Diskretna matematika 2

Zadaća 5

March 23, 2025

Borna Gojšić

---

1. Odredite red od
   a) 5 modulo 17,
   b) 7 modulo 29,

   Je li 5 primitivni korijen modulo 17? Je li 7 primitivni korijen modulo 29?

Rj:

a) Neka je d red od 5 modulo 17. Tada imamo $d \mid \varphi(17) = 16 = 2^4$.

$$5^2 \equiv 25 \equiv 8 \pmod{17}, \quad 5^4 \equiv 8^2 \equiv 64 \equiv 13 \equiv -4 \pmod{17}$$

$$5^8 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$$

Dakle, red od 5 modulo 17 je 16, tj. 5 je primitivni korijen modulo 17.

b) Neka je d red od 7 modulo 29. Tada imamo $d \mid \varphi(29) = 28 = 2^2 \cdot 7$.

$$7^2 \equiv 49 \equiv 20 \equiv -9 \pmod{29}, \quad 7^4 \equiv (-9)^2 \equiv 81 \equiv 23 \equiv -6 \pmod{29}$$

$$7^7 \equiv (-6) \cdot (-9) \cdot 7 \equiv 54 \cdot 7 \equiv 25 \cdot 7 \equiv -4 \cdot 7 \equiv -28 \equiv 1 \pmod{29}$$

Dakle, red od 7 modulo 29 je 7.

2. Neka je p neparan prost broj i $n = 3^p + 1$. Odredite red od 3 modulo n.

Rj:

$$3^p \equiv -1 \pmod{n} \implies 3^{2p} \equiv 1 \pmod{n}$$

Dakle, red od 3 modulo n je $2p$.

3. Neka je p prost broj te neka je red od a modulo p jednak 8. Ako je $x = a^2$, $y = a^3 - a$, $z = a^3 + a$, dokažite da je $x^2 \equiv -1 \pmod{p}$, $y^2 \equiv 2 \pmod{p}$, $z^2 \equiv -2 \pmod{p}$.

Rj: Ako je $a^8 \equiv 1 \pmod{p}$, onda imamo $(a^4)^2 - 1 = (a^4-1)(a^4+1) = kp$. Imamo $\text{nzd}(a^4-1, a^4+1) \mid 2$. Budući da je red od a modulo p jednak 8 i p je neparan prost broj, znamo da je $p \nmid a^4 - 1$. Dakle, imamo $p \mid a^4 + 1$, tj. $a^4 \equiv -1 \pmod{p}$. Odavde imamo $x^2 = (a^2)^2 \equiv -1 \pmod{p}$. Nadalje, imamo:

$$(a^3 \pm a)^2 = a^6 \pm 2a^4 + a^2 \equiv a^2(a^4 + 1) \pm 2a^4 \equiv a^2 \cdot 0 \pm 2 \cdot (-1) \equiv \mp 2 \pmod{p}$$

Ovavde trivijalno slijedi $y^2 \equiv 2 \pmod{p}$ i $z^2 \equiv -2 \pmod{p}$

4. Neka je p prost broj koji ne dijeli a, te neka je red od a modulo p jednak 3. Dokažite sljedeće tvrdnje:
   a) $p \equiv 1 \pmod 3$,
   b) $a^2 + a + 1 \equiv 0 \pmod p$,
   c) $(2a+1)^2 \equiv -3 \pmod p$,
   d) red od $a+1$ modulo p jednak je 6.

Rj:

a) Budući da je red d od a modulo p jednak 3, imamo $d \mid \varphi(p) = p - 1$. Dakle, $p - 1 = 3k$ za neki $k \in \mathbb{N}$, tj. $p \equiv 1 \pmod 3$.

b)
$$a^3 - 1 \equiv 0 \pmod p \implies (a-1)(a^2+a+1) \equiv 0 \pmod p$$
Budući da je red od a modulo p jednak 3, imamo $a - 1 \not\equiv 0 \pmod p$. Dakle, $a^2 + a + 1 \equiv 0 \pmod p$.

c)
$$(2a+1)^2 = 4a^2 + 4a + 1 = 4(a^2+a+1) - 3 \equiv -3 \pmod p$$

d)
$$(a+1)^2 \equiv a^2 + 2a + 1 \equiv 2(a^2+a+1) - a - 1 \equiv -a - 1 \pmod p$$
Dakle, budući da red od a modulo p nije 2 imamo $a \not\equiv -1 \pmod p$, tj.
$$(a+1)^2 \equiv -a - 1 \not\equiv 0 \pmod p$$
Nadalje,
$$(a+1)^3 \equiv a^3 + 3a^2 + 3a + 1 \equiv 1 + 3(a^2+a+1) - 2 \equiv -1 \pmod p$$
Sada je očito da je:
$$(a+1)^6 \equiv ((a+1)^3)^2 \equiv (-1)^2 \equiv 1 \pmod p$$
Dakle, red od $a+1$ modulo p je 6.

5. a) Koliko ima primitivnih korijena modulo 43? Odredite najmanji medu njima.
   b) Koliko ima primitivnih korijena modulo 59? Odredite najmanji medu njima.

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

a) Dakle, postoji $\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = 1 \cdot 2 \cdot 6 = 12$ primitivnih korijena modulo 43. Nađimo sad najmanji od njih:
$$2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^6 \equiv 64 \equiv 21, \quad 2^7 \equiv 42 \equiv -1 \pmod{43} \implies 2^{14} \equiv 1 \pmod{43}$$
$$3^2 \equiv 9, \quad 3^3 \equiv 27, \quad 3^6 \equiv 729 \equiv -2, \quad 3^7 \equiv -6, \quad 3^{14} \equiv 36 \equiv -7$$
$$3^{21} \equiv 42 \equiv -1 \pmod{43}$$
Dakle, najmanji primitivni korijen modulo 43 je 3.

b) Dakle, postoji $\varphi(58) = \varphi(2 \cdot 29) = 1 \cdot 28 = 28$ primitivnih korijena modulo 59.

$$2^{29} \equiv 2 \cdot (4)^{19} \equiv 8 \cdot 64^6 \equiv 8 \cdot 5^6 \equiv 8 \cdot 125^2 \equiv 8 \cdot 7^2 \equiv 8 \cdot 49 \equiv 8 \cdot -10 \equiv -80 \not\equiv 1 \pmod{59}$$

Dakle, najmanji primitivni korijen modulo 59 je 2.

6. Odredite sve primitivne korijene
   a) modulo 31,
   b) modulo 23.

Rj: Znamo da $d \mid \varphi(p) = p-1$ i znamo da postoji točno $\varphi(p-1)$ primitivnih korijena modulo p. Također, neka je a primitivni korijen modulo p i $n \in \mathbb{N}$ takav da je $\text{nzd}(n, \varphi(p)) = 1$. Trivijalno vidimo da je $(a^n)^{\varphi(p)} \equiv 1^n \equiv 1 \pmod{p}$. Preptostavimo da postoji $m \leq \varphi(p)$ takav da je $(a^n)^m \equiv a^{mn} \equiv 1 \pmod{p}$. Budući da je red od a modulo p jednak $\varphi(p)$, imamo $\varphi(p) \mid mn$. Budući da je $\text{nzd}(n, \varphi(p)) = 1$, imamo $\varphi(p) \mid m$, tj. $m \geq \varphi(p)$ pa imamo $m = \varphi(p)$. Dakle, tada je i a^n primitivni korijen modulo p.

a) Dakle, $d \mid 30 = 2 \cdot 3 \cdot 5$. Dakle, $d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$ i imamo $\varphi(30) = 1 \cdot 2 \cdot 4 = 8$ primitivnih korijena modulo 31.

$$2^5 \equiv 32 \equiv 1 \pmod{31}$$

2 nije primitivni korijen modulo 31 pa ne moramo provjeravati brojeve oblike 2^α.

$$3^2 \equiv 9, \quad 3^3 \equiv 27 \equiv -4, \quad 3^5 \equiv -36 \equiv -5, \quad 3^6 \equiv 16, \quad 3^{10} \equiv 25, \quad 3^{15} \equiv 30 \pmod{31}$$

Dakle, 3 je primitivni korijen modulo 31.

$$3^7 \equiv 16 \cdot 3 \equiv 48 \equiv 17, \quad 3^{11} \equiv -6 \cdot 3 \equiv 13, \quad 3^{13} \equiv -6 \cdot -4 \equiv 24, \quad 3^{17} \equiv -1 \cdot 9 \equiv 22 \pmod{31}$$

$$3^{19} \equiv -1 \cdot (-4) \cdot 3 \equiv 12, \quad 3^{23} \equiv 12 \cdot -4 \cdot 3 \equiv 36 \cdot -4 \equiv -20 \equiv 11 \pmod{31}$$

$$3^{29} \equiv 12 \cdot -6 \equiv -72 \equiv 21 \pmod{31}$$

Dakle, svi primitivni korijeni modulo 31 su 3, 11, 12, 13, 17, 21, 22 i 24.

b) Dakle, $d \mid 22 = 2 \cdot 11$. Dakle, $d \in \{1, 2, 11, 22\}$ i imamo $\varphi(22) = 10$ primitivnih korijena modulo 23.

$$2^{11} \equiv 2 \cdot 9^2 \equiv 2 \cdot 81 \equiv 2 \cdot 12 \equiv 24 \equiv 1 \pmod{23}$$

$$3^{11} \equiv 3 \cdot 9 \cdot 9^4 \equiv 27 \cdot 12^2 \equiv 4 \cdot 144 \equiv 4 \cdot 6 \equiv 24 \equiv 1 \pmod{23}$$

Ne moramo provjeravati $n = 2^\alpha 3^\beta$ jer je $n^{11} \equiv 1 \pmod{23}$.

$$5^2 \equiv 25 \equiv 2, \quad 5^{11} \equiv 5 \cdot 25 \cdot 25^4 \equiv 10 \cdot 4^2 \equiv 10 \cdot 16 \equiv 160 \equiv 22 \pmod{23} \quad \checkmark$$

5 je primitivni korijen modulo 23. Dakle, svi ostali primitivni korijeni su oblika 5^n gdje je $\text{nzd}(n, 22) = 1$. Dakle, imamo

$$5^3 \equiv 25 \cdot 5 \equiv 10, \quad 5^5 \equiv 10 \cdot 2 \equiv 20, \quad 5^7 \equiv 20 \cdot 10 \equiv -30 \equiv 17 \pmod{23}$$

$$5^9 \equiv 17 \cdot 2 \equiv 34 \equiv 11, \quad 5^{13} \equiv 11 \cdot 2 \cdot 2 \equiv -1 \cdot 2 \equiv 21, \quad 5^{15} \equiv -2 \cdot 2 \equiv -4 \equiv 19 \pmod{23}$$

$$5^{17} \equiv -4 \cdot 2 \equiv -8 \equiv 15, \quad 5^{19} \equiv -8 \cdot 2 \equiv -16 \equiv 7, \quad 5^{21} \equiv 7 \cdot 2 \equiv 14 \pmod{23}$$

Dakle, svi primitivni korijeni modulo 23 su 5, 7, 10, 11, 14, 15, 17, 19, 20 i 21.

7. Odredite sve proste module koji imaju točno 32 primitivna korijena.

Rj: Ako je p prost broj, onda postoji točno $\varphi(p-1)$ primitivnih korijena modulo p. Dakle, u ovom slučaju imamo $\varphi(p-1) = 32 = 2^5$. Neka je $n = p-1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Tada imamo $\varphi(n) = (p_1-1)p_1^{\alpha_1-1} \cdots (p_k-1)p_k^{\alpha_k-1}$. Iz $p_i - 1 \mid 32$ imamo $p_i - 1 \in \{1,2,4,8,16,32\}$, tj. $p_i \in \{2,3,5,17\}$. Imamo par slučejeva:

1. Ako je $p_i = 17$, onda imamo $n = 17 \cdot k$ pa je $\varphi(n) = 16 \cdot \varphi(k) = 32$, tj. $\varphi(k) = 2$ pa je $k \in \{3,4,6\}$, tj. $n \in \{51, 68, 102\}$. Dakle, $p \in \{52, 69, 103\}$, a od njih je samo 103 prost.
2. Ako je $n = 5 \cdot 3 \cdot 2^\alpha$, imamo $\varphi(n) = 4 \cdot 2^\alpha = 32$, tj. $\alpha = 3$ pa je $n = 120$. Dakle, $p = 121$, ali to nije prost broj.
3. Ako je $n = 5 \cdot 2^\alpha$, imamo $\varphi(n) = 4 \cdot 2^{\alpha-1} = 32$, tj. $\alpha = 4$ pa je $n = 80$. Dakle, $p = 81$, ali to nije prost broj.
4. Ako je $n = 3 \cdot 2^\alpha$, imamo $\varphi(n) = 2^\alpha = 32$, tj. $\alpha = 5$ pa je $n = 96$. Dakle, $p = 97$ što je prost broj.
5. Ako je $n = 2^\alpha$, onda je $\varphi(n) = 2^{\alpha-1} = 32$, tj. $\alpha = 6$ pa je $n = 64$. Dakle, $p = 65$, ali to nije prost broj.

Dakle, svi prosti brojevi koji imaju točno 32 primitivna korijena su 97 i 103.

8. Riješite pomoću indeksa sljedeće kongruencije:
   a) $2x^{16} \equiv 5 \pmod{31}$,
   b) $36x^{15} \equiv 26 \pmod{37}$,
   c) $41x^9 \equiv 22 \pmod{43}$,
   d) $15x^6 \equiv 11 \pmod{53}$.

Rj:

a) 3 je primitivni korijen modulo 31. Dakle, imamo:

$$\operatorname{ind}_3 2 + 16 \cdot \operatorname{ind}_3 x \equiv \operatorname{ind}_3 5 \pmod{30} \implies 24 + 16 \cdot \operatorname{ind}_3 x \equiv 20 \pmod{30}$$

$$16 \cdot \operatorname{ind}_3 x \equiv 26 \pmod{30} \implies 8 \cdot \operatorname{ind}_3 x \equiv 13 \pmod{15} \implies \operatorname{ind}_3 x \equiv 11 \pmod{15}$$

Dakle, $\operatorname{ind}_3 x \in \{11, 26\}$, tj. $x \equiv 13, 18 \pmod{31}$.

b) 2 je primitivni korijen modulo 37. Dakle, imamo:

$$\operatorname{ind}_2(-1) + 15 \cdot \operatorname{ind}_2 x \equiv \operatorname{ind}_2 26 \pmod{36} \implies 18 + 15 \cdot \operatorname{ind}_2 x \equiv 12 \pmod{36}$$

$$15 \cdot \operatorname{ind}_2 x \equiv 30 \pmod{36} \implies 5 \cdot \operatorname{ind}_2 x \equiv 10 \pmod{12}$$

Budući da je $\operatorname{nzd}(5,12) = 1$, imamo $\operatorname{ind}_2 x \equiv 2 \pmod{12}$, tj. $\operatorname{ind}_2 x \equiv 2, 14, 26 \pmod{36}$. Dakle, $x \equiv 3, 4, 30 \pmod{37}$.

c) 3 je primitivni korijen modulo 43. Dakle, imamo:

$$\text{ind}_3(-1) + \text{ind}_3(2) + 9 \cdot \text{ind}_3 x \equiv \text{ind}_3 22 \pmod{42} \implies 21 + 27 + 9 \cdot \text{ind}_3 x \equiv 15 \pmod{42}$$

$$9 \cdot \text{ind}_3 x \equiv 9 \pmod{42} \implies 3 \cdot \text{ind}_3 x \equiv 3 \pmod{14}$$

Budući da je $\text{nzd}(3, 14) = 1$, imamo $\text{ind}_3 x \equiv 1 \pmod{14}$, tj. $\text{ind}_3 x \equiv 1, 15, 29 \pmod{42}$. Dakle, $x \equiv 3, 18, 22 \pmod{43}$.

d) 2 je primitivni korijen modulo 53. Dakle, imamo:

$$\text{ind}_2 15 + 6 \cdot \text{ind}_2 x \equiv \text{ind}_2 11 \pmod{52} \implies 12 + 6 \cdot \text{ind}_2 x \equiv 6 \pmod{52}$$

$$6 \cdot \text{ind}_2 x \equiv -6 \pmod{52} \implies 3 \cdot \text{ind}_2 x \equiv -3 \pmod{26}$$

Dakle, $\text{ind}_2 x \equiv 25 \pmod{26}$, tj. $\text{ind}_2 x \equiv 25, 51 \pmod{52}$. Dakle, $x \equiv 26, 27 \pmod{53}$.

9. Riješite pomoću indeksa sljedeće kongruencije:
   a) $7^x \equiv 6 \pmod{17}$,
   b) $17^x \equiv 27 \pmod{31}$,
   c) $28^x \equiv 27 \pmod{43}$,
   d) $10^x \equiv 8 \pmod{59}$.

Rj:

a) 3 je primitivni korijen modulo 17. Dakle, imamo:

$$x \,\text{ind}_3 7 \equiv \text{ind}_3 6 \pmod{16} \implies 11x \equiv 15 \pmod{16} \implies x \equiv -3 \equiv 13 \pmod{16}$$

jer je $3^{11} \equiv 7 \pmod{17}$ i $3^{15} \equiv 6 \pmod{17}$.

b) 3 je primitivni korijen modulo 31. Dakle, imamo:

$$x \,\text{ind}_3 17 \equiv \text{ind}_3 27 \pmod{30} \implies 7x \equiv 3 \pmod{30} \implies x \equiv 9 \pmod{30}$$

c) 3 je primitivni korijen modulo 43. Dakle, imamo:

$$x \,\text{ind}_3 28 \equiv \text{ind}_3 27 \pmod{42} \implies 5x \equiv 3 \pmod{42} \implies x \equiv 9 \pmod{42}$$

d) 2 je primitivni korijen modulo 59. Dakle, imamo:

$$x \,\text{ind}_2 10 \equiv \text{ind}_2 8 \pmod{58} \implies 7x \equiv 3 \pmod{58} \implies x \equiv 17 \pmod{58}$$