Diskretna matematika 2

Zadaća 6

March 9, 2025

Borna Gojšić

---

1. Odredite sve kvadratne ostatke modulo 29.

Rj: Reducirani sustav oznaka modulo 29 je $\{-14, \ldots, -1, 1, \ldots, 14\}$. Dakle, trebamo promatrati brojeve od 1 do 14 i pogledati ostatke njihovih kvadrata modulo 29 da bismo dobili sve kvadratne ostatke modulo 29.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	1	4	9	16	25	36	49	64	81	100	121	144	169	196
$x^2 \pmod{29}$	1	4	9	16	25	7	20	6	23	13	5	28	24	22

Dakle, kvadratni ostaci modulo 29 su 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25 i 28.

2. Ako je p neparan prost broj, dokažite da je

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$$

Rj: Budući da u skupu $\{-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}\}$ ima točno $\frac{p-1}{2}$ brojeva koji su kvadratni ostaci modulo p i svi ostali su kvadratni neostaci modulo p, imamo:

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \frac{p-1}{2} \cdot 1 + \frac{p-1}{2} \cdot (-1) = 0$$

3. Izračunajte Legendreove simbole

a) $\left(\frac{-35}{97}\right)$ b) $\left(\frac{111}{991}\right)$ c) $\left(\frac{160}{163}\right)$ d) $\left(\frac{164}{167}\right)$ e) $\left(\frac{436}{683}\right)$

Rj:

a)

$$\begin{aligned}\left(\frac{-35}{97}\right) &= \left(\frac{-1}{97}\right)\left(\frac{5}{97}\right)\left(\frac{7}{97}\right) = (-1)^{\frac{97-1}{2}} \cdot (-1)^{\frac{96\cdot 4}{4}} \cdot \left(\frac{97}{5}\right) \cdot (-1)^{\frac{96\cdot 6}{4}} \cdot \left(\frac{97}{7}\right) \\ &= \left(\frac{2}{5}\right) \cdot \left(\frac{6}{7}\right) = -1 \cdot \left(\frac{-1}{7}\right) = -1 \cdot (-1)^{\frac{6}{2}} = 1\end{aligned}$$

b)

$$\left(\frac{111}{991}\right) = \left(\frac{3}{991}\right)\left(\frac{37}{991}\right) = (-1)^{\frac{110\cdot 990}{4}} \cdot \left(\frac{991}{3}\right) \cdot (-1)^{\frac{36\cdot 990}{4}} \cdot \left(\frac{991}{37}\right)$$
$$= -\left(\frac{1}{3}\right)\left(\frac{29}{37}\right) = -(-1)^{\frac{28\cdot 36}{4}} \cdot \left(\frac{37}{29}\right) = -\left(\frac{8}{29}\right) = -(1)^3 = -1$$

c)

$$\left(\frac{160}{163}\right) = \left(\frac{-3}{163}\right) = \left(\frac{-1}{163}\right)\left(\frac{3}{163}\right) = -1 \cdot (-1)^{\frac{2\cdot 162}{4}} \left(\frac{163}{3}\right) = \left(\frac{1}{3}\right) = 1$$

d)

$$\left(\frac{164}{167}\right) = \left(\frac{-3}{167}\right) = \left(\frac{-1}{167}\right)\left(\frac{3}{167}\right) = -1 \cdot (-1)^{\frac{2\cdot 166}{4}} \left(\frac{167}{3}\right) = \left(\frac{2}{3}\right) = -1$$

e)

$$\left(\frac{436}{683}\right) = \left(\frac{2}{683}\right)^2 \left(\frac{109}{683}\right) = (-1)^{\frac{108\cdot 682}{4}} \left(\frac{683}{109}\right) = \left(\frac{29}{109}\right) = (-1)^{\frac{108\cdot 28}{4}} \left(\frac{109}{29}\right)$$
$$= \left(\frac{-7}{29}\right) = \left(\frac{-1}{29}\right)\left(\frac{7}{29}\right) = (-1)^{\frac{6\cdot 28}{4}} \left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1$$

4. Izračunajte Jacobijeve simbole $\left(\frac{40}{403}\right)$ i $\left(\frac{907}{1455}\right)$

Rj: Budući da je $403 = 13 \cdot 31$, imamo:

$$\left(\frac{40}{403}\right) = \left(\frac{40}{13}\right)\left(\frac{40}{31}\right) = \left(\frac{1}{13}\right)\left(\frac{9}{31}\right) = 1$$

Nadalje, budući da je $1455 = 3 \cdot 5 \cdot 97$, imamo:

$$\left(\frac{907}{1455}\right) = \left(\frac{907}{3}\right)\left(\frac{906}{5}\right)\left(\frac{907}{97}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right)\left(\frac{34}{97}\right) = -\left(\frac{2}{97}\right)\left(\frac{17}{97}\right) = -(-1)^{\frac{16\cdot 96}{4}} \left(\frac{97}{17}\right)$$
$$= -\left(\frac{-5}{17}\right) = -\left(\frac{-1}{17}\right)\left(\frac{5}{17}\right) = -(-1)^{\frac{16}{2}} \cdot (-1)^{\frac{16\cdot 4}{4}} \left(\frac{17}{5}\right) = -\left(\frac{2}{5}\right) = 1$$

5. a) Izračunajte Jacobijeve simbole $\left(\frac{-60}{377}\right)$ i $\left(\frac{-60}{323}\right)$

   b) Je li -60 kvadratni ostatak modulo 377? Detaljno obrazložite odgovor!

   c) Je li -60 kvadratni ostatak modulo 323? Detaljno obrazložite odgovor!

Rj:

a) Budući da je $377 = 13 \cdot 29$, imamo:

$$\left(\frac{-60}{377}\right) = \left(\frac{-60}{13}\right)\left(\frac{-60}{29}\right) = \left(\frac{5}{13}\right)\left(\frac{-2}{29}\right) = \left[(-1)^{\frac{48}{4}}\left(\frac{13}{5}\right)\right]\left[(-1)^{\frac{28}{2}}\left(\frac{2}{29}\right)\right]$$
$$= \left(\frac{3}{5}\right) \cdot (-1) = 1$$

Budući da je $323 = 17 \cdot 19$, imamo:

$$\left(\frac{-60}{323}\right) = \left(\frac{-60}{17}\right)\left(\frac{-60}{19}\right) = \left[\left(\frac{2}{17}\right)\right]^3\left[\left(\frac{2}{19}\right)\right]^4 = \left(\frac{2}{17}\right) = 1$$

b) -60 nije kvadratni ostatak jer je $\left(\frac{-60}{13}\right) = -1$.

c) Budući da je $\left(\frac{-60}{17}\right) = \left(\frac{-60}{19}\right) = 1$, znamo da je -60 kvadratni ostatak modulo 323.

6. Odredite sve neparne proste brojeve p takve da je:

   a) $\left(\frac{6}{p}\right) = 1$

   b) $\left(\frac{-60}{p}\right) = -1$

   c) $\left(\frac{40}{p}\right) = -1$

Rj:

a)

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1$$

Imamo dvije mogućnosti:

1. Ako imamo da je $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$, onda iz $\left(\frac{2}{p}\right) = 1$ slijedi $p \equiv 1, 7 \pmod 8$, te $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1$. Dakle, ako je $p \equiv 1 \pmod 8$, onda je i $p \equiv 1 \pmod 3$, tj. $p \equiv 1 \pmod{24}$. A, ako je $p \equiv 7 \pmod 8$, onda je i $p \equiv 2 \pmod 3$, tj. $p \equiv 23 \pmod{24}$.
2. Ako imamo da je $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$ onda iz $\left(\frac{2}{p}\right) = -1$ slijedi $p \equiv 3, 5 \pmod 8$, te $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = -1$. Dakle, ako je $p \equiv 3 \pmod 8$, onda je i $p \equiv 1 \pmod 3$, tj. $p \equiv 19 \pmod{24}$. A, ako je $p \equiv 5 \pmod 8$, onda je i $p \equiv 2 \pmod 3$, tj. $p \equiv 5 \pmod{24}$.

Dakle, $p \equiv 1, 5, 19, 23 \pmod{24}$.

b)

$$\left(\frac{-60}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{2^2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{2(p-1)}{4}} \cdot \left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$$
$$= \left(\frac{p}{3}\right)\left(\frac{p}{5}\right) = -1$$

Imamo dvije mogućnosti:

1. Ako je $\left(\frac{p}{3}\right) = 1$ i $\left(\frac{p}{5}\right) = -1$, onda imamo $p \equiv 1 \pmod 3$ i $p \equiv \pm 2 \pmod 5$. Dakle, $p \equiv 7, 13 \pmod{15}$.
2. Ako je $\left(\frac{p}{3}\right) = -1$ i $\left(\frac{p}{5}\right) = 1$, onda imamo $p \equiv 2 \pmod 3$ i $p \equiv \pm 1 \pmod 5$. Dakle, $p \equiv 11, 14 \pmod{15}$.

Dakle, imamo $p \equiv 7, 11, 13, 14 \pmod{15}$.

c)

$$\left(\frac{40}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = -1$$

Imamo dvije mogućnosti:

1. Ako je $\left(\frac{2}{p}\right) = 1$ i $\left(\frac{5}{p}\right) = -1$, onda imamo $p \equiv 1, 7 \pmod 8$ i $p \equiv \pm 2 \pmod 5$. Dakle, $p \equiv 7, 17, 23, 33 \pmod{40}$.
2. Ako je $\left(\frac{2}{p}\right) = -1$ i $\left(\frac{5}{p}\right) = 1$, onda imamo $p \equiv 3, 5 \pmod 8$ i $p \equiv \pm 1 \pmod 5$. Dakle, $p \equiv 11, 19, 21, 29 \pmod{40}$

Dakle, imamo $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$.

7. a) Odredite sve neparne proste brojeve p takve da je $\left(\frac{-3}{p}\right) = 1$
   b) Dokažite da postoji beskonačno mnogo prostih brojeva oblika $6k + 1$.

Rj:

a)
$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-1)\cdot 2}{4}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1$$
Jedini kvadratni ostatak modulo 3 je 1, pa imamo $p \equiv 1 \pmod 3$, tj. $p = 3k + 1$. Budući da je p neparan, imamo i $p = 6k + 1$.

b) Neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi oblika $6k+1$. Promotrimo broj $m = p_1^2 p_2^2 \cdots p_n^2 + 3$.
$$m \equiv 0 \pmod p \iff x^2 \equiv -3 \pmod p \iff \left(\frac{-3}{p}\right) = 1$$
Dakle, m ima prosti faktor p oblika $6k + 1$. Očito $p \neq p_i$ za $i \in \{1, 2, \ldots, n\}$, pa imamo kontradikciju. Dakle, postoji beskonačno mnogo prostih brojeva oblika $6k + 1$.

8. Izračunajte
   a) $\left(\frac{17}{p}\right)$
   b) $\left(\frac{19}{p}\right)$

   za sve neparne proste brojeve p.

Rj:

a)

$$\left(\frac{17}{p}\right) = (-1)^{\frac{(p-1)\cdot 16}{4}} \left(\frac{p}{17}\right) = \left(\frac{p}{17}\right)$$

Sada ćemo izračunati sve kvadratne ostatke modulo 17:

x	1	2	3	4	5	6	7	8
x^2	1	4	9	16	25	36	49	64
$x^2 \pmod{29}$	1	4	9	16	8	2	15	13

Dakle, imamo $\left(\frac{17}{p}\right) = \begin{cases} 1, & \text{ako je } p \equiv 1,2,4,8,9,13,15,16 \pmod{17} \\ 0, & \text{ako je } p = 17 \\ -1, & \text{ako je } p \equiv 3,5,6,7,10,11,12,14 \pmod{17} \end{cases}$

b)

$$\left(\frac{19}{p}\right) = (-1)^{\frac{(p-1)\cdot 18}{4}} \left(\frac{p}{19}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{19}\right)$$

Sada ćemo izračunati sve kvadratne ostatke modulo 19:

x	1	2	3	4	5	6	7	8	9
x^2	1	4	9	16	25	36	49	64	81
$x^2 \pmod{29}$	1	4	9	16	6	17	11	7	5

Imamo 4 slučaja, ali možemo promotriti samo prva dva i ostale dobiti komplementom:

1. Ako je $\left(\frac{p}{19}\right) = 1$ i $p \equiv 1 \pmod{4}$, onda je $p \equiv 1,4,5,6,7,11,13,16,17 \pmod{19}$ i $p \equiv 1 \pmod{4}$. Dakle, $p \equiv 1,5,13,17,25,45,49,61,73 \pmod{76}$.
2. Ako je $\left(\frac{p}{19}\right) = -1$ i $p \equiv 3 \pmod{4}$ onda je $p \equiv 2,3,8,9,10,12,14,15,18 \pmod{19}$ i $p \equiv 3 \pmod{4}$. Dakle, $p \equiv 3,15,27,31,47,59,67,71,75 \pmod{76}$.

Dakle, imamo:

$$\left(\frac{19}{p}\right) = \begin{cases} 1, & \text{ako je } p \equiv 1,3,5,13,15,17,25,27,31,45, \\ & \qquad 47,49,59,61,67,71,73,75 \pmod{76} \\ 0, & \text{ako je } p = 19 \\ -1, & \text{inače} \end{cases}$$

9. Odredite sve neparne proste brojeve p takve da kongruencija $x^2 + 45 \equiv 0 \pmod{p}$ ima rješenja.

Rj:

$$\left(\frac{-45}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)\left(\frac{3^2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{4(p-1)}{4}} \left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = 1$$

Imamo dvije mogućnosti:

1. Kvadratni ostaci modulo 5 su 1 i 4 pa kongruencija ima rješenja za $p \equiv \pm 1 \pmod{5}$ i $p \equiv 1 \pmod{4}$, tj. $p \equiv 1, 9 \pmod{20}$.
2. Kvadratni neostaci modulo 5 su 2 i 3 pa kongruencija ima rješenja za $p \equiv \pm 2 \pmod{5}$ i $p \equiv 3 \pmod{4}$, tj. $p \equiv 3, 7 \pmod{20}$.

10. Neka je p neparan prost broj s primitivnim korijenom g te neka je a cijeli broj takav da je $\text{nzd}(a, p) = 1$. Dokažite da je a kvadratni ostatak modulo p ako i samo ako je indeks $\text{ind}_g a$ paran.

Rj: Neka je g primitvni korijen modulo p. Pretpostavimo prvo da je $\text{ind}_g a$ paran. Tada imamo $g^{2k} \equiv a \pmod{p}$ za neki $k \in \mathbb{Z}$. Dakle, a je kvadratni ostatak modulo p. Pretpostavimo sada da je a kvadratni ostatak modulo p. Tada imamo $x^2 \equiv a \pmod{p}$ za neki $x \in \mathbb{Z}$. Po definciji primitvnog korijena, postoji $k \in \mathbb{Z}$ takav da je $g^k \equiv x \pmod{p}$. Dakle, $g^{2k} \equiv a \pmod{p}$, tj. $\text{ind}_g a$ je paran.

11. Neka je q prost broj oblika $q = p^2 + 4a^2$ gdje je p neparan prost broj te a cijeli broj. Dokažite da je $\left(\frac{p}{q}\right) = 1$.
Uputa: Koristite Gaussov zakon reciprociteta

Rj: Budući da je $q = p^2 + 4a^2$, i p je neparan prost broj, imamo $q \equiv (\pm 1)^2 \equiv 1 \pmod{4}$. Dakle, q je prost broj oblika $4k + 1$. Nadalje,

$$\left(\frac{q}{p}\right) = \left(\frac{p^2 + 4a^2}{p}\right) = \left(\frac{(2a)^2}{p}\right) = 1$$

Sada koristimo Gaussov zakon reciprociteta:

$$\left(\frac{p}{q}\right) \cdot 1 = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = (-1)^{\frac{(p-1)\cdot 4k}{4}} = 1$$

12. Neka je a neparan prost broj te neka je b cijeli broj takav da je $p = a^2 + 5b^2$ prost. Dokažite da je a kvadratni ostatak modulo p ako i samo ako je $p \equiv 1 \pmod 5$.

Rj:

$$\left(\frac{a}{p}\right) = (-1)^{\frac{(a-1)(p-1)}{4}} \cdot \left(\frac{p}{a}\right)$$

Budući da je a neparan prost broj, imamo $a \equiv \pm 1 \pmod 4$ pa je $p \equiv 1 + 0 \equiv 1 \pmod 4$ jer b mora biti paran kako bi p bio neparan. Dakle, imamo:

$$\left(\frac{a}{p}\right) = (-1)^{\frac{(a-1)(p-1)}{4}} \cdot \left(\frac{p}{a}\right) = \left(\frac{p}{a}\right)$$

Znamo da je

$$\left(\frac{p}{a}\right) \equiv (a^2 + 5b^2)^{\frac{a-1}{2}} \equiv 5^{\frac{a-1}{2}} b^{a-1} \equiv 5^{\frac{a-1}{2}} \equiv \left(\frac{5}{a}\right) \pmod a$$

Dakle, imamo

$$\left(\frac{p}{a}\right) = \left(\frac{5}{a}\right) = (-1)^{a-1} \cdot \left(\frac{a}{5}\right) = \left(\frac{a}{5}\right)$$

Ako je a kvadratni ostatak modulo 5, onda je $a = 5k \pm 1$ pa je $p = 5l + 1$. Dakle,

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{5}{a}\right) = 1$$

Ako je a kvadratni neostatak modulo 5, onda je $a = 5k \pm 2$ pa je $p = 5l + 4$.

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{5}{a}\right) = -1$$

Jedini preostali slučaj je $a = 5$, ali onda imamo $25 \mid p$ pa p nije prost. Dakle, a je kvadratni ostatak modulo p ako i samo ako je $p \equiv 1 \pmod 5$.

13. Riješite sustav kongruencija

$$x^2 \equiv 21 \pmod{67}$$
$$x^2 \equiv 44 \pmod{83}$$

Uputa: Uočite $67 \equiv 83 \equiv 3 \pmod 4$.

Rj: Budući da su 67 i 83 oba oblika $4k+3$, imamo:

$$x \equiv \pm 21^{\frac{67+1}{4}} \equiv \pm 21^{17} \equiv \pm 21 \cdot 39^8 \equiv \pm 21 \cdot (-20)^4 \equiv \pm 21 \cdot (-2)^2 \equiv \pm 17 \pmod{67}$$
$$x \equiv \pm 44^{\frac{83+1}{4}} \equiv \pm 44^{21} \equiv \pm 44 \cdot 27^{10} \equiv \pm 44 \cdot 65^5 \equiv \pm 44 \cdot 65 \cdot (-8)^2 \equiv \pm 38 \cdot 64 \equiv \pm 25 \pmod{83}$$

Sada možemo riješiti 4 implicitna sustava kongruencija malim kineskim teoremom:

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	83	0	1	67	0
0	1	67	1	-1	16	4
1	-1	16	-4	5	3	5
-4	5	3	21	-26	1	3
21	-26	1			0	

Dakle, $21 \cdot 83 - 26 \cdot 67 = 1$ pa imamo $x_1^+ = 21 \cdot 83 \cdot 17 - 26 \cdot 67 \cdot 25 \equiv 2764 \pmod{5561}$ i $x_2^+ = 21 \cdot 83 \cdot 17 + 26 \cdot 67 \cdot 25 \equiv 888 \pmod{5561}$. Dakle, rješenja su $x \equiv \pm 2764, \pm 888 \pmod{5561}$.