Diskretna matematika 2

Zadaća 3

April 27, 2025

Borna Gojšić

---

1. Dokažite da je broj $3^{105} + 4^{105}$ djeljiv sa 7 i 13, a nije djeljiv s 11.

> **Rj:** Imamo $\varphi(7) = 6$, $\varphi(13) = 12$, $\varphi(11) = 10$. Dakle, imamo
>
> $$3^{105} + 4^{105} \equiv 3^3 + 4^3 \equiv 27 + 64 \equiv 91 \equiv 0 \pmod{7},$$
>
> $$3^{105} + 4^{105} \equiv 3^9 + 4^9 \equiv (3^3)^3 + (4^3)^3 \equiv 27^3 + 64^3 \equiv 1^3 + 12^3 \equiv 1 - 1 \equiv 0 \pmod{13},$$
>
> pa je $3^{105} + 4^{105}$ djeljiv s 7 i 13.

2. Odredite ostatak pri dijeljenju broja $1111^{222} \cdot 33^{444}$ s brojem 19.

> **Rj:** Znamo da je $\varphi(19) = 18$, pa je
>
> $$1111^{222} \cdot 33^{444} \equiv 13^6 \cdot 14^{12} = (13 \cdot 196)^6 \equiv 2^6 \equiv 64 \equiv 7 \pmod{19}$$
>
> i stoga je ostatak pri dijeljenju broja $1111^{222} \cdot 33^{444}$ s brojem 19 jednak 7.

3. Odredite ostatak pri dijeljenju broja 73^{73} s brojem 38.

> **Rj:** $\varphi(38) = \varphi(2 \cdot 19) = 18$, pa je
>
> $$73^{73} \equiv 73^1 \equiv 35 \pmod{38}.$$
>
> i stoga je ostatak pri dijeljenju broja 73^{73} s brojem 38 jednak 35.

4. Odredite ostatak pri dijeljenju broja 53^{181} s brojem 105.

> **Rj:** Budući da je $105 = 3 \cdot 5 \cdot 7$, imamo
>
> $$53^{181} \equiv 2^{181} \equiv 2^1 \equiv 2 \pmod{3}$$
> $$53^{181} \equiv 3^{181} \equiv 3^1 \equiv 3 \pmod{5}$$
> $$53^{181} \equiv 4^{181} \equiv 4 \pmod{7}$$
>
> Dakle, imamo sustav kongruencija:
>
> $$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 4 \pmod{7}.$$

Rješavamo sustav kineskom teoremom o ostacima s $m = 105$ i $x_0 = 35x_1 + 21x_2 + 15x_3$, gdje imamo
$$35x_1 \equiv 1 \pmod 3, \quad 21x_2 \equiv 1 \pmod 5, \quad 15x_3 \equiv 1 \pmod 7.$$

$$\begin{aligned} 2x_1 &\equiv 2 \pmod 3 \implies x_1 = 1 \\ x_2 &\equiv 3 \pmod 5 \implies x_2 = 3 \\ x_3 &\equiv 4 \pmod 7 \implies x_3 = 4 \end{aligned}$$

Dakle, imamo $x_0 = 35 + 21 \cdot 3 + 15 \cdot 4 = 158$, pa je $53^{181} \equiv 158 \equiv 53 \pmod{105}$.

5. Odredite ostatak pri dijeljenju broja 314^{162} s brojem 165.

Rj: Budući da je $165 = 3 \cdot 5 \cdot 11$, imamo

$$\begin{aligned} 314^{162} &\equiv 2^{162} \equiv 2^0 \equiv 1 \pmod 3 \\ 314^{162} &\equiv (-1)^{162} \equiv 1 \pmod 5 \\ 314^{162} &\equiv 6^{162} \equiv 6^2 \equiv 3 \pmod{11} \end{aligned}$$

Sada rješavamo sustav kongruencija pomoću CRT:

$$\begin{aligned} 5 \cdot 11x_1 \equiv 1 &\implies x_1 \equiv 1 \pmod 3 \implies x_1 = -2 \\ 3 \cdot 11x_2 \equiv 1 &\implies 3x_2 \equiv 1 \pmod 5 \implies x_1 = 2 \\ 3 \cdot 5x_3 \equiv 3 &\implies 5x_3 \equiv 1 \pmod{11} \implies x_1 = 9 \end{aligned}$$

Dakle, $x_0 = -2 \cdot 55 + 2 \cdot 33 + 9 \cdot 15 = 91$, pa je $314^{162} \equiv 91 \pmod{165}$.

6. Odredite ostatak pri dijeljenju $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$ s 4.

Rj: Budući da je $\varphi(4) = 2$,

$$\sum_{i=1}^{100} i^5 \equiv \sum_{i=1}^{100} i \equiv 25 \sum_{i=1}^{4} i = 25 \cdot 10 \equiv 1 \cdot 2 \equiv 2 \pmod 4.$$

pa je ostatak sume pri dijeljenju s 4 jednak 2.

7. Odredite posljednje dvije znamenke broja 53^{82}.

Rj: Znamo da je $\varphi(100) = 40$, pa je

$$53^{82} \equiv 53^2 \equiv 2809 \equiv 9 \pmod{100}.$$

Dakle, posljednje dvije znamenke broja 53^{82} su 09.

8. Odredite posljednje dvije znamenke broja 71^{245}.

Rj: Znamo da je $\varphi(25) = 20$ i $\varphi(4) = 2$, pa je

$$71^{245} \equiv 71^5 \equiv (-4)^5 \equiv -4 \cdot 16^2 \equiv -4 \cdot (-9)^2 \equiv -4 \cdot 81 \equiv -4 \cdot 6 \equiv -24 \equiv 1 \pmod{25}$$
$$71^{245} \equiv (-1)^{245} \equiv -1 \equiv 3 \pmod{4}$$

Sada rješavamo sustav kongruencija pomoću CRT:

$$4x_1 \equiv 1 \pmod{25} \implies x_1 = 19$$
$$25x_2 \equiv 3 \pmod{4} \implies x_2 \equiv 3 \pmod{4} \implies x_2 = -1$$

Dakle, $x_0 = 4 \cdot 19 + 25 \cdot (-1) = 51$. Dakle, posljednje dvije znamenke broja 71^{245} su 51.

9. a) Odredite posljednje dvije znamenke broja 14^{2012}.
   b) Odredite posljednje tri znamenke broja 14^{2012}.

Rj:

a) Znamo da je $\varphi(25) = 20$ i $\varphi(4) = 2$, pa je

$$14^{2012} \equiv 14^{12} \equiv 196^6 \equiv (-4)^6 \equiv 16^3 \equiv (-9)^3 \equiv -729 \equiv -4 \pmod{25}$$
$$14^{2012} \equiv 0 \pmod{4}$$

Sada rješavamo sustav kongruencija pomoću CRT:

$$4x_1 \equiv -4 \pmod{25} \implies x_1 = -1$$
$$25x_2 \equiv 0 \pmod{4} \implies x_2 \equiv 0 \pmod{4} \implies x_2 = 0$$

Dakle, $x_0 = 4 \cdot -1 + 25 \cdot 0 = -4 \equiv 96 \pmod{100}$. Dakle, posljednje dvije znamenke broja 14^{2012} su 96.

b) Znamo da je $\varphi(125) = 100$ i $\varphi(8) = 4$, pa je

$$14^{2012} \equiv 14^{12} \equiv 196^6 \equiv (71)^6 \equiv 5041^3 \equiv 41^3 \equiv 46 \pmod{125}$$
$$14^{2012} \equiv 0 \pmod{8}$$

Sada rješavamo sustav kongruencija pomoću CRT:

$$8x_1 \equiv 46 \pmod{125} \implies x_1 = 37$$
$$125x_2 \equiv 0 \pmod{8} \implies x_2 = 0$$

Dakle, $x_0 = 8 \cdot 37 + 125 \cdot 0 = 296$. Dakle, posljednje tri znamenke broja 14^{2012} su 296.

10. Odredite posljednje tri znamenke broja $1^{2013} + 2^{2013} + 3^{2013} + \cdots + 1000^{2013}$.

Rj:

$$(1000 - n)^{2013} + n^{2013} \equiv (-n)^{2013} + n^{2013} \equiv 0 \pmod{1000}$$

$$\sum_{i=1}^{1000} i^{2013} \equiv \sum_{i=1}^{499} i^{2013} + 500^3 + \sum_{i=1}^{499} (1000 - i)^{2013} \equiv 0 \pmod{1000}$$

Dakle, posljednje tri znamenke su 000.

11. Neka je p neparan prost broj.
   a) Dokažite da je $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.
   b) Dokažite da je $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$.

Rj:

a)

$$\sum_{i=1}^{p-1} i^{p-1} \equiv \sum_{i=1}^{p-1} 1 \equiv p - 1 \equiv -1 \pmod{p}.$$

b)

$$\sum_{i=1}^{p-1} i^{p-1} \equiv \sum_{i=1}^{p-1} i \equiv \frac{p(p-1)}{2} \equiv 0 \pmod{p}.$$

Posljednja jednakost slijedi iz činjenice da je p neparan, pa je $p - 1$ paran, pa je $p \mid \frac{p(p-1)}{2}$.

12. Neka su m i n relativno prosti prirodni brojevi. Dokažite da je tada

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn},$$

gdje je φ Eulerova funkcija.

Rj: Budući da imamo $\text{nzd}(m, n) = 1$, imamo $m^{\varphi(n)} \equiv 1 \pmod{n}$ i $n^{\varphi(m)} \equiv 1 \pmod{m}$, pa imamo

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 0 + 1 \equiv 1 \pmod{m}$$

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 + 0 \equiv 1 \pmod{n}$$

Sada imamo $m \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$ i $n \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$, pa je $mn \mid m^{\varphi(n)} + n^{\varphi(m)} - 1$.

13. Neka je p prost, te neka su a i b prirodni brojevi takvi da je $a^p \equiv b^p \pmod{p}$. Dokažite da je tada $a^p \equiv b^p \pmod{p^2}$.
Uputa: Koristite identitet $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$, $n \in \mathbb{N}$.

Rj: Po malom Fermatovom teoremu, imamo: $a^p \equiv a \pmod{p}$ i $b^p \equiv b \pmod{p}$. Dakle,

$$a \equiv b \pmod{p}$$

Onda imamo $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv p \cdot a^{p-1} \equiv 0 \pmod{p}$. Dakle, imamo $p \mid a - b$ i $p \mid a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$. Stoga $p^2 \mid (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})$, tj. $a^p \equiv b^p \pmod{p^2}$.