Diskretna matematika 2

Zadaća 2

March 2, 2025

Borna Gojšić

---

1. Dokažite da za svaki prirodan broj n vrijedi
   a) $n^3 \equiv n \pmod 6$
   b) $n^5 \equiv n \pmod{30}$

Rj:

a) Primijetimo da je $n^3 - n = n(n^2-1) = n(n-1)(n+1)$. $n-1$, n i $n+1$ su 3 uzastopna prirodna broja. Dakle, bar 1 od njih je djeljiv s 2 i također bar 1 od njih je djeljiv s 3. Dakle, imamo $2 \mid n^3 - n$ i $3 \mid n^3 - n$, odnosno $6 \mid n^3 - n$, tj. $n^3 \equiv n \pmod 6$.

b) Primijetimo da je $n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = n(n-1)(n+1)(n^2+1)$. Već smo dokazali da $6 \mid n(n+1)(n-1)$. Sada, ako $5 \nmid n, n-1, n+1$, onda imamo $n = 5k \pm 2$ za neki $k \in \mathbb{Z}$. Sada vidimo da je $n^2 + 1 = 25k^2 \pm 20k + 5$, odnosno $5 \mid n^2 + 1$. Dakle, $30 \mid n^5 - n$, tj. $n^5 \equiv n \pmod{30}$.

2. a) Ako je $13x \equiv 13y \pmod{65}$, dokažite da je $x \equiv y \pmod 5$. Vrijedi li obrat te tvrdnje?
   b) Ako je $a \equiv b \pmod m$, dokažite da je $a^2 \equiv b^2 \pmod m$. Vrijedi li obrat te tvrdnje? Obrazložite!

Rj:

a) Ako je $13x \equiv 13y \pmod{65}$, tada je $13(x-y) = 65k$ za neki $k \in \mathbb{Z}$. Iz toga slijedi da je $x - y = 5k$, odnosno $x \equiv y \pmod 5$.
Ako je $x \equiv y \pmod 5$, tada je $x - y = 5k$ za neki $k \in \mathbb{Z}$. Iz toga slijedi da je $13(x-y) = 65k$, odnosno $13x \equiv 13y \pmod{65}$.

b) Ako je $a \equiv b \pmod m$, tada je $a - b = mk$ za neki $k \in \mathbb{Z}$. Iz toga slijedi da je $a^2 - b^2 = (a-b)(a+b) = mk(a+b)$, odnosno $a^2 \equiv b^2 \pmod m$.
Obrat te tvrdnje ne vrijedi. Na primjer, za $m = 5$, $a = 1 \equiv 1 \pmod 5$ i $b = 4 \equiv -1 \pmod 5$ imamo $a^2 \equiv 1 \equiv 1 \equiv b^2 \pmod 5$, ali $a \equiv 1 \not\equiv 4 \equiv b \pmod 5$.

3. Riješite sljedeće kongruencije:
   a) $175x \equiv 252 \pmod{294}$
   b) $415x \equiv 15 \pmod{1115}$
   c) $238x \equiv 350 \pmod{420}$

Rj:

a) Prvo ćemo Euklidovim algoritmom odrediti $d = \gcd(175, 294)$.

a	b	$\lfloor \frac{a}{b} \rfloor$
294	175	1
175	119	1
119	56	2
56	7	8
7	0	

Dakle, $d = 7$. $175 : 7 = 25$, $252 : 7 = 36$, $294 : 7 = 42$. Sada rješavamo kongruenciju $25x \equiv 36 \pmod{42}$. Koristit ćemo prošireni Euklidov algoritam za rješavanje kongruencije.

y	g	v	w	$\lfloor \frac{a}{b} \rfloor$
0	42	1	25	1
1	25	-1	17	1
-1	17	2	8	2
2	8	-5	1	8
-5	1		0	

Dakle, imamo $u \equiv -5 \pmod{42}$. Konačno, $x \equiv -5 \cdot 36 \equiv -180 \equiv 30 \pmod{42}$. Sada su sva rješenja početne kongruencije $x \equiv 30 + 42k \pmod{294}$ za $k \in \{0, 1, 2, 3, 4, 5, 6\}$.

b) Prvo ćemo Euklidovim algoritmom odrediti $d = \gcd(415, 1115) = 5$. $415 : 5 = 83$, $15 : 5 = 3$, $1115 : 5 = 223$. Sada rješavamo kongruenciju $83x \equiv 3 \pmod{223}$.

y	g	v	w	$\lfloor \frac{a}{b} \rfloor$
0	223	1	83	2
1	83	-2	57	1
-2	57	3	26	2
3	26	-8	5	5
-8	5	43	1	5
43	1		0	

Dakle, imamo $u \equiv 43 \pmod{223}$. Konačno, $x \equiv 43 \cdot 3 \equiv 129 \pmod{223}$. Sada su sva rješenja početne kongruencije $x \equiv 129 + 223k \pmod{1115}$ za $k \in \{0, 1, 2, 3, 4\}$.

c) Euklidovim algoritmom dobijemo: $d = \gcd(238, 420) = 14$. Dakle, $238 : 14 = 17$, $350 : 14 = 25$, $420 : 14 = 30$, pa rješavamo kongruenciju $17x \equiv 25 \pmod{30}$.

y	g	v	w	$\lfloor \frac{a}{b} \rfloor$
0	30	1	17	1
1	17	-1	13	1
-1	13	2	4	3
2	4	-7	1	4
-7	1		0	

Dakle, imamo $u \equiv -7 \pmod{30}$. Konačno, $x \equiv -7 \cdot 25 \equiv -175 \equiv 5 \pmod{30}$. Sada su sva rješenja početne kongruencije $x \equiv 5 + 30k \pmod{420}$ za $k \in \{0, 1, 2, 3, \ldots, 12, 13\}$.

4. a) Riješite kongruenciju $159x \equiv 66 \pmod{201}$.
   b) Odredite sve prirodne brojeve n iz intervala $[1100, 1400]$ koji zadovoljavaju kongruenciju $159n \equiv 66 \pmod{201}$.
   c) Odredite sve prirodne brojeve m za koje vrijedi $159 \equiv 66 \pmod{m}$.

Rj:

a) Euklidovim algoritmom dobijemo: $d = \gcd(159, 201) = 3$. Dakle, $159 : 3 = 53$, $66 : 3 = 22$, $201 : 3 = 67$, pa rješavamo kongruenciju $53x \equiv 22 \pmod{67}$.

y	g	v	w	$\left\lfloor \frac{a}{b} \right\rfloor$
0	67	1	53	1
1	53	-1	14	3
-1	14	4	11	1
4	11	-5	3	3
-5	3	19	2	1
19	2	-24	1	2
-24	1		0	

Dakle, imamo $u \equiv -24 \pmod{67}$. Konačno, $x \equiv -24 \cdot 22 \equiv -528 \equiv 8 \pmod{67}$. Sada su sva rješenja početne kongruencije $x \equiv 8, 75, 142 \pmod{201}$.

b) Znamo da je $1100 \equiv 95 \pmod{201}$, pa je najmanji broj iz $[1100, 1400]$ koji zadovoljava kongruenciju $1100 + (142 - 95) = 1147$. Sada lako dobijemo sve brojeve iz intervala $[1100, 1400]$ koji zadovoljavaju kongruenciju: $1147, 1214, 1281, 1348$.

c) $159 \equiv 66 \pmod{m}$ znači $m \mid 159 - 66 = 93$. Rastav 93 na proste faktore je $93 = 3 \cdot 31$. Dakle, $m \in \{1, 3, 31, 93\}$.

5. Riješite sljedeće sustave kongruencija:
   a) $x \equiv 7 \pmod{17}$, $x \equiv 18 \pmod{31}$, $x \equiv 33 \pmod{37}$
   b) $x \equiv 2 \pmod{5}$, $x \equiv 1 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 5 \pmod{17}$
   c) $5x \equiv 3 \pmod{7}$, $16x \equiv 7 \pmod{17}$, $25x \equiv 2 \pmod{37}$.

Rj:

a) Imamo $m = 17 \cdot 31 \cdot 37 = 19499$ i $x_0 = 1147x_1 + 629x_2 + 527x_3$. Dakle, imamo sljedeći sustav:

$$1147x_1 \equiv 7 \pmod{17}, \quad 629x_2 \equiv 18 \pmod{31}, \quad 527x_3 \equiv 33 \pmod{37}$$

$$8x_1 \equiv 7 \pmod{17}, \quad 9x_2 \equiv 18 \pmod{31}, \quad 9x_3 \equiv 33 \pmod{37}$$

Dakle, imamo $x_1 = 3$, $x_2 = 2$ i $x_3 = 16$, $x_0 = 13131$ i $x \equiv 13131 \pmod{19499}$.

b) Imamo $m = 5 \cdot 6 \cdot 11 \cdot 17 = 5610$ i $x_0 = 1122x_1 + 935x_2 + 510x_3 + 330x_4$. Dakle, imamo sljedeći sustav:

$$1122x_1 \equiv 2 \pmod{5}, \quad 935x_2 \equiv 1 \pmod{6}, \quad 510x_3 \equiv 4 \pmod{11}, \quad 330x_4 \equiv 5 \pmod{17}$$

$$2x_1 \equiv 2 \pmod{5}, \quad 5x_2 \equiv 1 \pmod{6}, \quad 4x_3 \equiv 4 \pmod{11}, \quad 7x_4 \equiv 5 \pmod{17}$$

Dakle, imamo $x_1 = 1$, $x_2 = -1$, $x_3 = 1$ i $x_4 = 8$, $x_0 = 3337$ i $x \equiv 3337 \pmod{5610}$.

c) Ovaj sustav ćemo prvo dovesti u oblik $x \equiv a \pmod{m}$ što možemo jer su svi moduli prosti brojevi pa postoje multiplikativni inverzi modulo m_j.

$$5x \cdot 3 \equiv 3 \cdot 3 \pmod 7, \quad 16x \cdot (-1) \equiv 7 \cdot (-1) \pmod{17}, \quad 25x \cdot 3 \equiv 2 \cdot 3 \pmod{37}$$

$$x \equiv 2 \pmod 7, \quad x \equiv 10 \pmod{17}, \quad x \equiv 6 \pmod{37}$$

Sada imamo $m = 7 \cdot 17 \cdot 37 = 4403$ i $x_0 = 629x_1 + 259x_2 + 119x_3$. Dakle, imamo sljedeći sustav:

$$629x_1 \equiv 2 \pmod 7, \quad 259x_2 \equiv 10 \pmod{17}, \quad 119x_3 \equiv 6 \pmod{37}$$

$$-x_1 \equiv 2 \pmod 7, \quad 4x_2 \equiv 10 \pmod{17}, \quad 8x_3 \equiv 6 \pmod{37}$$

Dakle, $x_1 = -2$, $x_2 = 11$, $x_3 = 10$, $x_0 = 2781$ i $x \equiv 2781 \pmod{4403}$.

6. Riješite sljedeće sustave kongruencija:
   a) $x \equiv 10 \pmod{15}$, $x \equiv 19 \pmod{21}$, $x \equiv 25 \pmod{60}$
   b) $x \equiv 13 \pmod{16}$, $x \equiv 5 \pmod{24}$, $x \equiv 8 \pmod{27}$, $x \equiv 2 \pmod 5$.

   Napomena: Uočite da moduli nisu u parovima relativno prosti.

Rj:

a) Kongruencije rastavljamo na kongruencije potencija prostih modula.

$$\begin{aligned} x \equiv 10 \pmod{15} &\implies x \equiv 10 \pmod 3, \quad x \equiv 10 \pmod 5 \\ x \equiv 19 \pmod{21} &\implies x \equiv 19 \pmod 3, \quad x \equiv 19 \pmod 7 \\ x \equiv 25 \pmod{60} &\implies x \equiv 25 \pmod 3, \quad x \equiv 25 \pmod 4, \quad x \equiv 25 \pmod 5 \end{aligned}$$

Dakle, imamo:

$$\begin{aligned} x \equiv 10 \pmod 3, \quad x \equiv 19 \pmod 3, \quad & x \equiv 25 \pmod 3 \implies x \equiv 1 \pmod 3 \\ & x \equiv 25 \pmod 4 \implies x \equiv 1 \pmod 4 \\ x \equiv 10 \pmod 5, \quad & x \equiv 25 \pmod 5 \implies x \equiv 0 \pmod 5 \\ & x \equiv 19 \pmod 7 \implies x \equiv 5 \pmod 7 \end{aligned}$$

Sada možemo primijeniti kineski teorem o ostacima. Imamo $m = 3 \cdot 4 \cdot 5 \cdot 7 = 420$ i $x_0 = 140x_1 + 105x_2 + 84x_3 + 60x_4$. Dakle, imamo sljedeći sustav:

$$140x_1 \equiv 1 \pmod 3, \quad 105x_2 \equiv 1 \pmod 4, \quad 84x_3 \equiv 0 \pmod 5, \quad 60x_4 \equiv 5 \pmod 7$$

$$2x_1 \equiv 1 \pmod 3, \quad x_2 \equiv 1 \pmod 4, \quad 4x_3 \equiv 0 \pmod 5, \quad 4x_4 \equiv 5 \pmod 7$$

Dakle, imamo $x_1 = 2$, $x_2 = 1$, $x_3 = 0$, $x_4 = 3$, $x_0 = 565$ i $x \equiv 565 \equiv 145 \pmod{420}$.

b)

$$\begin{aligned} & x \equiv 13 \pmod{16} \\ & x \equiv 5 \pmod{24} \implies x \equiv 5 \pmod 3, \quad x \equiv 5 \pmod 8 \\ & x \equiv 8 \pmod{27} \\ & x \equiv 2 \pmod 5 \end{aligned}$$

Dakle, imamo:

$$\begin{aligned} x \equiv 13 \pmod{16}, \quad x \equiv 5 \pmod{8} &\implies x \equiv 13 \pmod{16} \\ x \equiv 5 \pmod{3}, \quad x \equiv 8 \pmod{27} &\implies x \equiv 8 \pmod{27} \\ &\qquad\quad x \equiv 2 \pmod{5} \end{aligned}$$

Sada možemo primijeniti kineski teorem o ostacima. Imamo $m = 16 \cdot 27 \cdot 5 = 2160$ i $x_0 = 135x_1 + 80x_2 + 432x_3$. Dakle, imamo sljedeći sustav:

$$135x_1 \equiv 13 \pmod{16}, \quad 80x_2 \equiv 8 \pmod{27}, \quad 432x_3 \equiv 2 \pmod{5}$$

$$7x_1 \equiv 13 \pmod{16}, \quad -x_2 \equiv 8 \pmod{27}, \quad 2x_3 \equiv 2 \pmod{5}$$

Dakle, $x_1 = 11$, $x_2 = -8$, $x_3 = 1$, $x_0 = 1277$ i $x \equiv 1277 \pmod{2160}$.

7. Odredite najmanji prirodan broj koji pri dijeljenju s brojevima 41, 42 i 43 daje ostatke 1, 2 i 3 (u tom redoslijedu).

Rj: Ovo je ekvivalentno rješavanju sustava kongruencija:

$$x \equiv 1 \pmod{41}, \quad x \equiv 2 \pmod{42}, \quad x \equiv 3 \pmod{43}$$

Budući da su 41 i 43 prosti brojevi, možemo koristiti kineski teorem o ostacima. Imamo $m = 74046$ i $x_0 = 1806x_1 + 1763x_2 + 1722x_3$. Dakle, imamo sljedeći sustav:

$$1806x_1 \equiv 1 \pmod{41}, \quad 1763x_2 \equiv 2 \pmod{42}, \quad 1722x_3 \equiv 3 \pmod{43}$$

$$2x_1 \equiv 1 \pmod{41}, \quad 41x_2 \equiv 2 \pmod{42}, \quad 2x_3 \equiv 3 \pmod{43}$$

Dakle, $x_1 = 21$, $x_2 = -2$, $x_3 = 23$, $x_0 = 74006$ i $x \equiv 74006 \pmod{74046}$. Budući da je $74006 < 74046$, najmanji prirodan broj koji zadovoljava uvjete je 74006.

8. a) Odredite najmanji prirodan broj n takav da $3^2 \mid n$, $4^2 \mid n+1$ i $5^2 \mid n+2$.
   b) Postoji li prirodan broj n takav da $2^2 \mid n$, $3^2 \mid n+1$ i $4^2 \mid n+2$? Obrazložite!

Rj:

a) Budući da su svi moduli relativno prosti u parovima, možemo primijeniti kineski teorem o ostacima. Imamo $m = 3^2 \cdot 4^2 \cdot 5^2 = 3600$ i $x_0 = 400x_1 + 225x_2 + 144x_3$. Dakle, imamo sljedeći sustav:

$$400x_1 \equiv 0 \pmod{9}, \quad 225x_2 \equiv -1 \pmod{16}, \quad 144x_3 \equiv -2 \pmod{25}$$

$$4x_1 \equiv 0 \pmod{9}, \quad x_2 \equiv -1 \pmod{16}, \quad 19x_3 \equiv -2 \pmod{25}$$

Dakle, $x_1 = 0$, $x_2 = -1$ i $x_3 = 17$, $x_0 = 2223$ i budući da je $2223 < 3600$, najmanji takav n je 2223.

b) Iz prve kongruencije imamo $n = 4k$, a iz zadnje $n = 16l - 2$. Dakle $4k = 16l - 2$, odnosno $2k = 8l - 1$. Lijeva strana je paran broj, a desna je neparan, pa nema rješenja.

9. Neka je p prost broj.
   a) Dokažite da je $\binom{p}{k} \equiv 0 \pmod{p}$ za $k \in \{1, 2, \ldots, p-1\}$.
   b) Dokažite da za svaki cijeli broj n vrijedi $(n+1)^p \equiv n^p + 1 \pmod{p}$.

Rj:

a) $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Ako je $k \in \{1, 2, \ldots, p-1\}$, tada $p \mid p!$, $p \nmid k!$ i $p \nmid (p-k)!$. Dakle, $p \mid \binom{p}{k}$.

b)

$$\begin{aligned}(n+1)^p &= \sum_{k=0}^{p} \binom{p}{k} n^k \\ &= n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k + 1 \\ &\equiv n^p + 1 \pmod{p}\end{aligned}$$