vodeći koeficijent od f nije djeljiv s p. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.

Dokaz: Za $n = 1$ tvrdnja je već dokazana prošli put.

Teorem (Lagrange)

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n. Pretpostavimo da je p prost broj, te da vodeći koeficijent od f nije djeljiv s p. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.

Dokaz: Za $n = 1$ tvrdnja je već dokazana prošli put.

Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja $n - 1$, te neka je f polinom stupnja n.

Teorem (Lagrange)

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n. Pretpostavimo da je p prost broj, te da vodeći koeficijent od f nije djeljiv s p. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.

Dokaz: Za $n = 1$ tvrdnja je već dokazana prošli put.

Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja $n-1$, te neka je f polinom stupnja n.

Za svaki $a \in \mathbb{Z}$ imamo $f(x) - f(a) = (x-a)g(x)$, gdje je g polinom stupnja $n-1$ s cjelobrojnim koeficijentima i s istim vodećim koeficijentom kao f. Zato ako kongruencija $f(x) \equiv 0 \pmod{p}$ ima rješenje $x = a$, onda sva rješenja ove kongruencije zadovoljavaju $(x-a)g(x) \equiv 0 \pmod{p}$.

Teorem (Lagrange)

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n. Pretpostavimo da je p prost broj, te da vodeći koeficijent od f nije djeljiv s p. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.

Dokaz: Za $n = 1$ tvrdnja je već dokazana prošli put.

Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja $n - 1$, te neka je f polinom stupnja n.

Za svaki $a \in \mathbb{Z}$ imamo $f(x) - f(a) = (x - a)g(x)$, gdje je g polinom stupnja $n - 1$ s cjelobrojnim koeficijentima i s istim vodećim koeficijentom kao f. Zato ako kongruencija $f(x) \equiv 0 \pmod{p}$ ima rješenje $x = a$, onda sva rješenja ove kongruencije zadovoljavaju $(x - a)g(x) \equiv 0 \pmod{p}$.

No, po induktivnoj prepostavci kongruencija $g(x) \equiv 0 \pmod{p}$ ima najviše $n - 1$ rješenja, pa kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja. $\square$

Teorem (Henselova lema)

Neka je $f(x)$ *polinom s cjelobrojnim koeficijentima. Ako je* $f(a) \equiv 0 \pmod{p^j}$ *i* $f'(a) \not\equiv 0 \pmod{p}$*, onda postoji jedinstveni* $t \in \{0, 1, 2, \ldots, p-1\}$ *takav da je* $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$*.*

Teorem (Henselova lema)

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Ako je $f(a) \equiv 0 \pmod{p^j}$ i $f'(a) \not\equiv 0 \pmod{p}$, onda postoji jedinstveni $t \in \{0, 1, 2, \ldots, p-1\}$ takav da je $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$.

Dokaz: Koristimo Taylorov razvoj polinoma f oko a:

$$f(a+tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + \cdots + t^n p^{nj} \frac{f^{(n)}(a)}{n!}. \tag{2}$$

Teorem (Henselova lema)

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Ako je $f(a) \equiv 0 \pmod{p^j}$ i $f'(a) \not\equiv 0 \pmod{p}$, onda postoji jedinstveni $t \in \{0, 1, 2, \ldots, p-1\}$ takav da je $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Dokaz: Koristimo Taylorov razvoj polinoma f oko a:

$$f(a + tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + \cdots + t^n p^{nj} \frac{f^{(n)}(a)}{n!}. \tag{2}$$

Pokažimo da su brojevi $\frac{f^{(k)}(a)}{k!}$ cijeli. Ovu je tvrdnju dovoljno dokazati za polinome oblika $g(x) = x^m$, gdje je $m \geq k$. No, tada je

$$\frac{g^{(k)}(a)}{k!} = \frac{m(m-1)\cdots(m-k+1)a^{m-k}}{k!} = \binom{m}{k} a^{m-k} \in \mathbb{Z}.$$

Zato iz (2) dobivamo

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}.$$

Zato iz (2) dobivamo

$$f(a+tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}.$$

Dakle, da bi bilo $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$, nužno je i dovoljno da bude

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p}. \tag{3}$$

Primjetimo da je u (3) broj $f(a)$ djeljiv s p^j.

Zato iz (2) dobivamo

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}.$$

Dakle, da bi bilo $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$, nužno je i dovoljno da bude

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p}. \tag{3}$$

Primjetimo da je u (3) broj $f(a)$ djeljiv s p^j.

Budući da je $f'(a) \not\equiv 0 \pmod{p}$, kongruencija (3) ima, po onom što je dokazano prošli put točno jedno rješenje. $\square$

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j.

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j.

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu.

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j.

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu.

Pretpostavimo da tvrdnja vrijedi za neki $j \in \mathbb{N}$, tj. da su $x_1, \ldots, x_{p-1}$ sva rješenja kongruencije $f(x) = x^{p-1} - 1 \pmod{p^j}$.

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j*.*

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu.

Pretpostavimo da tvrdnja vrijedi za neki $j \in \mathbb{N}$, tj. da su $x_1, \ldots, x_{p-1}$ sva rješenja kongruencije $f(x) = x^{p-1} - 1 \pmod{p^j}$.

Tada je $f(x_i) \equiv 0 \pmod{p^j}$ i $f'(x_i) = (p-1)x^{p-2} \not\equiv 0 \pmod{p^j}$, pa po Henselovoj lemi postoji jedinstveni $t_j \in \{0, 1, \ldots, p-1\}$ takav da je $f(x_i + t_i p^j) \equiv 0 \pmod{p^{j+1}}$.

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j*.*

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu.

Pretpostavimo da tvrdnja vrijedi za neki $j \in \mathbb{N}$, tj. da su $x_1, \ldots, x_{p-1}$ sva rješenja kongruencije $f(x) = x^{p-1} - 1 \pmod{p^j}$.

Tada je $f(x_i) \equiv 0 \pmod{p^j}$ i $f'(x_i) = (p-1)x^{p-2} \not\equiv 0 \pmod{p^j}$, pa po Henselovoj lemi postoji jedinstveni $t_j \in \{0, 1, \ldots, p-1\}$ takav da je $f(x_i + t_i p^j) \equiv 0 \pmod{p^{j+1}}$.

Sada su $x_i' = x_i + t_i p^j$, $i = 1, \ldots, p-1$ rješenja kongruencije $f(x) \equiv 0 \pmod{p^{j+1}}$.

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j.

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu.

Pretpostavimo da tvrdnja vrijedi za neki $j \in \mathbb{N}$, tj. da su $x_1, \ldots, x_{p-1}$ sva rješenja kongruencije $f(x) = x^{p-1} - 1 \pmod{p^j}$.

Tada je $f(x_i) \equiv 0 \pmod{p^j}$ i $f'(x_i) = (p-1)x^{p-2} \not\equiv 0 \pmod{p^j}$, pa po Henselovoj lemi postoji jedinstveni $t_j \in \{0, 1, \ldots, p-1\}$ takav da je $f(x_i + t_i p^j) \equiv 0 \pmod{p^{j+1}}$.

Sada su $x_i' = x_i + t_i p^j$, $i = 1, \ldots, p-1$ rješenja kongruencije $f(x) \equiv 0 \pmod{p^{j+1}}$.

Pokažimo da su to sva rješenja. Zaista, ako je x' neko rješenje, onda je $f(x') \equiv 0 \pmod{p^j}$, pa je $x' \equiv x_i \pmod{p^j}$ za neki $i = 1, \ldots, p-1$.

Propozicija

Kongruencija $x^{p-1} - 1 \equiv 0 \pmod{p^j}$ *ima točno* $p-1$ *rješenja za svaki prost broj* p *i prirodan broj* j.

Dokaz: Za $j = 1$ tvrdnja vrijedi po Malom Fermatovom teoremu.

Pretpostavimo da tvrdnja vrijedi za neki $j \in \mathbb{N}$, tj. da su $x_1, \dots, x_{p-1}$ sva rješenja kongruencije $f(x) = x^{p-1} - 1 \pmod{p^j}$.

Tada je $f(x_i) \equiv 0 \pmod{p^j}$ i $f'(x_i) = (p-1)x^{p-2} \not\equiv 0 \pmod{p^j}$, pa po Henselovoj lemi postoji jedinstveni $t_j \in \{0, 1, \dots, p-1\}$ takav da je $f(x_i + t_i p^j) \equiv 0 \pmod{p^{j+1}}$.

Sada su $x_i' = x_i + t_i p^j$, $i = 1, \dots, p-1$ rješenja kongruencije $f(x) \equiv 0 \pmod{p^{j+1}}$.

Pokažimo da su to sva rješenja. Zaista, ako je x' neko rješenje, onda je $f(x') \equiv 0 \pmod{p^j}$, pa je $x' \equiv x_i \pmod{p^j}$ za neki $i = 1, \dots, p-1$.

Sada iz jedinstvenosti od t_i slijedi da je $x' \equiv x_i' \pmod{p^{j+1}}$. $\square$

Definicija

Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.

Definicija

Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.

Propozicija

Neka je d red od a modulo n. Tada za prirodan broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d|k$. Posebno, $d|\varphi(n)$.

Dokaz: Ako $d|k$, recimo $k = d \cdot l$, onda je $a^k \equiv (a^d)^l \equiv 1 \pmod{n}$.

Definicija

Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.

Propozicija

Neka je d red od a modulo n. Tada za prirodan broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d|k$. Posebno, $d|\varphi(n)$.

Dokaz: Ako $d|k$, recimo $k = d \cdot l$, onda je $a^k \equiv (a^d)^l \equiv 1 \pmod{n}$.

Obratno, neka je $a^k \equiv 1 \pmod{n}$. Podijelimo k sa d, pa dobivamo $k = q \cdot d + r$, gdje je $0 \leq r < d$.

Definicija

Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.

Propozicija

Neka je d red od a modulo n. Tada za prirodan broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d|k$. Posebno, $d|\varphi(n)$.

Dokaz: Ako $d|k$, recimo $k = d \cdot l$, onda je $a^k \equiv (a^d)^l \equiv 1 \pmod{n}$.

Obratno, neka je $a^k \equiv 1 \pmod{n}$. Podijelimo k sa d, pa dobivamo $k = q \cdot d + r$, gdje je $0 \leq r < d$.

Sada je

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q \cdot a^r \equiv a^r \pmod{n},$$

pa zbog minimalnosti od d slijedi da je $r = 0$, tj. $d|k$. $\square$

Definicija

Ako je red od a modulo n jednak $\varphi(n)$, onda se a zove primitivni korijen modulo n.

Ako postoji primitivni korijen modulo n, onda je grupa reduciranih ostataka modulo n s množenjem modulo n ciklička, tj. svaki element reduciranog sustava ostataka je potencija primitivnog korijena.

Teorem

Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p.

Dokaz: Svaki od brojeva $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu d, koji je djelitelj od $\varphi(p) = p - 1$. Označimo sa $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d.

Teorem

Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p.

Dokaz: Svaki od brojeva $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu d, koji je djelitelj od $\varphi(p) = p-1$. Označimo sa $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d. Tada je

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

Teorem

Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p.

Dokaz: Svaki od brojeva $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu d, koji je djelitelj od $\varphi(p) = p-1$. Označimo sa $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d.
Tada je

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

Tvrdnja: $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$.

Teorem

Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p.

Dokaz: Svaki od brojeva $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu d, koji je djelitelj od $\varphi(p) = p-1$. Označimo sa $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d. Tada je

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

Tvrdnja: $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$.

Neka je $\psi(d) \neq 0$, te neka je a broj koji pripada eksponentu d modulo p.

Teorem

Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p.

Dokaz: Svaki od brojeva $1, 2, \ldots, p-1$ pripada modulo p nekom eksponentu d, koji je djelitelj od $\varphi(p) = p - 1$. Označimo sa $\psi(d)$ broj brojeva u nizu $1, 2, \ldots, p-1$ koji pripadaju eksponentu d. Tada je

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

Tvrdnja: $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$.

Neka je $\psi(d) \neq 0$, te neka je a broj koji pripada eksponentu d modulo p. Promotrimo kongruenciju

$$x^d \equiv 1 \pmod{p}.$$

Ona ima rješenja $a, a^2, \ldots, a^d$ i po Lagrangeovom teoremu to su sva rješenja.

Pokažimo da brojevi a^m, za $1 \leq m \leq d$ i $(m, d) = 1$, predstavljaju sve brojeve koji pripadaju eksponentu d modulo p.

Pokažimo da brojevi a^m, za $1 \leq m \leq d$ i $(m, d) = 1$, predstavljaju sve brojeve koji pripadaju eksponentu d modulo p.

Zaista, svaki od njih ima red d, jer ako je $a^{md'} \equiv 1 \pmod{p}$, onda $d|md'$, pa $d|d'$, dakle red ne može biti manji od d, pa je točno d.

Pokažimo da brojevi a^m, za $1 \leq m \leq d$ i $(m, d) = 1$, predstavljaju sve brojeve koji pripadaju eksponentu d modulo p.

Zaista, svaki od njih ima red d, jer ako je $a^{md'} \equiv 1 \pmod{p}$, onda $d | md'$, pa $d | d'$, dakle red ne može biti manji od d, pa je točno d.

Ako je b bilo koji broj koji pripada eksponentu d modulo p, onda pošto je b rješenje jedndžbe $x^d \equiv 1 \pmod{p}$, vrijedi da je $b \equiv a^m$ za neki m, $1 \leq m \leq d$.

Pokažimo da brojevi a^m, za $1 \leq m \leq d$ i $(m, d) = 1$, predstavljaju sve brojeve koji pripadaju eksponentu d modulo p.

Zaista, svaki od njih ima red d, jer ako je $a^{md'} \equiv 1 \pmod{p}$, onda $d | md'$, pa $d | d'$, dakle red ne može biti manji od d, pa je točno d.

Ako je b bilo koji broj koji pripada eksponentu d modulo p, onda pošto je b rješenje jedndžbe $x^d \equiv 1 \pmod{p}$, vrijedi da je $b \equiv a^m$ za neki m, $1 \leq m \leq d$.

Budući da je

$$b^{\frac{d}{(m,d)}} \equiv (a^d)^{\frac{m}{(m,d)}} \equiv 1 \pmod{p},$$

iz činjenice da je red od b modulo p jednak d, slijedi da je $(m, d) = 1$ (jer bi u suprotnom red bio manji od d).

Pokažimo da brojevi a^m, za $1 \leq m \leq d$ i $(m, d) = 1$, predstavljaju sve brojeve koji pripadaju eksponentu d modulo p.

Zaista, svaki od njih ima red d, jer ako je $a^{md'} \equiv 1 \pmod{p}$, onda $d | md'$, pa $d | d'$, dakle red ne može biti manji od d, pa je točno d.

Ako je b bilo koji broj koji pripada eksponentu d modulo p, onda pošto je b rješenje jedndžbe $x^d \equiv 1 \pmod{p}$, vrijedi da je $b \equiv a^m$ za neki m, $1 \leq m \leq d$.

Budući da je

$$b^{\frac{d}{(m,d)}} \equiv (a^d)^{\frac{m}{(m,d)}} \equiv 1 \pmod{p},$$

iz činjenice da je red od b modulo p jednak d, slijedi da je $(m, d) = 1$ (jer bi u suprotnom red bio manji od d).

Dakle, dobili smo da je $\psi(d) = \varphi(d)$.

Dakle dokazali smo tvrdnu da $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$.

Dakle dokazali smo tvrdnu da $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$.

Po Teoremu koji smo ranije dokazali je

$$p - 1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d) = p - 1,$$

pa ako bi bilo $\psi(d) = 0 < \varphi(d)$ za neki d, onda bi suma $\sum_{d|p-1} \psi(d)$ bila manja od $p - 1$, što je kontradikcija.

Dakle dokazali smo tvrdnu da $\psi(d) \neq 0$ povlači $\psi(d) = \varphi(d)$.

Po Teoremu koji smo ranije dokazali je

$$p - 1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d) = p - 1,$$

pa ako bi bilo $\psi(d) = 0 < \varphi(d)$ za neki d, onda bi suma $\sum_{d|p-1} \psi(d)$ bila manja od $p - 1$, što je kontradikcija.

Stoga je $\psi(d) \neq 0$ za svaki d, pa iz dokazane tvrdnje slijedi $\psi(d) = \varphi(d)$ za svaki d, pa i $\psi(p-1) = \varphi(p-1)$.

$\square$

Teorem

Neka je p neparan prost broj, te neka je g primitivni korijen modulo p. Tada postoji $x \in \mathbb{Z}$ takav da je $g' = g + px$ primitivni korijen modulo p^j za sve $j \in \mathbb{N}$.

Dokaz: Označimo s $g' = g + px$, gdje je x nepoznanica.

Teorem

Neka je p neparan prost broj, te neka je g primitivni korijen modulo p. Tada postoji $x \in \mathbb{Z}$ takav da je $g' = g + px$ primitivni korijen modulo p^j za sve $j \in \mathbb{N}$.

Dokaz: Označimo s $g' = g + px$, gdje je x nepoznanica.

Imamo $g^{p-1} = 1 + py$, za neki $y \in \mathbb{Z}$. Po binomnom teoremu je

$$g'^{p-1} = 1 + py + (p-1)pxg^{p-2} + \binom{p-1}{2} p^2 x^2 g^{p-3} + \cdots + p^{p-1} x^{p-1},$$

tj. $g'^{p-1} = 1 + pz$, gdje je $z \equiv y + (p-1)g^{p-2}x \pmod{p}$.

Teorem

Neka je p neparan prost broj, te neka je g primitivni korijen modulo p. Tada postoji $x \in \mathbb{Z}$ *takav da je* $g' = g + px$ *primitivni korijen modulo* p^j *za sve* $j \in \mathbb{N}$.

Dokaz: Označimo s $g' = g + px$, gdje je x nepoznanica.

Imamo $g^{p-1} = 1 + py$, za neki $y \in \mathbb{Z}$. Po binomnom teoremu je

$$g'^{p-1} = 1 + py + (p-1)pxg^{p-2} + \binom{p-1}{2} p^2 x^2 g^{p-3} + \cdots + p^{p-1} x^{p-1},$$

tj. $g'^{p-1} = 1 + pz$, gdje je $z \equiv y + (p-1)g^{p-2}x \pmod{p}$.

Koeficijent uz x nije djeljiv sa p, pa možemo odabrati x tako da bude $(z, p) = 1$.

Teorem

Neka je p neparan prost broj, te neka je g primitivni korijen modulo p. Tada postoji $x \in \mathbb{Z}$ takav da je $g' = g + px$ primitivni korijen modulo p^j za sve $j \in \mathbb{N}$.

Dokaz: Označimo s $g' = g + px$, gdje je x nepoznanica.

Imamo $g^{p-1} = 1 + py$, za neki $y \in \mathbb{Z}$. Po binomnom teoremu je

$$g'^{p-1} = 1 + py + (p-1)pxg^{p-2} + \binom{p-1}{2} p^2 x^2 g^{p-3} + \cdots + p^{p-1} x^{p-1},$$

tj. $g'^{p-1} = 1 + pz$, gdje je $z \equiv y + (p-1)g^{p-2}x \pmod{p}$.

Koeficijent uz x nije djeljiv sa p, pa možemo odabrati x tako da bude $(z, p) = 1$.

Tvrdimo da tada g' ima traženo svojstvo. Dokažimo to.

Pretpostavimo da g' pripada eksponentu d modulo p^j. Tada d dijeli $\varphi(p^j) = p^{j-1}(p-1)$.

Pretpostavimo da g' pripada eksponentu d modulo p^j. Tada d dijeli $\varphi(p^j) = p^{j-1}(p-1)$.

No, g' je primitivni korijen modulo p, pa $p-1$ dijeli d. Dakle, $d = p^k(p-1)$ za neki $k < j$. Nadalje, imamo

$$(1+pz)^p = 1+p^2 z_1, \quad (1+pz)^{p^2} = (1+p^2 z_1)^p = 1+p^3 z_2, \quad \dots,$$

$$(1+pz)^{p^k} = 1+p^{k+1} z_k,$$

gdje je $(z_i, p) = 1$ za $i = 1, \dots, k$.

Pretpostavimo da g' pripada eksponentu d modulo p^j. Tada d dijeli $\varphi(p^j) = p^{j-1}(p-1)$.

No, g' je primitivni korijen modulo p, pa $p-1$ dijeli d. Dakle, $d = p^k(p-1)$ za neki $k < j$. Nadalje, imamo

$$(1+pz)^p = 1 + p^2 z_1, \quad (1+pz)^{p^2} = (1+p^2 z_1)^p = 1 + p^3 z_2, \quad \dots,$$

$$(1+pz)^{p^k} = 1 + p^{k+1} z_k,$$

gdje je $(z_i, p) = 1$ za $i = 1, \dots, k$.

Budući da je

$$g'^d \equiv (1+pz)^{p^k} \equiv 1 + p^{k+1} z_k \equiv 1 \pmod{p^j},$$

jer pripada eksponentu d, zaključujemo da je $j \le k+1$.

Pretpostavimo da g' pripada eksponentu d modulo p^j. Tada d dijeli $\varphi(p^j) = p^{j-1}(p-1)$.

No, g' je primitivni korijen modulo p, pa $p-1$ dijeli d. Dakle, $d = p^k(p-1)$ za neki $k < j$. Nadalje, imamo

$$(1+pz)^p = 1 + p^2 z_1, \quad (1+pz)^{p^2} = (1+p^2 z_1)^p = 1 + p^3 z_2, \quad \ldots,$$

$$(1+pz)^{p^k} = 1 + p^{k+1} z_k,$$

gdje je $(z_i, p) = 1$ za $i = 1, \ldots, k$.

Budući da je

$$g'^d \equiv (1+pz)^{p^k} \equiv 1 + p^{k+1} z_k \equiv 1 \pmod{p^j},$$

jer pripada eksponentu d, zaključujemo da je $j \le k+1$.

Pošto je $k < j$, zaključujemo da je $j = k+1$.

Pretpostavimo da g' pripada eksponentu d modulo p^j. Tada d dijeli $\varphi(p^j) = p^{j-1}(p-1)$.

No, g' je primitivni korijen modulo p, pa $p-1$ dijeli d. Dakle, $d = p^k(p-1)$ za neki $k < j$. Nadalje, imamo

$$(1+pz)^p = 1 + p^2 z_1, \quad (1+pz)^{p^2} = (1+p^2 z_1)^p = 1 + p^3 z_2, \quad \ldots,$$

$$(1+pz)^{p^k} = 1 + p^{k+1} z_k,$$

gdje je $(z_i, p) = 1$ za $i = 1, \ldots, k$.

Budući da je

$$g'^d \equiv (1+pz)^{p^k} \equiv 1 + p^{k+1} z_k \equiv 1 \pmod{p^j},$$

jer pripada eksponentu d, zaključujemo da je $j \leq k+1$.

Pošto je $k < j$, zaključujemo da je $j = k+1$.

To povlači da je $d = \varphi(p^j)$. $\square$

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Neka je g primitivni korijen modulo p^j; on postoji prema prethodno dokazanom teoremu. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparanm i nazovimo ga g'.

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Neka je g primitivni korijen modulo p^j; on postoji prema prethodno dokazanom teoremu. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparanm i nazovimo ga g'.

Neka je $d = \varphi(2p^j) = \varphi(p^j)$. Tada je (g') reda d modulo $(2p^j)$, pa je on primitivni korijen modulo $2p^j$

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Neka je g primitivni korijen modulo p^j; on postoji prema prethodno dokazanom teoremu. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparanm i nazovimo ga g'.

Neka je $d = \varphi(2p^j) = \varphi(p^j)$. Tada je (g') reda d modulo $(2p^j)$, pa je on primitivni korijen modulo $2p^j$

Ostaje još dokazati nužnost. Neka je najprije $n = 2^j$ za $j \geq 3$.

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Neka je g primitivni korijen modulo p^j; on postoji prema prethodno dokazanom teoremu. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparanm i nazovimo ga g'.

Neka je $d = \varphi(2p^j) = \varphi(p^j)$. Tada je (g') reda d modulo $(2p^j)$, pa je on primitivni korijen modulo $2p^j$

Ostaje još dokazati nužnost. Neka je najprije $n = 2^j$ za $j \geq 3$.

Tada za neparan broj a vrijedi $a^2 \equiv 1 \pmod 8$. Budući da $8 | a^2 - 1$ i $2 | a^2 + 1$ imamo $a^4 \equiv 1 \pmod{16}$.

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2,\, 4,\, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Neka je g primitivni korijen modulo p^j; on postoji prema prethodno dokazanom teoremu. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparanm i nazovimo ga g'.

Neka je $d = \varphi(2p^j) = \varphi(p^j)$. Tada je (g') reda d modulo $(2p^j)$, pa je on primitivni korijen modulo $2p^j$

Ostaje još dokazati nužnost. Neka je najprije $n = 2^j$ za $j \geq 3$.

Tada za neparan broj a vrijedi $a^2 \equiv 1 \pmod 8$. Budući da $8 | a^2 - 1$ i $2 | a^2 + 1$ imamo $a^4 \equiv 1 \pmod{16}$.

Ponavljajući ovaj argument dobivamo: $a^{2^{j-2}} \equiv 1 \pmod{2^j}$ za $j \geq 3$.

Teorem

Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz: Jasno je da je 1 primitivni korijen modulo 2, te da je 3 primitivni korijen modulo 4.

Neka je g primitivni korijen modulo p^j; on postoji prema prethodno dokazanom teoremu. Odaberimo među brojevima g i $g + p^j$ onaj koji je neparanm i nazovimo ga g'.

Neka je $d = \varphi(2p^j) = \varphi(p^j)$. Tada je (g') reda d modulo $(2p^j)$, pa je on primitivni korijen modulo $2p^j$

Ostaje još dokazati nužnost. Neka je najprije $n = 2^j$ za $j \geq 3$.

Tada za neparan broj a vrijedi $a^2 \equiv 1 \pmod 8$. Budući da $8|a^2 - 1$ i $2|a^2 + 1$ imamo $a^4 \equiv 1 \pmod{16}$.

Ponavljajući ovaj argument dobivamo: $a^{2^{j-2}} \equiv 1 \pmod{2^j}$ za $j \geq 3$. Budući da je $\varphi(2^j) = 2^{j-1}$, dokazali smo da ne postoji primitivni korijen modulo 2^j za $j \geq 3$.

Konačno, neka je $n = n_1 n_2$, gdje je $(n_1, n_2) = 1$, $n_1 > 2$, $n_2 > 2$.

Konačno, neka je $n = n_1 n_2$, gdje je $(n_1, n_2) = 1$, $n_1 > 2$, $n_2 > 2$.

Brojevi $\varphi(n_1)$ i $\varphi(n_2)$ su parni, pa imamo

$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_1)}\right)^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1},$$
$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_2)}\right)^{\frac{1}{2}\varphi(n_1)} \equiv 1 \pmod{n_2}.$$

Konačno, neka je $n = n_1 n_2$, gdje je $(n_1, n_2) = 1$, $n_1 > 2$, $n_2 > 2$. Brojevi $\varphi(n_1)$ i $\varphi(n_2)$ su parni, pa imamo

$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_1)}\right)^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1},$$
$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_2)}\right)^{\frac{1}{2}\varphi(n_1)} \equiv 1 \pmod{n_2}.$$

Stoga je $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$, što znači da ne postoji primitivni korijen modulo n. $\square$

Napomena

T*zv. Artinova hipoteza glasi: Neka je $\pi(N)$ broj prostih brojeva $\leq N$, a $v_2(N)$ broj prostih brojeva $q \leq N$ za koje je 2 primitivni korijen. Tada je $v_2(N) \sim A \cdot \pi(N)$, gdje je $A = \prod_p (1 - \frac{1}{p(p-1)}) \approx 0.3739558$.*

Napomena

Tzv. *Artinova hipoteza glasi: Neka je $\pi(N)$ broj prostih brojeva $\leq N$, a $v_2(N)$ broj prostih brojeva $q \leq N$ za koje je 2 primitivni korijen. Tada je $v_2(N) \sim A \cdot \pi(N)$, gdje je $A = \prod_p (1 - \frac{1}{p(p-1)}) \approx 0.3739558$.*

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 $\mathrm{ind}_g\, a$ ili $\mathrm{ind}\, a$.