Poglavlje 2

Kongruencije

Redovi i primitivni korijeni

Teorem: *Neka je $n \in \mathbb{N}$ i $a \in \mathbb{Z}$ relativno prost s n. Neka je d najmanji prirodni broj takav da je $a^d \equiv 1 \pmod{n}$. Ako za neki $m \in \mathbb{N}$ vrijedi $a^m \equiv 1 \pmod{n}$, tada $d \mid m$.*

Broj d zove se red od a mod n i označava se s $\mathrm{ord}_n(a)$.

Teorem: *Neka je $n \in \mathbb{N}$ i $a, b \in \mathbb{Z}$ relativno prosti s n. Ako za neke $m_1, m_2 \in \mathbb{N}$ vrijedi $n \mid a^{m_1} - b^{m_1}$ i $n \mid a^{m_2} - b^{m_2}$, tada vrijedi $n \mid a^{(m_1,m_2)} - b^{(m_1,m_2)}$.*

Teorem: *Neka je $n \in \mathbb{N}$. Tada postoji primitivni korijen mod n ako i samo ako je $n = 2, 4, p^k, 2p^k$, gdje je $p > 2$ prost broj.*

Teorem: *Neka je p prost broj i $k \in \mathbb{N}$. Tada postoji točno $\varphi(\varphi(p^k)) = \varphi(p^{k-1}(p-1))$ primitivnih korijena mod p^k.*

Zadatak 2.25. Neka je p prost broj. Dokažite tvrdnju

$$p \mid 1^d + 2^d + \ldots + (p-1)^d \iff p - 1 \nmid d.$$

Rješenje. Neka je a primitivni korijen mod p. Tada suma iz zadatka postaje

$$1 + a^d + a^{2d} + \ldots + a^{(p-2)d} \pmod{p}.$$

Ako $p - 1 \mid d$, tada je ostatak pri dijeljenju s p jednak $1 + 1 + \ldots + 1 = p - 1$. Ako $p - 1 \nmid d$, tada je $a^d \neq 1 \pmod{p}$ pa je ostatak mod p jednak

$$1 + a^d + a^{2d} + \ldots + a^{(p-2)d} \equiv \frac{a^{(p-1)d} - 1}{a^d - 1} \equiv 0 \pmod{p}.$$

Zadatak 2.26. Neka je $p > 3$ prost broj. Dokažite da je $\prod_{\substack{1<a<p \\ \text{prim. korijen mod p}}} a \equiv 1 \pmod{p}$.

Rješenje. Ako je a primitivni korijen mod p, tada je i a^{-1} (multiplikativni inverz) također primitivni korijen i vrijedi da $a \neq a^{-1} \pmod{p}$ jer $a^2 \neq 1 \pmod{p}$. Dakle, u produktu možemo upariti elemente koji pomnoženi daju 1.

Zadatak 2.27. Odredite sve proste brojeve p za koje $p \mid a^{5p^2+2} - a$ za sve $a \in \mathbb{Z}$.

Rješenje. Neka je a primitivni korijen mod p. Tada je $a^{5p^2+2} - a \equiv a^7 - a \pmod{p}$ što vrijedi ako i samo ako $p - 1 \mid 6$. Dakle, sva rješenja su $p = 2, 3, 7$.

Zadatak 2.28. Dokažite da sve $a, n \in \mathbb{N}$ veće od 1 vrijedi $n \mid \varphi(a^n - 1)$.

Rješenje. Vrijedi da je $\mathrm{ord}_{a^n-1} a = n$ jer $a^n - 1 \mid a^n - 1$. Također, kako $(a^n - 1, a) = 1$, vrijedi $a^n - 1 \mid a^{\varphi(a^n-1)} - 1$. Stoga $n = \mathrm{ord}_{a^n-1} a \mid \varphi(a^n - 1)$.

Zadatak 2.29. Neka je p prost broj. Dokažite da broj $p^p - 1$ ima prost djelitelj veći od p.

Rješenje. Znamo da je $p^p - 1 = (p - 1)(p^{p-1} + \ldots + p + 1)$ i da je

$$(p - 1, p^{p-1} + \ldots + p + 1) = (p - 1, 1 + \ldots + 1 + 1) = (p - 1, p) = 1.$$

Neka je q prost broj takav da $q \mid p^{p-1} + \ldots + p + 1$. Tada $q \mid p^p - 1$ i $q \mid p^{q-1} - 1$. Zato $q \mid p^{(p,q-1)} - 1$ pa mora vrijediti $p \mid q - 1$ što dokazuje da je $q > p$.

Zadatak 2.30. Odredite najmanji neparni prosti djelitelj broja $2019^8 + 1$.

Rješenje. Imamo da $p \mid 2019^8 + 1 \implies p \mid 2019^{16} - 1$. Kako također znamo da $p \mid 2019^{p-1} - 1$ te je $(2019^8 + 1, 2019^8 - 1) = 2$, zaključujemo da je $\mathrm{ord}_p(2019) = 16$ pa mora biti $p \equiv 1 \pmod{16}$.

Najmanji prost broj $p \equiv 1 \pmod{16}$ je $p = 17$, međutim

$$2019^8 + 1 \equiv (-4)^8 + 1 \equiv 2 \pmod{17}.$$

Idući takav prost broj je $p = 97$ i imamo

$$2019^8 + 1 \equiv (-18)^8 + 1 \equiv 0 \pmod{97}.$$

Dakle, rješenje je 97.

Zadatak 2.31. Odredite sve $n \in \mathbb{N}$ takve da $n \mid 2^n - 1$.

Rješenje. Broj n je očito neparan. Neka je p najmanji prosti djelitelj broja n. Tada vrijedi

$$p \mid 2^{p-1} - 1, 2^n - 1 \implies p \mid 2^{(p-1,n)} - 1.$$

Kako je p najmanji prosti broj koji dijeli n, broj $p - 1$ je relativno prost sa svim prostim djeliteljima broja n. Stoga je $(p - 1, n) = 1$ i $p \mid 2^1 - 1 = 1$.

To je kontradikcija s pretpostavkom da n ima proste djelitelje pa mora biti $n = 1$. Lako se provjeri da je to jedino rješenje zadatka.

Zadatak 2.32. Odredite sve $n \in \mathbb{N}$ takve da $n \mid a^{n+1} - a$ za sve $a \in \mathbb{Z}$.

Rješenje. Primijetimo prvo da n mora biti kvadratno slobodan. Inače, ako $p^2 \mid n$, dobivamo kontradikciju za $n = p$ jer tada $p^{n+1} - p \equiv -p \pmod{p^2}$.

Neka je $n = p_1 \ldots p_k$, $p_1 < \ldots < p_k$, i neka je a_i primitivni korijen mod p_i. Zbog $p_i \mid a_i^{n+1} - a_i$ slijedi da $p_i - 1 \mid (n + 1) - 1 = n$. Sada ćemo redom dati ograničenja na brojeve p_i.

Kako je $(p_1 - 1, p_1 \dots p_k) = 1$, mora biti $p_1 = 2$.
Kako je $(p_2 - 1, p_1 \dots p_k) = (p_2 - 1, p_1) = 2$, mora biti $p_2 = 3$.
Kako je $(p_3 - 1, p_1 \dots p_k) = (p_3 - 1, p_1 p_2) \mid 6$, mora biti $p_3 = 7$.
Kako je $(p_4 - 1, p_1 \dots p_k) = (p_4 - 1, p_1 p_2 p_3) \mid 42$, mora biti $p_4 = 43$.
Kako je $(p_5 - 1, p_1 \dots p_k) = (p_5 - 1, p_1 p_2 p_3 p_4) \mid 1806$, mora biti $p_5 - 1 \mid 1807$, ali ne postoji takav prost broj veći od 43.
Dakle, sva rješenja su $n = 1, 2, 6, 42, 1806$.

Zadatak 2.33. Odredite sve proste brojeve p, q takve da za sve $a \in \mathbb{Z}$ vrijedi $3pq \mid a^{3pq} - a$.

Rješenje. Brojevi p, q moraju biti različiti od 3, inače uzimanjem $a = 3$ dobivamo kontradikciju mod 9. Također je $p \neq q$, inače uzimanjem $a = p$ dobivamo kontradikciju mod p^2. Neka je BSO $p < q$.

Neka je a primitivni korijen mod p. Tada vrijedi

$$p \mid a^{3pq} - a \implies p - 1 \mid 3pq - 1 \implies p - 1 \mid 3q - 1.$$

Analogno se dobiva $q - 1 \mid 3p - 1$. Kako je $p < q$, to znači da je $3p - 1 = k(q - 1)$ za neki $k \leq 3$. Slučajeve $k = 1, 3$ možemo eliminirati promatranjem mod 3 pa mora vrijediti $3p - 1 = 2(q - 1) \implies q = \frac{3p+1}{2}$. Zaključujemo sljedeće:

$$p - 1 \mid 3q - 1 \implies p - 1 \mid 3\frac{3p + 1}{2} - 1 = \frac{9p + 1}{2} \implies p - 1 \mid 9p + 1 \implies p - 1 \mid 10.$$

Stoga je $p \in \{2, 11\}$. Iz jednakosti $q = \frac{3p+1}{2}$ zaključujemo da je $p = 11$, $q = 17$. Nije teško provjeriti da je $a^{3 \cdot 11 \cdot 17} - a$ djeljivo s $3 \cdot 11 \cdot 17$ za sve $a \in \mathbb{Z}$.

Zadatak 2.34. Ako su p, q prosti brojevi takvi da je $q \mid 2^p + 3^p$, dokažite da je $q = 5$ ili $q > p$.

Rješenje. Očito $q \neq 2, 3$, pretpostavimo da je $q \geq 7$. Vrijedi

$$q \mid 3^{2p} - 2^{2p}, 3^{q-1} - 2^{q-1} \implies q \mid 3^{(2p,q-1)} - 2^{(2p,q-1)}.$$

Ako je $q \leq p$, tada je $(q - 1, 2p) = (q - 1, 2) \mid 2$ pa $q \mid 3^2 - 2^2 = 5$ i dobivamo kontradikciju. Dakle, mora biti $q > p$.

Zadatak 2.35. Odredite sve proste brojeve p, q takve da $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Rješenje. Očito $p, q \neq 2, 5$. Znamo da je $5^p - 2^p \equiv 3 \pmod{p}$ i $5^q - 2^q \equiv 3 \pmod{q}$. Pretpostavimo prvo da $p, q \neq 3$. Onda mora vrijediti

$$p \mid 5^q - 2^q, 5^{p-1} - 2^{p-1} \implies p \mid 5^{(q,p-1)} - 2^{(q,p-1)},$$

$$q \mid 5^p - 2^p, 5^{q-1} - 2^{q-1} \implies q \mid 5^{(p,q-1)} - 2^{(p,q-1)}.$$

Neka je BSO $p \leq q$. Tada je $(p - 1, q) = 1$ pa $q \mid 5 - 2 = 3$, kontradikcija.

Stoga je bar jedan od p, q jednak 3. Pretpostavimo da je $p = 3$. Tada

$$3q \mid (5^3 - 2^3)(5^q - 2^q) = 117(5^q - 2^q) \implies q \mid 117(5 - 2) = 3^3 \cdot 17.$$

Stoga su sva rješenja $(p, q) = (3, 3), (3, 17), (17, 3)$. Lako se provjeri da su to zaista rješenja.

Zadatak 2.36. Neka je n prirodan broj. Odredite najmanji $m \in \mathbb{N}$ takav da je $a^m \equiv 1 \pmod{n}$ za svaki cijeli broj a relativno prost s n.

Rješenje. Neka je $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Ako je $a^m \equiv 1 \pmod{n}$, tada je nužno i $a^m \equiv 1 \pmod{p_i^{\alpha_i}}$ za svaki $i \in \{1, \dots, k\}$. Stoga mora vrijediti

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) \mid m, \quad i \in \{1, \dots, k\}$$

(jer možemo uzeti da je a primitivni korijen mod $p_i^{\alpha_i}$). Dakle $[p_1^{\alpha_1 - 1}(p_1 - 1), \dots, p_k^{\alpha_k - 1}(p_k - 1)] \mid m$.

Neka je sada $m = [p_1^{\alpha_1 - 1}(p_1 - 1), \dots, p_k^{\alpha_k - 1}(p_k - 1)]$. Uzmimo cijele brojeve $a_1, \dots, a_k$ koji su primitivni korijeni mod $p_1^{\alpha_1 - 1}(p_1 - 1), \dots, p_k^{\alpha_k - 1}(p_k - 1)$. Po CRT-u postoji rješenje sustava

$$a \equiv a_i \pmod{p_i^{\alpha_i}}, \quad i \in \{1, \dots, k\}.$$

Tada vrijedi $a^m \equiv 1 \pmod{p_i^{\alpha_i}}$ pa je $a^m \equiv 1 \pmod{n}$. Dakle, rješenje je $m = [p_1^{\alpha_1 - 1}(p_1 - 1), \dots, p_k^{\alpha_k - 1}(p_k - 1)]$.

Napomena: Carmichaelovi brojevi su složeni brojevi $n \in \mathbb{N}$ takvi da za sve $b \in \mathbb{Z}$ vrijedi $b^n \equiv b \pmod{n}$. Primijetie da su svi Carmichaelovi brojevi ujedno i Fermat pseudoprosti.

Uz korištenje prošlog zadatka nije teško dokazati Korseltov teorem koji kaže da je složen broj $n \in \mathbb{N}$ Carmichaelov ako i samo ako je kvadratno slobodan te za sve proste brojeve p vrijedi $p \mid n \implies p - 1 \mid n - 1$.