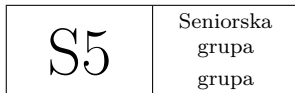


Sustavi ostataka i mali Fermatov teorem



Seniorska grupa
grupa

Predavanja subotom
Osijek, sezona 2019./2020.

mmm.hr

Mladi nadareni matematičari "Marin Getaldić"



Mladi nadareni matematičari
"Marin Getaldić"

matematicari.mmm

1 Sustavi ostataka

Definicija 1.1 (Potpuni sustav ostataka)

Skup \mathcal{S}_P ćemo nazivati potpuni sustav ostataka modulo n ako se u njemu pojavljuju svi ostaci pri dijeljenju s n , odnosno, $\mathcal{S}_P = \{0, 1, 2, 3, \dots, n-1\}$.

Definicija 1.2 (Reducirani sustav ostataka)

Skup \mathcal{S}_R ćemo nazivati reduciranim sustav ostataka modulo n ako se u njemu pojavljuju svi ostaci pri dijeljenju s n koji su relativno prosti s n , odnosno, formalije zapisano, $\mathcal{S}_R = \{x \mid 0 \leq x < n, \gcd(x, n) = 1\}$.

1.1 Svojstva sustava ostataka

1. Skup $\{0 + a, 1 + a, 2 + a, \dots, (n-1) + a\}$ je potpuni sustav ostataka modulo n za svaki $a \in \mathbb{N}$.
2. Skup $\{0a, 1a, 2a, \dots, (p-1)a\}$ je potpuni sustav ostataka modulo p za svaki p prost broj i a takav da $p \nmid a$.
3. Neka je $\mathcal{S}_R = \{a_0, a_1, \dots, a_k\}$ reducirani sustav ostataka modulo n , i neka je a neki broj relativno prost s n . Onda je skup $\mathcal{A} = \{a \cdot a_0, a \cdot a_1, \dots, a \cdot a_k\}$ reducirani sustav ostataka modulo n gledajući svaki od elemenata skupa modulo n .

2 Mali Fermatov teorem

Teorem 2.1 (Mali fermatov teorem)

Neka je p prost broj i $a \in \mathbb{N}$ t.d. $p \nmid a$, onda vrijedi:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz. Neka je a relativno prost s p . Promotrimo \mathcal{S}_R i $\mathcal{A} = \{a, 2a, \dots, (p-1)a\}$. Znamo da je i \mathcal{A} reducirani sustav ostataka nakon reduciranja članova modulo p pa znamo da je

$$1 \cdot 2 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot \dots \cdot (p-1)a \pmod{p},$$

$$\iff a^{p-1} \equiv 1 \pmod{p}.$$

Ako $p \mid a$ možemo vidjeti da vrijedi $a^p \equiv a \pmod{p}$, a to također vrijedi kada $p \nmid a$ pa zaključujemo da $\forall a \in \mathbb{N}$ vrijedi $a^p \equiv a \pmod{p}$. □

3 Zadaci

1. Odredite ostatak broja 5^{500} sa 7.
2. Pronađi sve p proste brojeve tako da $p \mid 29^p + 1$.
3. Neka $14 \mid a_1 + a_2 + \dots + a_{2019}$ pokažite da onda $14 \mid a_1^7 + a_2^7 + \dots + a_{2019}^7$.
4. Za svaki *prost* broj p dokažite da $a^p \equiv b^p \pmod{p} \implies a^p \equiv b^p \pmod{p^2}$.
5. Neka je m paran broj te neka su

$$\{a_1, a_2, \dots, a_m\} \text{ i } \{b_1, b_2, \dots, b_m\}$$

potpuni sustavi ostataka *modulo* m . Dokažite da

$$\{a_1 + b_1, a_2 + b_2, \dots, a_m + b_m\}$$

nije potpun skup ostataka *modulo* m .

6. Dokažite da za svaki *prost* broj postoji beskonačno mnogo brojeva oblika $2^n - n$, $n \in \mathbb{N}$, koji su djeljivi sa p .
7. Pokažite da za sve p, q proste brojeve postoje $m, n \in \mathbb{N}$ takvi da $p^m + q^n \equiv 1 \pmod{pq}$.
8. Nađi sve prirodne brojeve relativno proste sa svim članovima beskonačnog niza

$$a_n = 2^n + 3^n + 6^n - 1, \quad n \geq 1.$$

9. (Wilsonov teorem) Dokaži da je za prost p ,

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

10. Neka je $p \geq 3$ te neka su

$$\{a_1, a_2, \dots, a_m\} \text{ i } \{b_1, b_2, \dots, b_m\}$$

potpuni sustavi ostataka *modulo* p . Dokažite da

$$\{a_1 b_1, a_2 b_2, \dots, a_m b_m\}$$

nije potpun skup ostataka *modulo* p .

11. Dokažite da ne postoji prirodan broj $n > 1$ takav da $n \mid 2^n - 1$.
12. Neka je $p > 2$ prost broj takav da $3 \mid p - 2$. Neka je

$$S = \{y^2 - x^3 - 1 \mid 0 \leq x, y \leq p - 1 \cap x, y \in \mathbb{Z}\}.$$

Pokaži da je maksimalno p elemenata skupa S djeljivo s p .