UVOD U TEORIJU BROJEVA

Rješenja kolokvija – grupa A, 26.01.2007.

1. a) Riješite kongruenciju:

$$672x \equiv 291 \pmod{957}.$$

Rješenje: Primjenimo Euklidov algoritam da odredimo $(957, 672)$ i nađemo q_i

$$\begin{aligned}
957 &= 672 \cdot 1 + 285\\
672 &= 285 \cdot 2 + 102\\
285 &= 102 \cdot 2 + \ \ 81\\
102 &= \ \ 81 \cdot 1 + \ \ 21\\
81 &= \ \ 21 \cdot 3 + \ \ 18\\
21 &= \ \ 18 \cdot 1 + \ \ \ \ \mathbf{3}\\
18 &= \ \ \ \ 3 \cdot 6
\end{aligned}$$

Vidimo da je $(957, 672) = 3$. Budući da $3 \mid 291$, kongruencija ima (tri) rješenja. Riješimo kongruenciju $224x \equiv 97 \pmod{319}$. Uočimo da bi iste q_i-eve dobili bi kada računali $(319, 224)$.

i	-1	0	1	2	3	4	5	6
q_i			1	2	2	1	3	1
y_i	0	1	-1	3	-7	10	-37	$\mathbf{47}$

Dakle, rješenje kongruencije $224u \equiv 1 \pmod{319}$ je $u \equiv 47 \pmod{319}$, pa je $x \equiv 97 \cdot 47 \equiv 4559 \equiv 93 \pmod{319}$ rješenje kongruencije $224x \equiv 97 \pmod{319}$. Konačno, rješenja polazne kongruencije su

$$x \equiv 93, 93 + 319, 93 + 2 \cdot 319 \equiv \mathbf{93}, \mathbf{412}, \mathbf{731} \pmod{\mathbf{957}}.$$ □

b) Riješite sustav kongruencija:

$$x \equiv 3 \pmod 5, \quad x \equiv 5 \pmod{11}, \quad x \equiv 9 \pmod{13}.$$

Rješenje: Brojevi 5, 11 i 13 su u parovima relativno prosti, pa možemo odmah primijeniti Kineski teorem o ostatcima. Tražimo x_1, x_2 i x_3 koji zadovoljavaju:

$$11 \cdot 13 \cdot x_1 \equiv 3 \pmod 5, \quad 5 \cdot 13 \cdot x_2 \equiv 5 \pmod{11}, \quad 5 \cdot 11 \cdot x_3 \equiv 9 \pmod{13},$$

odnosno

$$3x_1 \equiv 3 \pmod 5, \quad 10x_2 \equiv 5 \pmod{11}, \quad 3x_3 \equiv 9 \pmod{13},$$

Dobijemo $x_1 = 1$, $x_2 = 6$ i $x_3 = 3$. Stoga je rješenje polaznog sustava $x_0 \equiv 11 \cdot 13 \cdot x_1 + 5 \cdot 13 \cdot x_2 + 5 \cdot 11 \cdot x_3 \equiv 143 + 390 + 165 \pmod{5 \cdot 11 \cdot 13} \equiv \mathbf{698} \pmod{\mathbf{715}}$. □

2. Koliko ima primitivnih korijena modulo 31? Nađite najmanji među njima, te riješite kongruenciju $2x^{16} \equiv 5 \pmod{31}$.

Rješenje: Budući je 31 prost broj, primitivnih korijena modulo 31 ima $\varphi(31 - 1) = \varphi(30) = \mathbf{8}$.

Djelitelji od 30 su 2, 3, 5, 6, 10, i 15. Budući je $2^5 \equiv 1 \pmod{31}$, 2 nije primitivni korijen modulo 31.

Pogledajmo broj 3. Uočimo da je dovoljno provjeriti potencije 6, 10 i 15. Budući je $3^6 = (3^3)^2 \equiv (-4)^2 = 16 \not\equiv 1 \pmod{31}$, $3^{10} = (3^5)^2 \equiv 26^2 \equiv 25 \not\equiv 1 \pmod{31}$, $3^{15} = 3^{10} \cdot 3^5 \equiv 30 \not\equiv 1 \pmod{31}$, **3** je primitivni korijen modulo 31.

Kada indeksiramo polaznu jednadžbu dobijemo:

$$\mathrm{ind}_3 2 + \mathrm{ind}_3 x^{16} \equiv \mathrm{ind}_3 5 \pmod{30}$$

Iz tablice ispod vidimo da je $\mathrm{ind}_3 2 = 24$ i $\mathrm{ind}_3 5 = 20$:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^i \pmod{31}$	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30
i	16	17	18	19	**20**	21	22	23	**24**	25	26	27	28	29	30
$3^i \pmod{31}$	28	22	4	12	**5**	15	14	11	**2**	$\cdots\cdots$					

(Uočimo da je $3^{15} \equiv -1 \pmod{31}$, pa vrijedi $3^i \equiv -3^{15+i} \pmod{31}$, te smo da odredimo $\mathrm{ind}_3 2$ mogli računati samo do 3^9) Imamo:

$$\begin{aligned}
24 + 16\,\mathrm{ind}_3 x &\equiv 20 \pmod{30}\\
8\,\mathrm{ind}_3 x &\equiv -2 \pmod{15}\\
4\,\mathrm{ind}_3 x &\equiv -1 \equiv 14 \pmod{15}\\
2\,\mathrm{ind}_3 x &\equiv 7 \pmod{15}\\
\mathrm{ind}_3 x &\equiv 11 \pmod{15}\\
\mathrm{ind}_3 x &\equiv 11, 26 \pmod{30}
\end{aligned}$$

Odnosno

$$x \equiv 3^{11}, 3^{26} \pmod{31} \equiv 13, 3^{24} \cdot 3^2 \pmod{31} \equiv \mathbf{13}, \mathbf{18} \pmod{\mathbf{31}}.$$

□

3. a) Odredite sve proste brojeve p takve da je $\left(\frac{54}{p}\right) = -1$.

Rješenje:

$$\left(\frac{54}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{3^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$$

Imamo dva slučaja: prvi $\left(\frac{2}{p}\right) = 1$, $\left(\frac{3}{p}\right) = -1$ i drugi $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = 1$.

U prvom imamo $\left(\frac{2}{p}\right) = 1$ za $p \equiv 1, 7 \pmod 8$, te $\left(\frac{3}{p}\right) = -1$ za $p \equiv 5, 7 \pmod{12}$. Rješavanjem ta četiri sustava kongruencija dobijemo dva rješenja $p \equiv 7, 17 \pmod{24}$.

U drugom imamo $\left(\frac{2}{p}\right) = -1$ za $p \equiv 3, 5 \pmod 8$, te $\left(\frac{3}{p}\right) = 1$ za $p \equiv 1, 11 \pmod{12}$. Rješavanjem ta četiri sustava kongruencija dobijemo dva rješenja $p \equiv 11, 13 \pmod{24}$.

Ukupno rješenje je $p \equiv \mathbf{7}, \mathbf{11}, \mathbf{13}, \mathbf{17} \pmod{\mathbf{24}}$. □

b) Izračunajte Legendreove simbole $\left(\frac{150}{127}\right)$ i $\left(\frac{231}{233}\right)$.

Rješenje:

$$\left(\frac{150}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{3}{127}\right)\left(\frac{5^2}{127}\right) = 1 \cdot (-1)\left(\frac{127}{3}\right) \cdot 1 = -\left(\frac{1}{3}\right) = \mathbf{-1}$$

$$\left(\frac{231}{233}\right) = \left(\frac{233}{231}\right) = \left(\frac{2}{231}\right) = \mathbf{1}$$

□

4. Odredite $h(-59)$, te nađite reduciranu binarnu kvadratnu formu ekvivalentnu sa $135x^2 - 169xy + 53y^2$.

Rješenje: Da bi odredili $h(-59)$ trebamo riješiti jednadžbu $4ac - b^2 = 59$, gdje su $a, b, c \in \mathbb{Z}$ i zadovoljavaju uvjet $-a < b \le a < c$ ili $0 \le b \le a = c$. Iz $59 > 3a^2$ slijedi $a \le 4$.

Budući je -59 neparan broj, b mora biti neparan. Promotrimo sve mogućnosti:

$$
\begin{array}{lll}
a=1 & b=1 & c=\frac{59+1}{4}=15, \text{pa smo dobili formu } x^2+xy+15y^2 \\
a=2 & b=\pm 1 & c=\frac{59+1}{8}=\frac{15}{2}\notin\mathbb{Z}. \\
a=3 \left\{ \begin{array}{l} \\ \\ \end{array}\right. & \begin{array}{l} b=\pm 1 \\ b=3 \end{array} & \begin{array}{l} c=\frac{59+1}{12}=5, \text{pa smo dobili dvije forme } 3x^2\pm xy+5y^2 \\ c=\frac{59+3^2}{12}=\frac{17}{3}\notin\mathbb{Z}. \end{array} \\
a=4 \left\{ \begin{array}{l} \\ \\ \end{array}\right. & \begin{array}{l} b=\pm 1 \\ b=\pm 3 \end{array} & \begin{array}{l} c=\frac{59+1}{16}=\frac{15}{4}\notin\mathbb{Z}. \\ c=\frac{59+3^2}{16}=\frac{17}{4}\notin\mathbb{Z}. \end{array}
\end{array}
$$

Ukupno smo dobili 3 forme, pa je $h(-59) = \mathbf{3}$.

Umjesto matričnog zapisa ću zbog jednostavnosti formu $ax^2 + bxy + cy^2$ pisati kao uređenu trojku (a, b, c). Pri tome koristim transformacije: $(a,b,c) \xrightarrow{U} (c,-b,a)$ i $(a,b,c) \xrightarrow{V^{\pm}} (a, b\pm 2a, a\pm b+c)$.

$(135, -169, 59) \xrightarrow[\text{jer je } a>c]{U} (53, 169, 135) \xrightarrow[\text{jer je } b>a]{V^-} (53, 63, 19) \xrightarrow[\text{jer je } a>c]{U} (19, -63, 53) \xrightarrow[\text{jer je } -b>a]{V^+}$
$(19, -25, 9) \xrightarrow[\text{jer je } a>c]{U} (9, 25, 19) \xrightarrow[\text{jer je } b>a]{V^-} (9, 7, 3) \xrightarrow[\text{jer je } a>c]{U} (3, -7, 9) \xrightarrow[\text{jer je } -b>a]{V^+} (3, -1, 5)$

Forma $\mathbf{3x^2 - xy + 5y^2}$ je reducirana i ekvivalentna polaznoj formi. □

5. a) Odredite sve prirodne brojeve n za koje vrijedi $\varphi(n) = 52$.

Rješenje: Ako je $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onda je

$$\varphi(n) = p_1^{\alpha_1-1}(p_1-1)\cdots p_r^{\alpha_r-1}(p_r-1).$$

Iz $(p_i - 1) \mid 52$ (djelitelji od 52 su 1, 2, 4, 13, 26 i 52) slijedi $p_i \in \{2, 3, 5, 53\}$. Stoga je n oblika $2^a \cdot 3^b \cdot 5^c \cdot 53^d$, gdje je $a \in \{0, 1, 2, 3\}$ (jer $8 \nmid 52$), $b \in \{0, 1\}$ (jer $3 \nmid 52$), $c \in \{0, 1\}$ (jer $5 \nmid 52$), $d \in \{0, 1\}$ (jer $53 \nmid 52$). Pa promotrimo sve slučajeve:

Ako je $d = 1$, mora biti $b = 0$, $c = 0$, $a \in \{0, 1\}$ (jer bi u protivnom bilo $\varphi(n) > 52$), te imamo dvije mogućnosti: $n = \mathbf{53}$ i $n = 2 \cdot 53 = \mathbf{106}$.

Ako je $d = 0$, promotrimo najveći mogući broj n koji bi se mogao dobiti: $\varphi(2^3 \cdot 3^1 \cdot 5^1) = 4 \cdot 2 \cdot 4 = 32 < 52$, pa zaključujemo da nema drugih rješenja.

Dakle, jedina rješenja su $n = \mathbf{53}$ i $n = \mathbf{106}$. □

b) Dokažite da ne postoje prirodni brojevi n i m takvi da vrijedi $\varphi(n) = 2 \cdot 13^{2m+1}$.

Rješenje: Budući da $\varphi(n)$ nije djeljiv sa 4, n ne može imati više od jednog neparnog prostog faktora, a ne može ni biti djeljiv sa 4. Zato je $n = p^k$ ili $n = 2p^k$. Tada je $\varphi(n) = (p-1) \cdot p^{k-1}$.

Budući da $\varphi(n)$ nije djeljiv i sa p i sa $p - 1$, mora biti $k = 1$.

Dakle, ostalo je samo provjeriti može li biti $\varphi(n) = p - 1$, tj. može li $2 \cdot 13^{2m+1} + 1$ biti prost broj. Budući je taj broj djeljiv sa 3 ($13 \equiv 1 \pmod 3 \Rightarrow 13^k \equiv 1 \pmod 3 \Rightarrow 2 \cdot 13^{2m+1} + 1 \equiv 3 \pmod 3$), odgovor je da ne može. □

6. a) Nađite sva rješenja Pellove jednadžbe $x^2 - 85y^2 = 1$ za koja vrijedi $1 < y < 100\,000$.

Rješenje: Razvijanjem u verižni razlomak dobije se:

$$\sqrt{85} = [9, \overline{4, 1, 1, 4, 18}]$$

Period $r = 5$ je neparan, pa su sva rješenja jednadžbe $x^2 - 89y^2 = 1$ dana sa (p_{10n-1}, q_{10n-1}), $n \in \mathbb{N}$.

i	-1	0	1	2	3	4	5	6	7	8	**9**	10
a_i		9	4	1	1	4	18	4	1	1	4	18
p_i	1	9	37	46	83	378	6887	27926	34813	62739	**285769**	5206581
q_i	0	1	4	5	9	41	747	3029	3776	6805	**30996**	546733

Budući je $q_{10} > 100\,000$, jedino rješenje je $(x, y) = (p_9, q_9) = (285\,769, 30\,996)$ (za $(p_{-1}, q_{-1}) = (1, 0)$ nije zadovoljen uvjet $1 < y$). □

b) Nađite sve Pitagorine trokute u kojima je jedna stranica jednaka 99.

Rješenje: Sve pitagorine trojke su dane identitetom:

$$[d(m^2 - n^2)]^2 + (2dmn)^2 = [d(m^2 + n^2]^2,$$

gdje su $d, m, n \in \mathbb{N}$, $(m, n) = 1$, $m > n$, m i n različite parnosti. Kako tražimo trojke u kojima je jedna stranica jednaka 99, to ne može biti druga stranica. Nadalje, iz $d \mid 99$ slijedi $d = 1, 3, 9, 11, 33$ (ili 99). Promotrimo sve mogućnosti:

$d = 1$. $\frac{63}{d} = 99 \equiv 3 \pmod 4$ pa jednadžba $m^2 + n^2 = 99$ nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 99$. $99 = 99 \cdot 1 = 33 \cdot 3 = 11 \cdot 9$. Kako je $(33, 3) \neq 1$, taj slučaj ne moramo promatrati (rješit ćemo ga kada budemo rješavali slučaj $d = 9$).

$$m + n = 99,\ m - n = 1 \implies m = 50, n = 49 \implies (\mathbf{99}, \mathbf{4900}, \mathbf{4901})$$
$$m + n = 11,\ m - n = 9 \implies m = 10, n = 1 \implies (\mathbf{99}, \mathbf{20}, \mathbf{101})$$

$d = 3$. $\frac{63}{d} = 33 \equiv 1 \pmod 4$ pa jednadžba $m^2 + n^2 = 33$ možda ima rješenja. Provjerom svih mogućnosti $n < m < \sqrt{33}$ vidimo da ipak nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 33$. Iz $33 = 33 \cdot 1 = 11 \cdot 3$ imamo:

$$m + n = 33,\ m - n = 1 \implies m = 17, n = 16 \implies (\mathbf{99}, \mathbf{1632}, \mathbf{1635})$$
$$m + n = 11,\ m - n = 3 \implies m = 7, n = 4 \implies (\mathbf{99}, \mathbf{168}, \mathbf{195})$$

$d = 9$. $\frac{63}{d} = 11 \equiv 3 \pmod 4$ pa jednadžba $m^2 + n^2 = 11$ nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 11$. Imamo samo jednu mogućnost:

$$m + n = 11,\ m - n = 1 \implies m = 6, n = 5 \implies (\mathbf{99}, \mathbf{540}, \mathbf{549})$$

$d = 11$. $\frac{63}{d} = 9 \equiv 1 \pmod 4$ pa jednadžba $m^2 + n^2 = 9$ možda ima rješenja. Provjerom svih mogućnosti $n < m < \sqrt{9} = 3$ vidimo da ipak nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 9$. Imamo samo jednu mogućnost:

$$m + n = 9,\ m - n = 1 \implies m = 5, n = 4 \implies (\mathbf{99}, \mathbf{440}, \mathbf{451})$$

$d = 33$. $\frac{63}{d} = 3 \equiv 3 \pmod 4$ pa jednadžba $m^2 + n^2 = 3$ nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 3$. Imamo samo jednu mogućnost:

$$m + n = 3,\ m - n = 1 \implies m = 2, n = 1 \implies (\mathbf{99}, \mathbf{132}, \mathbf{165})$$

Ukupno smo dobili **7** Pitagorinih trojki. □

Vinko Petričević

UVOD U TEORIJU BROJEVA

Rješenja kolokvija – grupa B, 26.01.2007.

1. a) Riješite kongruenciju:

$$639x \equiv 381 \pmod{876}.$$

Rješenje: Primjenimo Euklidov algoritam da odredimo $(876, 639)$ i nađemo q_i

$$\begin{aligned}
876 &= 639 \cdot 1 + 237 \\
639 &= 237 \cdot 2 + 165 \\
237 &= 165 \cdot 1 + 72 \\
165 &= 72 \cdot 2 + 21 \\
72 &= 21 \cdot 3 + 9 \\
21 &= 9 \cdot 2 + \mathbf{3} \\
9 &= 3 \cdot 3
\end{aligned}$$

Vidimo da je $(876, 639) = 3$. Budući da $3 \mid 381$, kongruencija ima (tri) rješenja. Riješimo kongruenciju $292x \equiv 127 \pmod{213}$. Uočimo da bi iste q_i-eve dobili bi kada računali $(292, 213)$.

i	-1	0	1	2	3	4	5	6
q_i			1	2	1	2	3	2
y_i	0	1	-1	3	-4	11	-37	$\mathbf{85}$

Dakle, rješenje kongruencije $213u \equiv 1 \pmod{292}$ je $u \equiv 85 \pmod{292}$, pa je $x \equiv 127 \cdot 85 \equiv 10795 \equiv 283 \pmod{292}$ rješenje kongruencije $213x \equiv 127 \pmod{292}$. Konačno, rješenja polazne kongruencije su

$$x \equiv 283, 283 + 292, 283 + 2 \cdot 292 \equiv \mathbf{283}, \mathbf{575}, \mathbf{867} \pmod{\mathbf{876}}.$$ □

b) Riješite sustav kongruencija:

$$x \equiv 4 \pmod 5, \quad x \equiv 3 \pmod 7, \quad x \equiv 9 \pmod{17}.$$

Rješenje: Brojevi 5, 7 i 17 u parovima relativno prosti, pa možemo odmah primijeniti Kineski teorem o ostatcima. Tražimo x_1, x_2 i x_3 koji zadovoljavaju:

$$7 \cdot 17 \cdot x_1 \equiv 4 \pmod 5, \quad 5 \cdot 17 \cdot x_2 \equiv 3 \pmod 7, \quad 5 \cdot 7 \cdot x_3 \equiv 9 \pmod{17},$$

odnosno

$$4x_1 \equiv 4 \pmod 5, \quad x_2 \equiv 3 \pmod 7, \quad x_3 \equiv 9 \pmod{17},$$

Dobijemo $x_1 = 1$, $x_2 = 3$ i $x_3 = 9$. Stoga je rješenje polaznog sustava $x_0 \equiv 7 \cdot 17 \cdot x_1 + 5 \cdot 17 \cdot x_2 + 5 \cdot 7 \cdot x_3 \equiv 119 + 225 + 315 \equiv 689 \pmod{5 \cdot 7 \cdot 17} \equiv \mathbf{94} \pmod{\mathbf{715}}$. □

2. Koliko ima primitivnih korijena modulo 37? Nađite najmanji među njima, te riješite kongruenciju $4x^{14} \equiv 7 \pmod{37}$.

Rješenje: Budući je 37 prost broj, primitivnih korijena modulo 37 ima $\varphi(37 - 1) = \varphi(36) = \mathbf{12}$.

Djelitelji od 36 su 2, 3, 4, 6, 9, 12 i 18. Uočimo da je dovoljno provjeriti potencije 12 i 18. Budući je $2^{12} = (2^6)^2 = 27^2 \equiv 26 \not\equiv 1 \pmod{37}$, $2^{18} = (2^9)^2 \equiv 31^2 \equiv 36 \not\equiv 1 \pmod{37}$, **2** je primitivni korijen modulo 37.

Kada indeksiramo polaznu jednadžbu dobijemo:

$$\mathrm{ind}_2 4 + \mathrm{ind}_2 x^{14} \equiv \mathrm{ind}_2 7 \pmod{36}$$

Iz tablice ispod vidimo da je $\mathrm{ind}_2 4 = 2$ i $\mathrm{ind}_2 7 = 32$:

i	1	**2**	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^i \pmod{37}$	2	**4**	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36
i	19	20	21	22	23	24	25	26	27	28	29	30	31	**32**	33	34	35	36
$2^i \pmod{37}$	35	33	29	21	5	10	20	3	6	12	24	11	22	**7**	······			

(Uočimo da je $2^{18} \equiv -1 \pmod{37}$), pa vrijedi $2^i \equiv -2^{18+i} \pmod{37}$), te smo da odredimo $\mathrm{ind}_2 7$ mogli računati samo do 2^{14}) Imamo:

$$\begin{aligned} 2 + 14\,\mathrm{ind}_2 x &\equiv 32 \pmod{36} \\ 7\,\mathrm{ind}_2 x &\equiv 15 \pmod{18} \\ \mathrm{ind}_2 x &\equiv 15 \pmod{18} \\ \mathrm{ind}_2 x &\equiv 15, 33 \pmod{36} \end{aligned}$$

Odnosno

$$x \equiv 2^{15}, 2^{33} \pmod{37} \equiv 23, 2 \cdot 2^{32} \pmod{37} \equiv \mathbf{23}, \mathbf{14} \pmod{\mathbf{37}}.$$ □

3. a) Odredite sve proste brojeve p takve da je $\left(\frac{90}{p}\right) = 1$.

$$\left(\frac{90}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{3^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$$

Imamo dva slučaja: prvi $(\frac{2}{p}) = 1$, $(\frac{5}{p}) = 1$ i drugi $(\frac{2}{p}) = -1$, $(\frac{5}{p}) = -1$.

U prvom imamo $(\frac{2}{p}) = 1$ za $p \equiv 1, 7 \pmod 8$, te $(\frac{p}{5}) = 1$ za $p \equiv 1, 4 \pmod 5$. Rješavanjem ta četiri sustava kongruencija dobijemo četiri rješenja $p \equiv 1, 9, 31, 39 \pmod{40}$.

U drugom imamo $(\frac{2}{p}) = -1$ za $p \equiv 3, 5 \pmod 8$, te $(\frac{p}{5}) = -1$ za $p \equiv 2, 3 \pmod 5$. Rješavanjem ta četiri sustava kongruencija dobijemo četiri rješenja $p \equiv 3, 13, 27, 37 \pmod{40}$.

Ukupno rješenje je $p \equiv \mathbf{1}, \mathbf{3}, \mathbf{9}, \mathbf{13}, \mathbf{27}, \mathbf{31}, \mathbf{37}, \mathbf{39} \pmod{\mathbf{40}}$. □

b) Izračunajte Legendreove simbole $\left(\frac{140}{113}\right)$ i $\left(\frac{227}{229}\right)$.

Rješenje:

$$\left(\frac{140}{113}\right) = \left(\frac{2^2}{113}\right)\left(\frac{5}{113}\right)\left(\frac{7}{113}\right) = 1 \cdot \left(\frac{113}{5}\right)\left(\frac{113}{7}\right) = \left(\frac{3}{5}\right)\left(\frac{1}{7}\right) = -1 \cdot 1 = \mathbf{-1}$$

$$\left(\frac{227}{229}\right) = \left(\frac{229}{227}\right) = \left(\frac{2}{227}\right) = \mathbf{-1}$$ □

4. Odredite $h(-71)$, te nađite reduciranu binarnu kvadratnu formu ekvivalentnu sa $32x^2 - 43xy + 15y^2$.

Rješenje: Da bi odredili $h(-71)$ trebamo riješiti jednadžbu $4ac - b^2 = 71$, gdje su $a, b, c \in \mathbb{Z}$ i zadovoljavaju uvjet $-a < b \le a < c$ ili $0 \le b \le a = c$. Iz $71 > 3a^2$ slijedi $a \le 4$.

Budući je -71 neparan broj, b mora biti neparan. Promotrimo sve mogućnosti:

$$a = 1 \quad b = 1 \quad c = \tfrac{71+1}{4} = 18, \text{pa smo dobili formu } x^2 + xy + 18y^2$$
$$a = 2 \quad b = \pm 1 \quad c = \tfrac{71+1}{8} = 9, \text{pa smo dobili dvije forme } 2x^2 \pm xy + 9y^2$$
$$a = 3 \begin{cases} b = \pm 1 & c = \tfrac{71+1}{12} = 6, \text{pa smo dobili dvije forme } 3x^2 \pm xy + 6y^2 \\ b = 3 & c = \tfrac{71+3^2}{12} = \tfrac{20}{3} \notin \mathbb{Z}. \end{cases}$$
$$a = 4 \begin{cases} b = \pm 1 & c = \tfrac{71+1}{16} = \tfrac{9}{2} \notin \mathbb{Z}. \\ b = \pm 3 & c = \tfrac{71+3^2}{16} = 5, \text{pa smo dobili dvije forme } 4x^2 \pm 3xy + 5y^2 \end{cases}$$

Ukupno smo dobili 7 formi, pa je $h(-71) = \mathbf{7}$.

Umjesto matričnog zapisa ću zbog jednostavnosti formu $ax^2 + bxy + cy^2$ pisati kao uređenu trojku (a, b, c). Pri tome koristim transformacije: $(a, b, c) \xrightarrow{U} (c, -b, a)$ i $(a, b, c) \xrightarrow{V^{\pm}} (a, b \pm 2a, a \pm b + c)$.

$(32, -43, 15) \xrightarrow[\text{jer je } a>c]{U} (15, 43, 32) \xrightarrow[\text{jer je } b>a]{V^-} (15, 13, 4) \xrightarrow[\text{jer je } a>c]{U} (4, -13, 15) \xrightarrow[\text{jer je } -b>a]{V^+}$
$(4, -5, 6) \xrightarrow[\text{jer je } -b>a]{V^+} (4, 3, 5)$

Forma $\mathbf{4x^2 + 3xy + 5y^2}$ je reducirana i ekvivalentna polaznoj formi. □

5. a) Odredite sve prirodne brojeve n za koje vrijedi $\varphi(n) = 28$.

Rješenje: Ako je $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onda je $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$.

Iz $(p_i - 1) \mid 28$ (djelitelji od 28 su 1, 2, 4, 7, 14 i 28) slijedi $p_i \in \{2, 3, 5, 29\}$. Stoga je n oblika $2^a \cdot 3^b \cdot 5^c \cdot 29^d$, gdje je $a \in \{0, 1, 2, 3\}$ (jer $8 \nmid 28$), $b \in \{0, 1\}$ (jer $3 \nmid 28$), $c \in \{0, 1\}$ (jer $5 \nmid 28$), $d \in \{0, 1\}$ (jer $29 \nmid 28$). Pa promotrimo sve slučajeve:

Ako je $d = 1$, mora biti $c = 0$, $b = 0$, $a \in \{0, 1\}$ (jer bi u protivnom bilo $\varphi(n) > 28$), te imamo dvije mogućnosti: $n = \mathbf{29}$ i $n = 2 \cdot 29 = \mathbf{58}$.

Ako je $d = 0$, promotrimo slučaj $c = 1$. Kako je $5 - 1 = 4$ slijedi $\varphi(2^a \cdot 3^b) = 7$, a to nema rješenja.

Ako je $d = 0, c = 0$, promotrimo najveći mogući broj n koji bi se mogao dobiti: $\varphi(2^3 \cdot 3^1) = 4 \cdot 2 = 8 < 28$, pa zaključujemo da nema drugih rješenja.

Dakle, jedina rješenja su $n = \mathbf{29}$ i $n = \mathbf{58}$. □

b) Dokažite da ne postoje prirodni brojevi n i m takvi da vrijedi $\varphi(n) = 2 \cdot 7^{4m+1}$.

Rješenje: Budući da $\varphi(n)$ nije djeljiv sa 4, n ne može imati više od jednog neparnog prostog faktora, a ne može ni biti djeljiv sa 4. Zato je $n = p^k$ ili $n = 2p^k$. Tada je $\varphi(n) = (p - 1) \cdot p^{k-1}$.

Budući da $\varphi(n)$ nije djeljiv i sa p i sa $p - 1$, mora biti $k = 1$.

Dakle, ostalo je samo provjeriti može li biti $\varphi(n) = p - 1$, tj. može li $2 \cdot 7^{4m+1} + 1$ biti prost broj. Budući je taj broj djeljiv sa 3 ($7 \equiv 1 \pmod 3 \Rightarrow 7^k \equiv 1 \pmod 3 \Rightarrow 2 \cdot 7^{4m+1} + 1 \equiv 3 \pmod 3$), odgovor je da ne može. □

6. a) Nađite sva rješenja Pellove jednadžbe $x^2 - 89y^2 = 1$ za koja vrijedi $1 < y < 100\,000$.

Rješenje: Razvijanjem u verižni razlomak dobije se:

$$\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}]$$

Period $r = 5$ je neparan, pa su sva rješenja jednadžbe $x^2 - 89y^2 = 1$ dana sa (p_{10n-1}, q_{10n-1}), $n \in \mathbb{N}$.

i	-1	0	1	2	3	4	5	6	7	8	**9**	10
a_i		9	2	3	3	2	18	2	3	3	2	18
p_i	1	9	19	66	217	500	9217	18934	66019	216991	**500001**	9217009
q_i	0	1	9	7	23	53	977	2007	6998	23001	**53000**	977001

Budući je $q_{10} > 100\,000$, jedino rješenje je $(x, y) = (p_9, q_9) = (500\,001, 53\,000)$ (za $(p_{-1}, q_{-1}) = (1, 0)$ nije zadovoljen uvjet $1 < y$). $\square$

b) Nađite sve Pitagorine trokute u kojima je jedna stranica jednaka 63.

Rješenje: Sve pitagorine trojke su dane identitetom:

$$[d(m^2 - n^2)]^2 + (2dmn)^2 = [d(m^2 + n^2]^2,$$

gdje su $d, m, n \in \mathbb{N}$, $(m, n) = 1$, $m > n$, m i n različite parnosti. Kako tražimo trojke u kojima je jedna stranica jednaka 63, to ne može biti druga stranica. Nadalje, iz $d \mid 63$ slijedi $d = 1, 3, 7, 9, 21$ (ili 63). Promotrimo sve mogućnosti:

$d = 1$. $\frac{63}{d} = 63 \equiv 3 \pmod 4$ pa jednadžba $m^2 + n^2 = 63$ nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 63$. $63 = 63 \cdot 1 = 21 \cdot 3 = 9 \cdot 7$. Kako je $(21, 3) \neq 1$, taj slučaj ne moramo promatrati (rješit ćemo ga kada budemo rješavali slučaj $d = 9$).

$$\begin{array}{lcl} m + n = 63,\, m - n = 1 \implies m = 32, n = 31 \implies (\mathbf{63}, \mathbf{1984}, \mathbf{1985}) \\ m + n = 9\ ,\, m - n = 7 \implies m = 8, n = 1 \implies (\mathbf{63}, \mathbf{16}, \mathbf{65}) \end{array}$$

$d = 3$. $\frac{63}{d} = 21 \equiv 1 \pmod 4$ pa jednadžba $m^2 + n^2 = 21$ možda ima rješenja. Provjerom svih mogućnosti $n < m < \sqrt{21}$ vidimo da ipak nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 21$. Iz $21 = 21 \cdot 1 = 7 \cdot 3$ imamo:

$$\begin{array}{l} m + n = 21,\, m - n = 1 \implies m = 11, n = 10 \implies (\mathbf{63}, \mathbf{660}, \mathbf{663}) \\ m + n = 7\ ,\, m - n = 3 \implies m = 5, n = 2 \implies (\mathbf{63}, \mathbf{60}, \mathbf{87}) \end{array}$$

$d = 7$. $\frac{63}{d} = 9 \equiv 1 \pmod 4$ pa jednadžba $m^2 + n^2 = 9$ možda ima rješenja. Provjerom svih mogućnosti $n < m < \sqrt{9} = 3$ vidimo da ipak nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 9$. Imamo samo jednu mogućnost:

$$m + n = 9,\, m - n = 1 \implies m = 5, n = 4 \implies (\mathbf{63}, \mathbf{280}, \mathbf{287})$$

$d = 9$. $\frac{63}{d} = 7 \equiv 3 \pmod 4$ pa jednadžba $m^2 + n^2 = 7$ nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 7$. Imamo samo jednu mogućnost:

$$m + n = 7,\, m - n = 1 \implies m = 4, n = 3 \implies (\mathbf{63}, \mathbf{216}, \mathbf{225})$$

$d = 21$. $\frac{63}{d} = 3 \equiv 3 \pmod 4$ pa jednadžba $m^2 + n^2 = 3$ nema rješenja. Promotrino jednadžbu $m^2 - n^2 = (m + n)(m - n) = 3$. Imamo samo jednu mogućnost:

$$m + n = 3,\, m - n = 1 \implies m = 2, n = 1 \implies (\mathbf{63}, \mathbf{84}, \mathbf{105})$$

Ukupno smo dobili **7** Pitagorinih trojki. $\square$

Vinko Petričević