

Uvod

U ovom predavanju govorit ćemo o dva važna teorema u teoriji brojeva. Podrazumijeva se znanje iz sustava ostataka i kongruencija. Od sada nadalje, ako ne piše drukčije, podrazumijevat će se da u svim tvrdnjama govorimo o prirodnim brojevima. Mnoge tvrdnje se mogu proširiti tako da obuhvaćaju i cijele brojeve. Oznaka (a, b) označava mjeru ili najmanji zajednički djeljitelj brojeva a i b .

Definicija 1. Skup $\{x_1, x_2, \dots, x_n\}$ zovemo potpuni sustav ostataka modulo n ako daju međusobno različite ostatke pri dijeljenju s n , tj ako vrijedi:

$$x_i \equiv x_j \pmod{n} \implies i = j$$

Definicija 2. Skup $\{y_1, y_2, \dots, y_k\}$ zovemo reducirani sustav ostataka ako je $(y_i, n) = 1$ za $i = 1, \dots, k$ te za svaki $m \in \mathbb{N}$ takav da je $(m, n) = 1$ postoji jedinstven y_i za koji je $m \equiv y_i \pmod{n}$

Teorem 1 (Mali Fermatov teorem). Neka je p prost broj. Ako $p \nmid a$ onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj vrijedi $a^p \equiv a \pmod{p}$

Definicija 3. Neka je $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ definirana ovako: $\varphi(n)$ je jednak broju elemenata iz skupa $\{1, 2, \dots, n\}$ koji su relativno prosti s n . Funkciju φ zovemo EULEROVA FUNKCIJA.

Teorem 2 (Eulerov teorem). Ako je $(a, m) = 1$ onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$

Zadaci

- Dokažite da je broj $2^{70} + 3^{70}$ djeljiv s 13.
- Odredite:
 - ostatak pri dijeljenju broja 5^{5000} sa 7
 - posljednje dvije znamenke broja 3^{400} .
- Odredite zadnje dvije znamenke broja 2^{1000}
- Neka su $a_1, a_2, \dots, a_{2020}$ takvi da $10 | a_1 + a_2 + \dots + a_{2020}$. Dokažite da $10 | a_1^5 + a_2^5 + \dots + a_{2020}^5$
- Ako su p i q različiti prosti brojevi, dokažite $p^{q-1} + q^{p-1} - 1$ djeljiv sa pq
- Dokažite da, ako prost broj p dijeli $a^p - 1$, tada p^2 također dijeli $a^p - 1$
- Dokažite da za svaki prost p postoji beskonačno mnogo brojeva oblika $2^n - n$ koji su djeljivi sa p
- Dokažite da iz bilo kojeg aritmetičkog niza čiji su članovi prirodni brojevi može biti izabran geometrijski niz
- Dokažite da $4k + 3 \nmid n^2 + 1$
- Nađite sve parove (m, n) prirodnih brojeva za koje je $m^2 = n^3 + 7$
- Ako je p prost broj, dokažite da je svaki prost djeljitelj broja $2^p - 1$ veći od p

Teorem 3 (Wilson). Za svaki prost broj p vrijedi: $(p-1)! \equiv -1 \pmod{p}$

- Dokažite Wilsonov teorem

Definicija 4. *Kažemo da je funkcija $\theta : \mathbb{N} \rightarrow \mathbb{R}$ multiplikativna ako je:*

(a) $\theta(1) = 1$

(b) $\theta(mn) = \theta(m)\theta(n)$ za sve m, n takve da je $(m, n) = 1$

13. Dokažite da je φ multiplikativna i da je $\varphi(n) = n * \prod_{p|n} (1 - \frac{1}{p})$

14. Odredite za koje n je $\varphi(n)$ neparan

15. Odredite sve n za koje je $\varphi(n) = 268$

16. Dokažite da je $\sum_{d|n} \varphi(d) = n$

Teorem 4 (Lagrange). *Neka je f polinom sa cjelobrojnim koeficijentima stupnja n , p prost broj te neka p ne dijeli vodeći koeficijent od f . Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p .*

17. Dokažite Lagrangeov teorem

18. Neka je $p \geq 5$ prost broj. Dokažite da je brojnik racionalnog broja $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$ djeljiv s p^2

Rješenja

1. Svaki prirodan broj n može davati ostatak 0, 1 ili 2 pri dijeljenju s 3, odnosno zapisano pomoću kongruencija: $n \equiv 0, 1$ ili $2 \pmod{3}$. Znamo da $a \equiv b \pmod{c} \Rightarrow a^k \equiv b^k \pmod{c}$ za svaki $k \in \mathbb{N}$ pa je $n^2 \equiv 0^2, 1^2$ ili $2^2 \pmod{3}$, odnosno $n^2 \equiv 0, 1$ ili $4 \pmod{3}$. Međutim, kako je $4 \equiv 1 \pmod{3}$, onda je $n^2 \equiv 0$ ili $1 \pmod{3}$. Na identičan način dobivamo da je $n^2 \equiv 0, 1, 4$ ili $9 \pmod{4}$, a kako je $4 \equiv 0 \pmod{4}$ i $9 \equiv 1 \pmod{4}$, znači da je $n^2 \equiv 0$ ili $1 \pmod{4}$, što smo i trebali pokazati.
2. Kako je $b \equiv -1 \pmod{b+1}$, slijedi $b^k \equiv (-1)^k \pmod{b+1}$. $(-1)^k$ može poprimiti samo vrijednosti 1 ili -1 , ovisno o parnosti broja k .
3. $2x + 3 \equiv 4 \pmod{7} \Rightarrow 2x \equiv 1 \equiv 8 \pmod{7} \Rightarrow x \equiv 4 \pmod{7}$, a zadnji korak smijemo napraviti jer su 2 i 7 relativno prosti.
4. Promatramo jednadžbu modulo 3. $15x^2 - 7y^2 \equiv 1 \pmod{3} \Rightarrow -7y^2 \equiv 1 \pmod{3} \Rightarrow 7y^2 \equiv -1 \equiv 2 \pmod{3}$. Kako je $7 \equiv 1 \pmod{3}$, zaključujemo $y^2 \equiv 2 \pmod{3}$, što nije moguće. Dakle, ova jednadžba nema rješenja u cijelim brojevima.
5. Ako je n paran $n^2 + 2n - 1$ je neparan pa nije djeljiv s 4.
Ako je n neparan, tada je $n \equiv -1, 1 \pmod{4}$, pa je $n^2 + 2n - 1 \equiv (-1)^2 + 2 \cdot (-1) - 1 \equiv -2 \pmod{4}$ ili $n^2 + 2n - 1 \equiv 1^2 + 2 \cdot 1 - 1 \equiv 2 \pmod{4}$, u oba slučaja opet nije djeljivo s 4.
- 6.

$$a_n = \begin{cases} 4^n + 3 & \text{za } n \equiv 0 \pmod{2}; \\ 4^n + 2 & \text{za } n \equiv 1 \pmod{2}. \end{cases}$$

Budući da su jedini kvadratni ostaci modulo 4 jednaki 1 ili 0, zaključujemo da se u nizu ne nalazi niti jedan potpun kvadrat.

7. Općinsko 2016. - 3. razred, 7. zadatak
8. Županijsko 2013. - 1. razred, 4. zadatak
9. Državno 2014. - 2. razred 3. zadatak