PRIMITIVNI KORIJENI. RJEŠAVANJE KONGRUENCIJA POMOĆU INDEKSA

Zadaća 5.

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?

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

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 $x^2 \equiv -1 \pmod{p}$, $y^2 \equiv 2 \pmod{p}$, $z^2 \equiv -2 \pmod{p}$.

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.

5. (a) Koliko ima primitivnih korijena modulo 43? Odredite najmanji među njima.

   (b) Koliko ima primitivnih korijena modulo 59? Odredite najmanji među njima.

6. Odredite sve primitivne korijene

   (a) modulo 31,

   (b) modulo 23.

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

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) $15x^6 \equiv 11 \pmod{53}$.

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) $10^x \equiv 8 \pmod{59}$.