Додатна настава за први разред
17.11.2004.

Конгруенције

Миливоје Лукић

Потпун систем остатака по модулу m ($m \geq 2$) је сваки скуп A такав да за свако $y \in \mathbb{Z}$ постоји тачно један $x \in A$ такав да је $y \equiv x \pmod{m}$.

Редукован систем остатака по модулу m је сваки скуп A чији су сви елементи узајамно прости са m, и такав да, за свако $y \in \mathbb{Z}$ које је узајамно просто са m, постоји тачно један $x \in A$ такав да је $y \equiv x \pmod{m}$.

Сваки потпун систем остатака по модулу m има тачно m елемената. Сваки редукован систем остатака по модулу m има исти број елемената, и тај број елемената је $\varphi(m)$, где је φ *Ојлерова функција* $\varphi : \mathbb{N} \to \mathbb{N}$. $\varphi(n)$ је број елемената скупа $\{1, 2, \ldots, n\}$ који су узајамно прости са n. Њена вредност је

$$\varphi(1) = 1, \quad \varphi\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)$$

где су p_i различити прости бројеви и α_i природни бројеви, $i = 1,\ 2,\ \ldots,\ k$.
Приметимо да, ако су m и n узајамно прости бројеви, важи

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Мала Фермаова теорема Нека је p прост број. За сваки цео број a узајамно прост са p важи

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

Ојлерова теорема Нека је n природан број. За сваки цео број a узајамно прост са n важи

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Вилсонова теорема За све просте бројеве p важи

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

За природан број $m > 1$, и цео број a узајамно прост са m, *поредак броја a по модулу m* је најмањи природан број δ за који важи $a^\delta \equiv 1 \pmod{m}$, у ознаци $\delta_m(a)$. Тада је

$$m | a^x - 1 \ \Leftrightarrow\ \delta_m(a) | x.$$

Једна последица овога је да увек важи $\delta_m(a) | \varphi(m)$.

Кинеска теорема о остацима Нека су $m_1,\ m_2,\ \ldots,\ m_n$ природни бројеви узајамно прости по паровима, и $a_1,\ a_2,\ \ldots,\ a_n$ цели бројеви. Тада постоје a и m такво да је систем конгруенција $x \equiv a_i \pmod{m_i}$, $i = 1,\ 2,\ \ldots,\ n$, еквивалентан са $x \equiv a \pmod{m}$.

1. Доказати да постоји природан број n, такав да је број $3^n - 1$ дељив са 1990.
2. Доказати да је број $2222^{5555} + 5555^{2222}$ дељив са 7.
3. Да ли постоји $n \in \mathbb{N}$ за које $247 | 2^n + 1$?
4. Доказати да је бар један од природних бројева n, $n+1$, $\ldots$, $n+7$ узајамно прост са сваким од преосталих бројева.
5. Нека су $m, n \in \mathbb{N}$ такви да је $(m, 11k - 1) = (n, 11k - 1)$ за све $k \in \mathbb{N}$. Доказати да је $m/n = 11^s$, за неко $s \in \mathbb{Z}$.

6. Одредити све парове (p, q) простих бројева такве да је $p^2 - 2q^2 = 1$.

7. Одредити све парове (x, y) природних бројева такве да важи $7^x - 3 \cdot 2^y = 1$.

8. Доказати да постоји бесконачно много целих бројева n који се не могу представити у облику $n = a^3 + b^3 + c^3$ ни за које $a, b, c \in \mathbb{Z}$.

9. Нека је p прост број, и k природан број мањи од p. Тада је

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

10. Нека је p прост број, и k природан број мањи од p. Тада је

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

11. Доказати да је за сваки непаран прост број p бројилац m разломка

$$\frac{m}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

дељив са p.

12. Ако је за природне бројеве a и n веће од 1 број $a^n - 1$ прост, онда је $a = 2$ и n је прост број. Бројеви $M_n = 2^n - 1$ називају се Мерсенови бројеви.

13. Ако је за неке природне бројеве a, k веће од 1 број $a^k + 1$ прост, онда је $k = 2^n$. Бројеви овог облика за $a = 2$, називају се Фермаови бројеви $F_n = 2^{2^n} + 1$.

14. Доказати да за све природне бројеве n важи $n^2 | (n+1)^n - 1$.

15. Доказати да за природне бројеве m, n и $a > 1$ важи

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

16. Доказати да за природне бројеве m и n, $m \neq n$, важи

$$\left(2^{2^m} + 1, 2^{2^n} + 1\right) = 1.$$

17. Доказати да за све природне бројеве m и $a > 1$ важи

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m).$$

18. Одредити све парове (m, n) природних бројева такве да важи $mn - 1 | n^3 + 1$.

19. Доказати да за било које $n \in \mathbb{N}$, у низу $2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots$ сви чланови почев од неког дају исти остатак по модулу n.

20. (ИМО2000.предлог) Одредити све природне бројеве $n \geq 2$ који задовољавају следећи услов: За све целе бројеве a, b узајамно просте са n,

$$a \equiv b \pmod{n} \quad \text{ако и само ако} \quad ab \equiv 1 \pmod{n}.$$