Naloge iz primitivnih korenov in kvadratnih ostankov

Luka Urbanc (luka.urbanc24@gmail.com)

22. november 2024

1 Primitivni koreni

Naloga 1.1

Koliko elementov reda k obstaja modulo p?

Naloga 1.2

Za katera praštevila p obstaja $x \in \mathbb{N}$, da je $x^4 \equiv -1 \pmod{p}$?

Naloga 1.3

Za vse $p \in \mathbb{P}$, $k \in \mathbb{N}$ izračunaj vsoto

$$\sum_{n=1}^{p-1} n^k \pmod{p}.$$

Naloga 1.4

Dokaži, da če za $p \in \mathbb{P}$, $p \geq 5$ vsoto

$$\sum_{n=1}^{p-1} \frac{1}{n}$$

zapišemo kot okrajšani ulomek, bo njegov števec deljiv s p^2.

Naloga 1.5

Naj bo $5 \leq p \in \mathbb{P}$. Dokaži, da lahko števila od 1 do $p-1$ v nekem vrstnem redu postaviš na krožnico tako, da za vsaka tri zaporedna števila a, b, c velja $p \mid b^2 - ac$.

Naloga 1.6

Izračunaj produkt primitivnih korenov modulo p za vsak $p \in \mathbb{P}$.
Bonus: izračunaj tudi njihovo vsoto.

Naloga 1.7

Naj bo $3 \leq p \in \mathbb{P}$. Dokaži, da obstaja permutacija $1, \ldots, p-1$ $a_1, a_2, \ldots, a_{p-1}$, da je $\sum_{i=1}^{p-1} i^{a_i}$ deljiv s p.

Naloga 1.8

Določi vse $j \in \mathbb{N}$, za katere

$$2021 \mid \sum_{\substack{1 \leq n \leq 2021 \\ \gcd(n, 2021)=1}} n^j.$$

Naloga 1.9

Naj so $a, b, c \in \mathbb{N}$. Dokaži, da obstaja $k \in \mathbb{N}$, da velja $\gcd(a^k + bc, b^k + ca, c^k + ab) > 1$.

Naloga 1.10

Naj sta $x, y \in \mathbb{Z}$ in $p \in \mathbb{P}$. Denimo, da obstajata $m, n \in \mathbb{N}$, $\gcd(m, n) = 1$, da velja $x^m \equiv y^n \pmod{p}$. Dokaži, da obstaja natanko en $z \pmod{p}$, da je $x \equiv z^n \pmod{p}$ in $y \equiv z^m \pmod{p}$.

Naloga 1.11

Naj bo $p \in \mathbb{P}, k \in \mathbb{N}$ in g primitivni koren mod p.

a) Če $k \mid p-1$, dokaži, da je $x^{\frac{p-1}{k}} - 1 \equiv \prod_{t=1}^{\frac{p-1}{k}} (x - g^{tk}) \pmod{p}$.

b) Dokaži, da je $x^{\frac{p-1}{\gcd(k,p-1)}} - 1 \equiv \prod_{t=1}^{\frac{p-1}{\gcd(k,p-1)}} (x - g^{t \gcd(k,p-1)}) \pmod{p}$.

c) Dokaži, da je $\prod_{i=1}^{p-1} (x - i^k) \equiv \left(x^{\frac{p-1}{\gcd(k,p-1)}} - 1 \right)^{\gcd(k,p-1)} \pmod{p}$.

Naloga 1.12

Naj bosta $p \in \mathbb{P}, k \in \mathbb{N}$. Denimo, da so za $0 \leq i \leq p-1$ števila $a_i = i^k + i$ paroma različna modulo p. Določi vse možne vrednosti $a_2 \pmod{p}$.

2 Kvadratni ostanki

Naloga 2.1

Naj bo $n \in \mathbb{N}, 4n+1 = p \in \mathbb{P}$. Dokaži $p \mid n^n - 1$.

Naloga 2.2

Naj bo $p \in \mathbb{P}$. Dokaži, da obstaja $x \in \mathbb{N}$, da $p \mid x^2 - x + 3$, natanko tedaj, ko obstaja $y \in \mathbb{N}$, da $p \mid y^2 - y + 25$.

Namig: najprej dokaži splošno lemo. Če so $a, b, c \in \mathbb{Z}$, $p \in \mathbb{P}$ in $p \nmid a$, potem ima enačba $ax^2 + bx + c \equiv 0 \pmod{p}$ rešitev, če in samo če $\left(\frac{b^2-4ac}{p}\right) \in \{0, 1\}$.

Naloga 2.3

Dokaži, da za $n \in \mathbb{N}$ $2^n + 1$ nima prafaktorjev, kongruentnih $7 \pmod{8}$.

Naloga 2.4

Pokaži, da $\frac{x^2+1}{y^2-5}$ ni celo število za vse naravne $x, y \geq 3$.

Naloga 2.5

Dokaži, da imajo vsi lihi delitelji števil oblike $5x^2+1$ ($x \in \mathbb{N}$) sodo števko na desetiškem mestu.

Naloga 2.6

Dokaži, da za lihi naravni števili $m, n \geq 3$ $2^m - 1$ ne deli $3^n - 1$.

Naloga 2.7

Dokaži, da $5^n - 3^n$ ni deljiv z $2^n + 65$ za vse $n \in \mathbb{N}$.

Naloga 2.8

Dokaži, da za $x, y, z \in \mathbb{N}$ $4xyz - x - y$ ni popoln kvadrat.

Naloga 2.9

Izračunaj vsoto

$$\left\lfloor \frac{2^0}{2003} \right\rfloor + \left\lfloor \frac{2^1}{2003} \right\rfloor + \cdots + \left\lfloor \frac{2^{2001}}{2003} \right\rfloor.$$

Naloga 2.10

Reši enačbo $y^2 = x^3 - 5$ za $x, y \in \mathbb{Z}$.

Naloga 2.11

Dokaži, da za $a, b, c \in \mathbb{Z}$, $abc \neq 0$, velja, da $3(ab + bc + ca)$ ne deli $a^2 + b^2 + c^2$.

Naloga 2.12

Dokaži, da če za naravni števili m, n velja $\varphi(5^m - 1) = 5^n - 1$, potem $\gcd(m, n) > 1$.