Rješenja nekih zadataka iz diskretne matematike

U ovom dokumentu nalaze se rješenja (s postupcima) nekih zadataka (ukupno 31 zadatak) s ispita koji su objavljeni na stranicama predmeta. Niti jedan od riješenih zadataka ne pokriva gradivo *Algebarske strukture*. **Ne garantiram točnost postupaka**, ali konačno rješenje se podudara sa službenim rješenjima.

MI 16./17. 1.

(a) $\binom{177}{113}$ s koliko nula završava?

$$\binom{177}{113} = \frac{177!}{113!\,64!} = n$$

$$\operatorname{ord}_2(177!) = \left\lfloor \frac{177}{2} \right\rfloor + \dots + \left\lfloor \frac{177}{2^7} \right\rfloor = 88+44+22+11+5+2+1 = 173$$

$$\operatorname{ord}_5(177!) = \left\lfloor \frac{177}{5} \right\rfloor + \dots + \left\lfloor \frac{177}{5^3} \right\rfloor = 35+7+1 = 43$$

$$\operatorname{ord}_2(113!) = \left\lfloor \frac{113}{2} \right\rfloor + \dots + \left\lfloor \frac{113}{2^6} \right\rfloor = 56+28+14+7+3+1 = 109$$

$$\operatorname{ord}_5(113!) = \left\lfloor \frac{113}{5} \right\rfloor + \left\lfloor \frac{113}{5^2} \right\rfloor = 22+4 = 26$$

$$\operatorname{ord}_2(64!) = \left\lfloor \frac{64}{2} \right\rfloor + \dots + \left\lfloor \frac{64}{2^6} \right\rfloor = 32+16+8+4+2+1 = 63$$

$$\operatorname{ord}_5(64!) = \left\lfloor \frac{64}{5} \right\rfloor + \left\lfloor \frac{64}{5^2} \right\rfloor = 12+2 = 14$$

$$\operatorname{ord}_2(n) = \operatorname{ord}_2(177!) - \operatorname{ord}_2(113!) - \operatorname{ord}_2(64!) = 173-109-63 = 1$$

$$\operatorname{ord}_5(n) = \operatorname{ord}_5(177!) - \operatorname{ord}_5(113!) - \operatorname{ord}_5(64!) = 43-26-14 = 3$$

$\min(\operatorname{ord}_2(n), \operatorname{ord}_5(n)) = \min(1,3) = 1 \Rightarrow$ Završava s jednom nulom.

(b) $$\frac{2217!}{9^n} = \frac{2217!}{3^{2n}} = \frac{2217!}{3^m}$$

$$\cancel{\operatorname{ord}_9(2217!) = \left\lfloor \frac{2217}{9} \right\rfloor + \dots + \left\lfloor \frac{2217}{9^3} \right\rfloor = 246+27+3 = 276}$$

$$\cancel{\Rightarrow n = 276}$$

$$\operatorname{ord}_3(2217!) = \left\lfloor \frac{2217}{3} \right\rfloor + \dots + \left\lfloor \frac{2217}{3^7} \right\rfloor = 739+246+82+27+9+3+1 = 1107$$

$$m = 2n = 1107 \Rightarrow \boxed{n = 553}$$

MI 16./17. 2

$x \equiv 12 \pmod{24}$ $\quad x \equiv 39 \pmod{45}$ $\quad x \equiv 8 \pmod{44}$

$x \equiv 12 \pmod{3}$ $\quad x \equiv 39 \pmod{5}$ $\quad x \equiv 8 \pmod{4}$

$x \equiv 12 \pmod{8}$ $\quad x \equiv 39 \pmod{9}$ $\quad x \equiv 8 \pmod{11}$

$\cancel{x \equiv 0 \pmod{3}}$ $\quad x \equiv 4 \pmod{5}$ $\quad \cancel{x \equiv 0 \pmod{4}}$

$x \equiv 4 \pmod{8}$ $\quad x \equiv 3 \pmod{9}$ $\quad x \equiv 8 \pmod{11}$

$x \equiv 4 \pmod{8} \Rightarrow x \equiv 0 \pmod{4}$

$x \equiv 3 \pmod{9} \Rightarrow x \equiv 0 \pmod{3}$

Ekvivalentan sustav:

$x \equiv 4 \pmod{8}$

$x \equiv 4 \pmod{5}$ $\qquad 5 \cdot 8 \cdot 9 \cdot 11 = 3960$

$x \equiv 3 \pmod{9}$

$x \equiv 8 \pmod{11}$

$x \equiv 5 \cdot 9 \cdot 11 \cdot x_1 + 8 \cdot 9 \cdot 11 x_2 + 8 \cdot 5 \cdot 11 \cdot x_3 + 8 \cdot 5 \cdot 9 \cdot x_4 \pmod{3960}$

$x \equiv 495 x_1 + 792 x_2 + 440 x_3 + 360 x_4 \pmod{3960}$

$495 x_1 \equiv 4 \pmod{8} \Rightarrow 7x_1 \equiv 4 \pmod{8} \Rightarrow x_1 = 4$

$792 x_2 \equiv 4 \pmod{5} \Rightarrow 2x_2 \equiv 4 \pmod{5} \Rightarrow x_2 = 2$

$440 x_3 \equiv 3 \pmod{9} \Rightarrow 8x_3 \equiv 3 \pmod{9} \Rightarrow x_3 = 6$

$360 x_4 \equiv 8 \pmod{11} \Rightarrow 8x_4 \equiv 8 \pmod{11} \Rightarrow x_4 = 1$

$x \equiv 495 \cdot 4 + 792 \cdot 2 + 440 \cdot 6 + 360 \cdot 1 \pmod{3960}$

$x \equiv 6564 \pmod{3960}$

$\boxed{x \equiv 2604 \pmod{3960}}$

$x - 2604 = 3960 \cdot k$

$x = 3960 \cdot k + 2604$

$x > 2 \cdot 10^6 \Rightarrow 3960 \cdot k + 2604 > 2 \cdot 10^6$

$k > \frac{2 \cdot 10^6 - 2604}{3960} \Rightarrow \boxed{k = 505}$

$\Uparrow$

$\boxed{x = 2002404}$

MI 16./17. 3.

(a) Najmanji primitivni korjen modulo 31.

Za svaki prosti broj g počevši od 2 treba provjeriti vrijede li jednadžbe

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

gdje su q prosti faktori od p-1.

$p = 31$

$p-1 = 30 \Rightarrow q = \{2,3,5\}$

g=2

$$2^{\frac{30}{2}} \equiv 2^{15} \equiv 1 \pmod{31}$$

$$2^{\frac{30}{3}} \equiv 2^{10} \equiv 1 \pmod{31}$$

$$2^{\frac{30}{5}} \equiv 2^{6} \equiv 2 \not\equiv 1 \pmod{31}$$

g=3

$$3^{15} \equiv 30 \not\equiv 1 \pmod{31}$$

$$3^{10} \equiv 25 \not\equiv 1 \pmod{31}$$

$$3^{6} \equiv 16 \not\equiv 1 \pmod{31}$$

$\Rightarrow$ 3 je najmanji primitivni korjen modulo 31.

(b) $\dfrac{10^n+23}{31} \in \mathbb{N} \iff 10^n+23 = 31\cdot k,\ k\in\mathbb{Z}$

$$10^n \equiv -23 \pmod{31}$$

$$10^n \equiv 8 \pmod{31}$$

$$\Rightarrow \operatorname{ind}_3 10^n \equiv \operatorname{ind}_3 8 \pmod{30}$$

$$n\cdot \operatorname{ind}_3 10 \equiv \operatorname{ind}_3 8 \pmod{30}$$

$$3^l \equiv 10 \pmod{31}$$

$$l = 0,1,\ldots,\varphi(31)-1 = 30-1 = 29$$

isprobavanjem u kalkulator $\dfrac{-10+3^l}{31}$ dok rezultat nije $\in \mathbb{Z}$

dobije se $l=14$ tj. vrijedi $3^{14} \equiv 10 \pmod{31}$

$$3^l \equiv 8 \pmod{31}$$

$$l = 12$$

$$14\cdot n \equiv 12 \pmod{30} \Rightarrow 7n \equiv 6 \pmod{15}$$

$$\Rightarrow n \equiv 3 \pmod{15}$$

$$n = 15k+3$$

$$2016 \geq n \geq 1994$$

$$1994 \leq 15k+3 \leq 2016$$

$$1991 \leq 15k \leq 2013$$

$$133 \leq k \leq 134$$

$$\Rightarrow k = \{133, 134\} \Rightarrow \boxed{n = \{1998, 2013\}}$$

MI 16./17. 4.

(a) Potpun: $\{0,1,2,\dots,19\}$

Reducirani: $\{1,3,7,9,11,13,17,19\}$ – svi brojevi od $\{1,\dots,20\}$ za koje vrijedi $(a,20)=1$

(c)

17^{90409}

Euler: $(17,100)=1 \Rightarrow 17^{\varphi(100)} \equiv 1 \pmod{100}$

$\Rightarrow 17^{40} \equiv 1 \pmod{100}$

$$\varphi(\underbrace{100}_{2^2\cdot 5^2}) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$$

$17^{90409} \equiv (17^{40})^{2260} \cdot 17^9 \equiv$

$\equiv 1^{2260} \cdot 17^9 \equiv 17^9 \equiv 13^3 \equiv 97 \pmod{100}$

Zadnje dvije znamenke su 97.

$\boxed{\text{MI 16./17. 5.}}$

(a) $\left(\frac{-74}{227}\right)=\left(\frac{-1}{227}\right)\cdot\left(\frac{74}{227}\right)\cancel{=(-1)^{\frac{227-1}{2}}\cdot(-1)^{\frac{(227-1)(74-1)}{4}}\left(\frac{227}{74}\right)=}$

$=(-1)^{113}\left(\frac{2}{227}\right)\left(\frac{37}{227}\right)=-1\cdot(-1)^{\frac{227^2-1}{8}}\cdot(-1)^{\frac{(227-1)(37-1)}{4}}\left(\frac{227}{37}\right)=$

$=-1\cdot(-1)\cdot 1\cdot\left(\frac{227}{37}\right)=\left(\frac{5}{37}\right)=(-1)^{\frac{36\cdot 4}{4}}\cdot\left(\frac{37}{5}\right)=$

$=\left(\frac{2}{5}\right)=(-1)^{\frac{25-1}{8}}=-1$ //

$\left(\frac{319}{227}\right)=\left(\frac{92}{227}\right)=\underbrace{\left[\left(\frac{2}{227}\right)\right]^2}_{=1}\cdot\left(\frac{23}{227}\right)=(-1)^{\frac{22\cdot 226}{4}}\cdot\left(\frac{227}{23}\right)=$

$=-1\cdot\left(\frac{20}{23}\right)=-1\left[\left(\frac{2}{23}\right)\right]^2\cdot\left(\frac{5}{23}\right)=-1\cdot(-1)^{\frac{22\cdot 4}{4}}\cdot\left(\frac{23}{5}\right)=$

$=-1\cdot\left(\frac{3}{5}\right)=-1\cdot(-1)^{\frac{2\cdot 4}{4}}\cdot\left(\frac{5}{3}\right)=-1\cdot\left(\frac{2}{3}\right)=-1\cdot(-1)^{\frac{9-1}{8}}=$

$=1$ //

(b) Ima li kongruencija $x^2\equiv(-74)\cdot 319 \pmod{227}$ rješenje?

$\left(\frac{-74\cdot 319}{227}\right)=\left(\frac{-74}{227}\right)\cdot\left(\frac{319}{227}\right)=-1\cdot 1=-1$

$\Rightarrow$ Legendreov simbol $\left(\frac{-74\cdot 319}{227}\right)$ jednak je -1 i iz tog slijedi da početna kongruencija nema rješenja i da je $-74\cdot 319$ kvadratni neostatak modulo 227.

Kod Legendreovog simbola $\left(\frac{a}{p}\right)$, p mora biti prost broj.

(c) $\left(\frac{1}{19}\right)+\left(\frac{2}{19}\right)+\dots+\left(\frac{16}{19}\right)$

Vrijedi: $\displaystyle\sum_{k=1}^{18}\left(\frac{k}{19}\right)=0$

$$\left(\frac{17}{19}\right)=(-1)^{\frac{18\cdot16}{4}}\cdot\left(\frac{19}{17}\right)=\left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=1$$

$$\left(\frac{18}{19}\right)=\left(\frac{2}{19}\right)\cdot\underbrace{\left[\left(\frac{3}{19}\right)\right]^2}_{1}=(-1)^{\frac{19^2-1}{8}}=-1$$

$$\Rightarrow \sum_{k=1}^{16}\left(\frac{k}{19}\right)=0$$

$\boxed{\text{MI 16./17. 6.}}$

(a) $\varphi(n)=10$

$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r}$ $\quad\varphi(n)=p_1^{\alpha_1-1}(p_1-1)\cdot\ldots\cdot p_r^{\alpha_r-1}(p_r-1)$

$p_i-1 \mid 10 \quad\Rightarrow\quad p_i=\{2,3,6,11\}$

p_i prost $\Rightarrow p_i=\{2,3,11\}$

$n=2^{\alpha_1}\cdot3^{\alpha_2}\cdot11^{\alpha_3}$

$\underline{1^\circ}$ $n=11k \Rightarrow \varphi(n)=\varphi(11k)=\varphi(11)\cdot\varphi(k)=10\cdot\varphi(k)=10$

$\Rightarrow \varphi(k)=1 \Rightarrow k=\{1,2\} \Rightarrow n=\{11,22\}$

$\underline{2^\circ}$ $n=2^{\alpha_1}\cdot3^{\alpha_2} \Rightarrow \varphi(n)=\varphi(2^{\alpha_1}3^{\alpha_2})=2^{\alpha_1-1}\cdot3^{\alpha_2-1}\cdot(3-2)=$

$=2^{\alpha_1}\cdot3^{\alpha_2-1}=10=2\cdot5 \Rightarrow$ nema rješenja.

$$\boxed{n=\{11,22\}}$$

(b) $\frac{\varphi(n)}{n} = \frac{2}{7}$

$7\varphi(n) = 2n \Rightarrow 7 \mid n \Rightarrow n = 7^{\alpha}\cdot m, \quad (m,7)=1$

$7\varphi(7^{\alpha}\cdot m) = 2\cdot 7^{\alpha}\cdot m$

$7\varphi(7^{\alpha})\cdot\varphi(m) = 2\cdot 7^{\alpha}\cdot m$

$\cancel{7\cdot 7^{\alpha-1}}\cdot \cancel{6}_{3}\cdot\varphi(m) = \cancel{7^{\alpha}}\cdot\cancel{2}\cdot m$

$3\varphi(m) = m \Rightarrow 3 \mid m \Rightarrow m = 3^{\beta}\cdot k, \quad (k,3)=1$

$3\varphi(3^{\beta}\cdot k) = 3^{\beta}\cdot k$

$3\varphi(3^{\beta})\cdot\varphi(k) = 3^{\beta}\cdot k$

$\cancel{3\cdot 3^{\beta-1}}\cdot 2\varphi(k) = \cancel{3^{\beta}}\cdot k$

$2\varphi(k) = k \Rightarrow 2 \mid k \Rightarrow k = 2^{\gamma}\cdot l, \quad (l,2)=1$

$2\cdot\varphi(2^{\gamma}\cdot l) = 2^{\gamma}\cdot l$

$\cancel{2\cdot 2^{\gamma-1}}\cdot\varphi(l) = \cancel{2^{\gamma}}\cdot l$

$\varphi(l) = l \Rightarrow l = 1 \Rightarrow \boxed{n = 7^{\alpha}\cdot 3^{\beta}\cdot 2^{\gamma}, \quad \alpha,\beta,\gamma\in\mathbb{N}}$

MI 16./17. 7.

Odredite sve Pitagorine trokute kojima je jedna stranica jednaka 78.

1. Stranice su oblika $(d(m^2-n^2),\ 2dmn,\ d(m^2+n^2))$.
2. m i n su različite parnosti
3. $(m,n) = 1$

Uputa: Za svaki d, $d \mid 78$ probati riješiti gornja tri oblika uvrštavanjem d u jednadžbu.
npr. $d=3 \Rightarrow 3(m^2-n^2) = 78 \Rightarrow m^2-n^2=26$
... i tako dalje.

$d \mid 78 \Rightarrow d = \{1, 2, 3, 6, 13, 26, 39, 78\}$

1° $d = 1$

$m^2 - n^2 = 78 \iff 78 \not\equiv 2 \pmod 4$

$78 \equiv 2 \pmod 4 \Rightarrow m^2 - n^2 \neq 78.$

$2mn = 78 \Rightarrow mn = 39 = 3 \cdot 13 \Rightarrow m = 13, n = 3$, ali moraju biti različitih parnosti

$m^2 + n^2 = 78 = 2 \cdot 3 \cdot 13 \iff \begin{matrix} 2 \equiv 1 \pmod 4 \\ 3 \equiv 1 \pmod 4 \\ 13 \equiv 1 \pmod 4 \end{matrix}$

$2 \not\equiv 1 \pmod 4 \Rightarrow m^2 + n^2 \neq 78.$

2° $d = 2$

$m^2 - n^2 = 39 \iff 39 \not\equiv 2 \pmod 4$

$\boxed{39 \equiv 3 \not\equiv 2 \pmod 4} \Rightarrow (m-n)(m+n) = 13 \cdot 3 = 39 \cdot 1$

$m - n = 3$, $m + n = 13$ $\vee$ $m - n = 1$, $m + n = 39$

$m = 8$, $n = 5$, $d = 2$ $\Downarrow$ $\boxed{(78, 160, 178)}$

$m = 20$, $n = 19$, $d = 2$ $\Downarrow$ $\boxed{(78, 1520, 1522)}$

$2mn = 39 \Rightarrow \Leftarrow$ jer $2 \cdot m \cdot n$ je sigurno parno, a 39 nije paran broj

$m^2 + n^2 = 39 = 3 \cdot 13 \iff \begin{matrix} 3 \equiv 1 \pmod 4 \\ 13 \equiv 1 \pmod 4 \end{matrix}$

$3 \not\equiv 1 \pmod 4 \Rightarrow m^2 + n^2 \neq 39.$

3° $d = 3$

$m^2 - n^2 = 26 \iff 26 \not\equiv 2 \pmod 4$

$26 \equiv 2 \pmod 4 \Rightarrow m^2 - n^2 \neq 26$

$2mn = 26 \Rightarrow m \cdot n = 13 = 13 \cdot 1$ m i n moraju biti različite parnosti.

$m^2 + n^2 = 2 \cdot 13 \iff \begin{matrix} 2 \equiv 1 \pmod 4 \\ 13 \equiv 13 \pmod 4 \end{matrix}$

$2 \not\equiv 1 \pmod 4 \Rightarrow m^2 + n^2 \neq 26.$

$\underline{4^\circ}$ $d=6$

$m^2-n^2=13 \iff 13 \not\equiv 2 \pmod 4$

$13 \equiv 1 \not\equiv 2 \pmod 4 \Rightarrow (m-n)(m+n)=1\cdot 13 \Rightarrow$ $\begin{array}{l} m-n=1 \\ \underline{m+n=13} \\ m=7 \\ n=6 \\ d=6 \end{array}$

$\Downarrow$

$\boxed{(78, 504, 510)}$

$2mn=13 \Rightarrow\Leftarrow$

$m^2+n^2=13 \iff 13 \equiv 1 \pmod 4$

$13 \equiv 1 \pmod 4 \Rightarrow m^2+n^2=13 \Rightarrow m=3, n=2, d=6$

$\Downarrow$

$\boxed{(30, 72, 78)}$

$\underline{5^\circ}$ $d=13$

$m^2-n^2=6 \iff 6 \not\equiv 2 \pmod 4$

$6 \equiv 2 \pmod 4 \Rightarrow m^2-n^2 \neq 6$

$2mn=6 \Rightarrow m\cdot n=3$ m i n moraju biti različitih parnosti.

$m^2+n^2=6=2\cdot 3 \iff$ $\begin{array}{l} 2 \equiv 1 \pmod 4 \\ 3 \equiv 1 \pmod 4 \end{array}$

$3 \not\equiv 1 \pmod 4 \Rightarrow m^2+n^2 \neq 6$

$\underline{6^\circ}$ $d=26$

$m^2-n^2=3 \iff 3 \not\equiv 2 \pmod 4$

$3 \not\equiv 2 \pmod 4 \Rightarrow (m-n)(m+n)=3 \Rightarrow$ $\begin{array}{l} m-n=1 \\ \underline{m+n=3} \\ m=2 \\ n=1 \\ d=2 \end{array} \Rightarrow \boxed{(78, 104, 130)}$

$m^2+n^2=3 \iff 3 \equiv 1 \pmod 4$

$3 \not\equiv 1 \pmod 4 \Rightarrow m^2+n^2 \neq 3$.

$2mn=26 \Rightarrow mn=13$ m i n moraju biti različitih parnosti.

$\underline{7^\circ}$ $d = 39$

$m^2 - n^2 = 2 \iff 2 \not\equiv 2 \pmod 4$

$2mn = 2 \Rightarrow mn = 1$ ⊗

$m^2 + n^2 = 2$ ⊗

NE POSTOJI PITAGORIN TROKUT SA STRANICAMA DULJINE 1 i 2.

$\underline{8^\circ}$ $d = 78$

$m^2 - n^2 = 1 \iff 1 \not\equiv 2 \pmod 4$

$(m-n)(m+n) = 1$

Rješenje:

(30, 72, 78) (78, 104, 130) (78, 160, 178) (78, 504, 510)

(78, 1520, 1522)

ZI 16./17. 1.

(a) $\alpha = [3; 2, 1]$

$$\alpha = 3 + \cfrac{1}{2 + \cfrac{1}{1}} = \frac{10}{3}$$

(b) $\beta = [3; \overline{2, 1}]$

$$\beta = 3 + \frac{1}{\gamma} \qquad \gamma = 2 + \cfrac{1}{1 + \cfrac{1}{\gamma}} = 2 + \frac{\gamma}{\gamma + 1} = \frac{2\gamma + 2 + \gamma}{\gamma + 1}$$

$$\Rightarrow \gamma = \frac{3\gamma + 2}{\gamma + 1} \Rightarrow \gamma^2 + \gamma = 3\gamma + 2 \Rightarrow \gamma^2 - 2\gamma - 2 = 0$$

$$\Rightarrow \gamma = 1 \oplus \sqrt{3}$$

$$\beta = 3 + \frac{1}{1 \pm \sqrt{3}} = \frac{5 + \sqrt{3}}{2}$$

$$\boxed{\beta = \frac{5 + \sqrt{3}}{2}}$$

(c)

$$\sqrt{1+303n^2} = m \quad , \quad n, m \in \mathbb{N}$$

$$m^2 = 1 + 303n^2$$

$$m^2 - 303n^2 = 1$$

$$d = 303$$

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{l-1}, 2a_0}]$$

$$\boxed{a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor \qquad a_0 = \lfloor \sqrt{d} \rfloor}$$

$$\boxed{s_{i+1} = a_i t_i - s_i \qquad t_{i+1} = \frac{d - (s_{i+1})^2}{t_i}} \qquad \boxed{s_0 = 0 \quad s_1 = a_0 \quad t_0 = 1}$$

	0	1	2	3	4	5	6	7	8
a_i	17	2	2	5	2	2	34	2	2
s_i	0	17	11	15	15	11	17	17	11
t_i	1	14	13	6	13	14	1	14	13

$\Rightarrow \boxed{l = 6}$

$$\sqrt{303} = [17; \overline{2, 2, 5, 2, 2, 34}]$$

l paran	l neparan
$x^2 - dy^2 = -1$ nema rješenja $x^2 - dy^2 = 1$ ima rješenja (p_{nl-1}, q_{nl-1}) fundamentalno: (p_{l-1}, q_{l-1})	$x^2 - dy^2 = -1$ $(p_{(2n-1)l-1}, q_{(2n-1)l-1})$ fundamentalno: (p_{l-1}, q_{l-1}) $x^2 - dy^2 = 1$ (p_{2nl-1}, q_{2nl-1}) fundamentalno: (p_{2l-1}, q_{2l-1})

$$\boxed{\begin{aligned} p_{n+1} &= p_n \cdot a_{n+1} + p_{n-1} \\ q_{n+1} &= q_n \cdot a_{n+1} + q_{n-1} \end{aligned}}$$

$$\boxed{\begin{aligned} p_{-1} &= 1 \\ q_{-1} &= 0 \\ p_0 &= a_0 \\ q_0 &= 1 \end{aligned}}$$

p je rješenje za u tj. x

q je rješenje za u tj. y

	-1	0	1	2	3	4	5	6
a_n		17	2	2	5	2	2	34
p_n	1	17	35	87	470	1027	2524	86843
q_n	0	1	2	5	27	59	145	4989

Najmanje rješenje Pellove jednadžbe nazivamo fundamentalno rješenje : (x_1, y_1) : $x_1 + y_1\sqrt{d}$.

$l = 6$

fundamentalno za $n = 1$:

$$(p_{nl-1}, q_{nl-1}) = (p_{1\cdot 6-1}, q_{1\cdot 6-1}) = (p_5, q_5) = (2524, 145)$$

$\Rightarrow \boxed{u = 145}$

$\boxed{\text{ZI } 16./17. \; 6.}$

RSA

$(n, e) = (8549, 239) = (83 \cdot 103, 239)$

$y = 242$

$x = ?$

$$\boxed{x = y^d \bmod n}$$

$d = ?$

$$\boxed{e \cdot d \equiv 1 \pmod{\varphi(n)}}$$

$\varphi(n) = \varphi(8549) = \varphi(83 \cdot 103) = (83-1)(103-1) = 8364$

$239 d \equiv 1 \pmod{8364}$

$$d = \frac{1 + 8364k}{239} = (k=1) = 35 \Rightarrow \boxed{d = 35}$$

$y^d = 242^{35} = 2^{35} \cdot 11^{35} \cdot 11^{35}$

$\cancel{2^{35} = (2^{15})^2 \cdot 2^5}$

$\cancel{2^{15} \equiv 7676 \pmod{8364}}$

$\cancel{2^{30} \equiv 7676^2 \equiv 4960 \pmod{8364}}$

$\cancel{2^{35} \equiv 2^5 \cdot 4960 \equiv 8168 \pmod{8364}}$

$\cancel{11^5 \equiv 2135 \pmod{8364}}$

$\cancel{11^{10} \equiv 2135^2 \equiv 8209 \pmod{8364}}$

$\cancel{11^{30} \equiv 8209^3 \equiv 6469 \pmod{8364}}$

$\cancel{11^{35} \equiv 2135 \cdot 6469 \equiv 2351 \pmod{8364}}$

$\cancel{y^d \equiv 242^{35} \equiv 2^{35} \cdot 11^{35} \cdot 11^{35} \equiv 8168 \cdot 2351 \cdot 2351 \equiv 7340 \pmod{8364}}$

OVO JE KRIVO JER SAM RAČUNAO $y^d \bmod \varphi(n)$, A NE $y^d \bmod n$!

$$y^d = 242^{35}$$

$$x = y^d \bmod n.$$

$$y^d = 242^{35} = (2\cdot 11\cdot 11)^{35} = 2^{35}\cdot 11^{35}\cdot 11^{35} = 2^{35}\cdot 11^{70}$$

$$2^{15} \equiv 7121 \pmod n$$

$$2^{30} \equiv 7121^2 \equiv 4522 \pmod n$$

$$2^{35} \equiv 2^5 \cdot 4522 \equiv 7920 \pmod n$$

$$11^5 \equiv 7169 \pmod n$$

$$11^{10} \equiv 7169^2 \equiv 6522 \pmod n$$

$$11^{15} \equiv 7169\cdot 6522 \equiv 1737 \pmod n$$

$$11^{30} \equiv 1737^2 \equiv 7921 \pmod n$$

$$11^{35} \equiv 7921\cdot 7169 \equiv 3191 \pmod n$$

$$11^{70} \equiv 3191^2 \equiv 622 \pmod n$$

$$y^d \equiv 242^{35} \equiv 2^{35}\cdot 11^{70} \equiv 7920\cdot 622 \equiv 2016 \pmod n$$

$$\Rightarrow \boxed{x = 2016}$$

Kriptiranje:

$$\boxed{y = x^e \bmod n}$$

$\boxed{\text{ZI } 16./17.\ 7.}$

Rabin

$(n, p, q) = (3713, 47, 79)$

$y = 2311$

$x < n$ i zadnja četiri bita su jednaka

provjera: $47 \equiv 79 \equiv 3 \pmod 4$

$$2311^{\frac{47+1}{4}} \equiv 2311^{12} \equiv 17^{6} \equiv 14 \pmod{47}$$

$$2311^{\frac{79+1}{4}} \equiv 2311^{20} \equiv 5^{10} \equiv 40 \pmod{79}$$

$x \equiv \pm 14 \pmod{47}$

$x \equiv \pm 40 \pmod{79}$

$47 \cdot 79 = 3713$

mali kineski: $x \equiv \pm 14 \cdot 79 \cdot m \pm 40 \cdot 47 \cdot n \pmod{3713}$

$$79m + 47n = 1$$

$79 = 47 \cdot 1 + 32$

$47 = 32 \cdot 1 + 15$

$32 = 15 \cdot 2 + 2$

$15 = 2 \cdot 7 + \underline{1}$

i	-1	0	1				
q_i			1	1	2	7	
m_i	1	0	1	-1	3	-22	$\Rightarrow m = -22$
n_i	0	1	-1	2	-5	37	$\Rightarrow n = 37$

$$x \equiv \pm 14 \cdot 79 \cdot 22 \pm 40 \cdot 47 \cdot 37 \pmod{3713}$$

$$x \equiv \pm 24332 \pm 69560 \pmod{3713}$$

$$x \equiv 1067, 3041, 2646, 672 \pmod{3713}$$

$\boxed{\text{Kriptiranje: } y = x^2 \bmod n}$

$(1067)_{10} = (\ldots 1011)_2$

$(3041)_{10} = (\ldots 0001)_2$

$(2646)_{10} = (\ldots 0110)_2$

$(672)_{10} = (\ldots \underline{0000})_2 \Rightarrow \boxed{x = 672}$

provjera: $x^2 \equiv 672^2 \equiv 2311 \pmod{3713}$

$\boxed{\text{MI } 14./15.\ 1.}$

$539 = 364 \cdot 1 + 175$

$364 = 175 \cdot 2 + 14$

$175 = 14 \cdot 12 + \underline{7} \Rightarrow nzd(539, 364) = 7$

$14 = 7 \cdot 2$

$z \in [-500, -200]$

$364z \equiv 119 \pmod{539}$

$52x \equiv 17 \pmod{77}$

$77m + 52u = 1$

$77 = 52 \cdot 1 + 25$

$52 = 25 \cdot 2 + 2$

$25 = 2 \cdot 12 + 1$

$2 = 2 \cdot 1$

i	-1	0	1	2	3	
q_i			1	2	12	
m_i	1	0	1	-2	25	$\Rightarrow m = 25$
u_i	0	1	-1	3	-37	$\Rightarrow u = -37$

$$77 \cdot 25 + 52 \cdot (-37) = 1$$

$52x \equiv 1 \pmod{77} \Rightarrow x \equiv -37 \pmod{77} \Rightarrow 52x \equiv 17 \pmod{77}$

$\Rightarrow x \equiv -37 \cdot 17 \equiv$

$\equiv 64 \pmod{77}$

$\cancel{z \equiv 64+77\cdot 0, 64+77\cdot 1, 64+77\cdot 2, 64+77\cdot 3, 64+77\cdot 4, 64+77\cdot 5, 64+77\cdot 6 \pmod{539}}$

$z \equiv 64, 141, 218, 295, 372, 449, 526 \pmod{539}$

---

opće rješenje: $\underline{64 + 77k}$

$-500 \leq 64 + 77k \leq -200$

$-7.32 \leq k \leq -3.42$

$\Rightarrow k \in \{-7, -6, -5, -4\}$

$\Rightarrow z \in \{-475, -398, -321, -244\}$

Zl 14./15. 2.

$x \equiv 11 \pmod{54}$ $x \equiv 29 \pmod{45}$ $x \equiv 9 \pmod{20}$

$x \equiv 11 \pmod{6}$ $x \equiv 29 \pmod{5}$ $x \equiv 9 \pmod{4}$

$x \equiv 11 \pmod{9}$ $x \equiv 29 \pmod{9}$ $x \equiv 9 \pmod{5}$

$x \equiv 5 \pmod{6}$ $\cancel{x \equiv 4 \pmod{5}}$ $x \equiv 1 \pmod{4}$

$\cancel{x \equiv 2 \pmod{9}}$ $x \equiv 2 \pmod{9}$ $x \equiv 4 \pmod{5}$

---

ekvivalentan sustav:

$x \equiv 1 \pmod{4}$

$x \equiv 4 \pmod{5}$

$x \equiv 5 \pmod{6}$

$x \equiv 2 \pmod{9}$

$x \equiv 11 \pmod{54}$ $x \equiv 29 \pmod{45}$ $x \equiv 9 \pmod{20}$

$x \equiv 11 \pmod{2}$ $x \equiv 29 \pmod{5}$ $x \equiv 9 \pmod{4}$

$x \equiv 11 \pmod{27}$ $x \equiv 29 \pmod{9}$ $x \equiv 9 \pmod{5}$

$\cancel{x \equiv 1 \pmod{2}}$ $\cancel{x \equiv 4 \pmod{5}}$ duplic! $\boxed{x \equiv 1 \pmod{4}}$

$\boxed{x \equiv 11 \pmod{27}}$ $x \equiv 2 \pmod{9}$ $\boxed{x \equiv 4 \pmod{5}}$

$x \equiv 1 \pmod{4} \Rightarrow x \equiv 1 \pmod{2}$

$x \equiv 11 \pmod{27} \Rightarrow x \equiv 2 \pmod{9}$

ekvivalentan sustav:

$x \equiv 1 \pmod{4}$

$x \equiv 4 \pmod{5}$

$x \equiv 11 \pmod{27}$

$x \equiv 1 \pmod 4$
$x \equiv 4 \pmod 5$
$x \equiv 11 \pmod{27}$

$4 \cdot 5 \cdot 27 = 540$

$$x \equiv 5 \cdot 27 \cdot x_1 + 4 \cdot 27 \cdot x_2 + 4 \cdot 5 \cdot x_3 \pmod{540}$$

$135 x_1 \equiv 1 \pmod 4 \Rightarrow 3x_1 \equiv 1 \pmod 4 \Rightarrow x_1 = 3$
$108 x_2 \equiv 4 \pmod 5 \Rightarrow 3x_2 \equiv 4 \pmod 5 \Rightarrow x_2 = 3$
$20 x_3 \equiv 11 \pmod{27} \Rightarrow 20x_3 \equiv 11 \pmod{27} \Rightarrow x_3 = 10$

$x \equiv 5 \cdot 27 \cdot 3 + 4 \cdot 27 \cdot 3 + 4 \cdot 5 \cdot 10 \pmod{540}$

$x \equiv 929 \equiv 389 \pmod{540}$

$x = 389 + 540k$

$x > 10^6$

$389 + 540k > 10^6$

$k > 1851.13 \Rightarrow k = 1852 \Rightarrow \boxed{x = 1000469}$

$\boxed{\text{ZI 14./15. 3.}}$

(a) Koliko ima primitivnih korijena modulo 43? Odredite najmanji među njima!

$\boxed{\text{Ima ih } \varphi(p-1)}$

$\varphi(43-1) = \varphi(42) = \varphi(2 \cdot 3 \cdot 7) = \varphi(2) \cdot \varphi(3) \cdot \varphi(7) =$
$= 1 \cdot 2 \cdot 6 = 12$

Test za 2:

$2^{\frac{42}{2}} \equiv 2^{21} \equiv 42 \not\equiv 1 \pmod{43}$
$2^{\frac{42}{3}} \equiv 2^{14} \equiv 1 \pmod{43}$
$\Rightarrow$ 2 nije p.k mod 43

Test za 3:

$3^{\frac{42}{2}} \equiv 3^{21} \equiv 37^3 \equiv 42 \not\equiv 1 \pmod{43}$
$3^{\frac{42}{3}} \equiv 3^{14} \equiv 37^2 \equiv 36 \not\equiv 1 \pmod{43}$
$3^{\frac{42}{7}} \equiv 3^6 \equiv 41 \not\equiv 1 \pmod{43}$
$\Rightarrow$ 3 je najmanji primitivan korijen modulo 43.

(b) $22^x \equiv 41 \pmod{43}$

$\text{ind}_3 22^x \equiv \text{ind}_3 41 \pmod{42}$

$x\,\text{ind}_3 22 \equiv \text{ind}_3 41 \pmod{42}$

$\text{ind}_3 22$

$3^l \equiv 22 \pmod{43}$

$l = 0, 1, \dots, \underbrace{\varphi(43)-1}_{=41}$

$\Rightarrow l = 15$

$\text{ind}_3 41$

$3^l \equiv 41 \pmod{43}$

$l = 0, 1, \dots, \underbrace{\varphi(43)-1}_{=41}$

$\Rightarrow l = 6$

$15x \equiv 6 \pmod{42}$ $\quad$ $\text{nzd}(15, 42) = 3$

$\Rightarrow 5x \equiv 2 \pmod{14}$

$\Rightarrow x \equiv 6 \pmod{14}$

$$\boxed{x \equiv 6, 20, 34 \pmod{42}}$$

MI 14./15. 4.

(b) Posljednje tri znamenke broja 14^{2014}.

Euler: $(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$1000 = 8 \cdot 125$ $\quad$ $(8, 125) = 1$

$\varphi(125) = \varphi(5^3) = 5^2 \cdot 4 = 100$

$(125, 14) = 1 \Rightarrow 14^{\varphi(125)} \equiv 1 \pmod{125}$

$14^{100} \equiv 1 \pmod{125}$

$14^{2000} \equiv 1 \pmod{125}$

$14^{2014} \equiv 14^{14} \equiv 71^7 \equiv 71 \cdot (71^2)^3 \equiv 71 \cdot 41^3 \equiv 71 \cdot 46 \equiv 16 \pmod{125}$

$14^{2014} = 2^{2014} \cdot 7^{2014} = \underline{2^3} \cdot 2^{2011} \cdot 7^{2014} \equiv 0 \pmod{8}$

Tražimo dakle:

$$a \equiv 16 \pmod{125}$$
$$a \equiv 0 \pmod{8}$$

$125m + 8n = 1$

$125 = 8 \cdot 15 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + \underline{1}$

i	-1	0	1	2	3	4	
q_i			15	1	1	1	
m_i	1	0	1	-1	2	-3	$\Rightarrow m = -3$
n_i	0	1	-15	16	-31	47	$\Rightarrow n = 47$

$$\therefore a \equiv 16 \cdot 8 \cdot n + 0 \cdot 125 \cdot m \pmod{1000}$$
$$a \equiv 16 \cdot 8 \cdot 47 \pmod{1000}$$
$$a \equiv 6016 \pmod{1000}$$
$$a \equiv 16 \pmod{1000} \Rightarrow \text{Zadnje tri znamenke: } \boxed{016}$$

Drugi način:

$$14^2 \equiv 196 \pmod{1000}$$
$$14^4 \equiv 196^2 \equiv 416 \pmod{1000}$$
$$14^8 \equiv 416^2 \equiv 56 \pmod{1000}$$
$$14^{14} \equiv 14^2 \cdot 14^4 \cdot 14^8 \equiv 196 \cdot 416 \cdot 56 \equiv 16 \pmod{1000}$$
$$14^{20} \equiv 14^{14} \cdot 14^4 \cdot 14^2 \equiv 16 \cdot 416 \cdot 196 \equiv 576 \pmod{1000}$$
$$14^{40} \equiv 576^2 \equiv 776 \pmod{1000}$$
$$14^{100} \equiv 14^{40} \cdot 14^{40} \cdot 14^{20} \equiv 776 \cdot 776 \cdot 576 \equiv 376 \pmod{1000}$$
$$14^{200} \equiv 376^2 \equiv 376 \pmod{1000}$$
$$14^{400} \equiv 376^2 \equiv 376 \pmod{1000}$$
$$14^{1600} \equiv (376^2)^2 \equiv 376 \pmod{1000}$$
$$14^{2000} \equiv 376 \cdot 376 \equiv 376 \pmod{1000}$$
$$14^{2014} \equiv 376 \cdot 16 \equiv 6016 \equiv 16 \pmod{1000}$$

$$\Rightarrow \text{Zadnje tri znamenke: } \boxed{016}$$

MI 14./15. 5.

(a) Ima li kongruencija $x^2 \equiv -7 \pmod{71}$ rješenja?

$$\left(\frac{-7}{71}\right) = \left(\frac{-1}{71}\right)\cdot\left(\frac{7}{71}\right) = \underbrace{(-1)^{\frac{71-1}{2}}}_{=-1} \cdot \underbrace{(-1)^{\frac{(71-1)(7-1)}{4}}}_{=-1} \cdot \left(\frac{71}{7}\right) =$$

$$= \left(\frac{71}{7}\right) = \left(\frac{1}{7}\right) = 1$$ $\Rightarrow$ Zadana kongruencija ima rješenje jer je Legendreov simbol $\left(\frac{-7}{71}\right)$ jednak 1, a to znači da je -7 kvadratni ostatak modulo 71 t.j. da $\exists x$: $x^2 \equiv -7 \pmod{71}$.

MI 14./15. 6.

(a) $\varphi(4^\alpha 5^\beta 6^\gamma) = 5760$

$$\varphi(2^{2\alpha}\cdot 5^\beta \cdot 2^\gamma \cdot 3^\gamma) = \varphi(2^{2\alpha+\gamma}\cdot 3^\gamma \cdot 5^\beta) =$$

$$= 2^{2\alpha+\gamma-1}\cdot 1 \cdot 3^{\gamma-1}\cdot 2 \cdot 5^{\beta-1}\cdot 4 = 2^{2\alpha+\gamma+2}\cdot 3^{\gamma-1}\cdot 5^{\beta-1} =$$

$$= 5760 = 2^7 \cdot 3^2 \cdot 5$$

$$2\alpha+\gamma+2 = 7$$
$$\gamma - 1 = 2$$
$$\beta - 1 = 1$$

$$\gamma = 3$$
$$\beta = 2$$

$$2\alpha + 3 + 2 = 7 \Rightarrow \alpha = 1$$

$$\boxed{\alpha = 1,\ \beta = 2,\ \gamma = 3}$$

(b) $\varphi(n) = \frac{n}{3}$

$3\varphi(n) = n \Rightarrow 3|n \Rightarrow n = 3^\alpha \cdot k, \quad (k,3)=1$

$3\varphi(3^\alpha k) = 3^\alpha k$

$3\varphi(3^\alpha)\cdot\varphi(k) = 3^\alpha k$

$\cancel{3\cdot 3^{\alpha-1}}\cdot 2\cdot\varphi(k) = \cancel{3^\alpha}\cdot k$

$2\cdot\varphi(k) = k \Rightarrow 2|k \Rightarrow k = 2^\beta\cdot m; \quad (m;2)=1$

$2\cdot\varphi(2^\beta\cdot m) = 2^\beta\cdot m$

$\cancel{2\cdot 2^{\beta-1}}\cdot\varphi(m) = \cancel{2^\beta}\cdot m$

$\varphi(m) = m \Rightarrow m = 1 \Rightarrow \boxed{n = 3^\alpha\cdot 2^\beta}, \quad \alpha,\beta\in\mathbb{N}$

MI 14./15. 7.

(a) Svi Pitagorini trokuti sa stranicom duljine 20.

$d|20 \Rightarrow d = \{1, 2, 4, 5, 10, 20\}.$

stranice su oblika: $d(m^2-n^2),\ 2dmn,\ d(m^2+n^2)$

1° $d=1$

$m^2-n^2=20 \iff 20\not\equiv 2 \pmod 4$

$20\equiv 0\not\equiv 2 \pmod 4 \Rightarrow (m-n)(m+n) = 4\cdot 5 = 20\cdot 1 = 2\cdot 10$

$\begin{cases} m-n=4 \\ m+n=5 \end{cases} \vee \begin{cases} m-n=1 \\ m+n=20 \end{cases} \vee \begin{cases} m-n=2 \\ m+n=10 \end{cases}$

$\Rightarrow n=0.5,\ m=4.5 \Rightarrow\Leftarrow \notin\mathbb{N}$; $n=9.5,\ m=11.5 \notin\mathbb{N}$; $n=4,\ m=6,\ d=1 \Rightarrow \boxed{(20, 48, 52)}$

$m^2+n^2 = 20 = 2^2\cdot 5 \iff \begin{cases} 2\equiv 1 \pmod 4 \\ 5\equiv 1 \pmod 4 \end{cases}$

$2\not\equiv 1 \pmod 4 \Rightarrow m^2+n^2\neq 20.$

$2mn = 20 \Rightarrow mn = 10 = 2\cdot 5 = 1\cdot 10$

$\Rightarrow m=5,\ n=2,\ d=1 \Rightarrow \boxed{(21, 20, 29)}$

$\Rightarrow m=10,\ n=1,\ d=1 \Rightarrow \boxed{(99, 20, 101)}$

$\underline{2^\circ}$ $d=2$

$m^2-n^2=10 \Rightarrow (m-n)(m+n)=2\cdot 5=10\cdot 1$

$$\begin{array}{c} m-n=2 \\ m+n=5 \\ \hline n=1.5 \\ m=3.5 \\ \notin N \end{array} \qquad \begin{array}{c} m-n=1 \\ m+n=10 \\ \hline n=4.5 \\ m=5.5 \\ \notin N \end{array}$$

$2mn=10 \Rightarrow m\cdot n \equiv 5$ (X)

$$m^2+n^2=10=2\cdot 5 \Leftrightarrow \begin{cases} 2\equiv 1 \pmod 4 \\ 5\equiv 1 \pmod 4 \end{cases}$$

$2\equiv 1 \pmod 4 \Rightarrow m^2+n^2\neq 10$

$\underline{3^\circ}$ $d=4$

$m^2-n^2\equiv 5 \Leftrightarrow 5\not\equiv 2 \pmod 4$

$5\equiv 1\not\equiv 2 \pmod 4 \Rightarrow (m-n)(m+n)=1\cdot 5$

$$\begin{array}{c} m-n=1 \\ m+n=5 \\ \hline n=2 \\ m=3 \\ d=4 \end{array} \Rightarrow \boxed{(20,48,52)}$$

$2mn=5 \Rightarrow\Leftarrow$

$m^2+n^2=5 \Leftrightarrow 5\equiv 1 \pmod 4$

$5\equiv 1 \pmod 4 \Rightarrow m^2+n^2=5 \Rightarrow m=2,\ n=1,\ d=4$

$\Rightarrow \boxed{(12,16,20)}$

$\underline{4^\circ}$ $d=5$

$m^2-n^2=4 \Leftrightarrow 4\not\equiv 2 \pmod 4$

$4\equiv 0\not\equiv 2 \pmod 4 \Rightarrow (m-n)(m+n)=2\cdot 2=1\cdot 4$

$$\begin{array}{c} m-n=2 \\ m+n=2 \\ \hline n=0 \\ m=2 \\ \Rightarrow\Leftarrow \end{array} \qquad \begin{array}{c} m-n=1 \\ m+n=4 \\ \hline n=1.5 \\ m=2.5 \\ \notin N \end{array}$$

$2mn=4 \Rightarrow mn=2 \Rightarrow m=2,\ n=1,\ d=5 \Rightarrow \boxed{(15,20,25)}$

$m^2+n^2=4=2\cdot 2 \Leftrightarrow 2\equiv 1 \pmod 4$

$2\not\equiv 1 \pmod 4 \Rightarrow m^2+n^2\neq 4$

$\underline{5^\circ}$ $d=10$

$$m^2-n^2=2$$
$$2mn=2$$
$$m^2+n^2=2$$

STRANICE PITAGORINOG TROKUTA NE MOGU BITI DULJINE 1 ILI 2.

$\underline{6^\circ}$ $d=20$

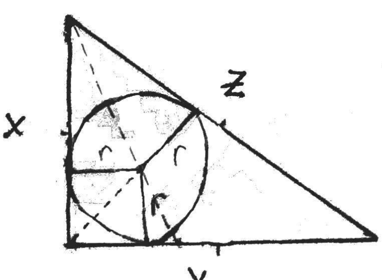
$$m^2-n^2=1$$
$$2mn=1$$
$$m^2+n^2=1$$

Rješenje:

(99, 20, 101) (21, 20, 29) (12, 16, 20) (20, 48, 52)

(15, 20, 25)

(b)



$$r=\frac{x+y-z}{2}=\frac{d(m^2-n^2)+2dmn-d(m^2+n^2)}{2}=$$

$$=\frac{\cancel{dm^2}-dn^2+2dmn-\cancel{dm^2}-dn^2}{2}=$$

$$=\frac{2dmn}{2}-\frac{2dn^2}{2}=dmn-dn^2\in\mathbb{N}$$

$$\boxed{r=\frac{x+y-z}{2}}$$

ZI 14./15. 1.

(a)

$$\frac{321}{777}$$

$777 = 321 \cdot 2 + 135$

$321 = 135 \cdot 2 + 51$

$135 = 51 \cdot 2 + 33$

$51 = 33 \cdot 1 + 18$

$33 = 18 \cdot 1 + 15$

$18 = 15 \cdot 1 + 3$

$15 = 3 \cdot 5$

$$\frac{321}{777} = [0; 2, 2, 2, 1, 1, 1, 5]$$

(b)

$\sqrt{146}$

$d = 146$

$a_0 = \lfloor \sqrt{d} \rfloor \qquad a_{i+1} = \left\lfloor \frac{a_0 + s_i}{t_i} \right\rfloor$

$s_{i+1} = t_i \cdot a_i - s_i \qquad s_0 = 0, \; s_1 = a_0$

$t_{i+1} = \frac{d - (s_{i+1})^2}{t_i} \qquad t_0 = 1$

	0	1	2	3
a_i	12	12	24	12
s_i	0	12	12	12
t_i	1	2	1	2

$\hookrightarrow \ldots$

$$\sqrt{146} = [12; \overline{12, 24}]$$

(c)

$$m \in \mathbb{N} : m < 100000$$

$$\frac{m^2 - 1}{146} = n^2, \quad n \in \mathbb{N}$$

$$m^2 - 146 n^2 = 1$$

$$l = 2$$

	-1	0	1	2	3	4	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~	~~11~~
a_n		12	12	24	12	24	~~12~~	~~24~~	~~12~~	~~24~~	~~12~~	~~24~~
p_n	1	12	145	3492	42049	177468						
q_n	0	1	12	289								

Za n pa ne treba računati.

l je paran pa je rješenje dano s: (p_{kl-1}, q_{kl-1})

Uvrštavamo $k = 1, 2, \ldots$

$$\Rightarrow \boxed{m = 145, 42049}$$

Tražene konvergente su (p_1, q_1) i (p_3, q_3).

$\boxed{\text{ZI } 14./15.\ 6.}$

RSA

$$(n,e) = (8549, 239) = (83\cdot 103, 239)$$

$$y = 1497$$

$$\varphi(n) = \varphi(8549) = \varphi(83\cdot 103) = 82\cdot 102 = 8364$$

$$e\cdot d \equiv 1 \pmod{\varphi(n)}$$

$$239\cdot d \equiv 1 \pmod{8364}$$

$$d = \frac{1+8364\cdot k}{239} = (k=1) = 35 \quad\Rightarrow\quad \boxed{d=35}$$

$$x = y^d \bmod n$$

$$y^d \equiv 1497^{35} \equiv 1497^{30}\cdot 1497\cdot 1171^2 \equiv 1497^{30}\cdot 4642 \equiv$$

$$\equiv (1497^5)^6\cdot 4642 \equiv 4642^6\cdot 4642 \equiv 4684^3\cdot 4642 \equiv$$

$$\equiv 4684\cdot 3122\cdot 4642 \equiv 4658\cdot 4642 \equiv 2015 \pmod{8549}$$

$$\Rightarrow \boxed{x = 2015}$$

ZI 14./15. 7.

Rabin

$(n,p,q) = (1829, 31, 59)$

$$31 \equiv 59 \equiv 3 \pmod 4$$

$y = 20$.

$$20^{\frac{31+1}{4}} \equiv 20^{8} \equiv 19 \pmod{31}$$

$$20^{\frac{59+1}{4}} \equiv 20^{15} \equiv 20 \cdot 46^{7} \equiv 20 \cdot 46 \cdot 51^{3} \equiv 20 \cdot 46 \cdot 19 \equiv 16 \pmod{59}$$

$$x \equiv \pm 19 \pmod{31} \qquad 31 \cdot 59 = 1829$$

$$x \equiv \pm 16 \pmod{59}$$

$$x \equiv \pm 19 \cdot 59 \cdot m \pm 16 \cdot 31 \cdot n \pmod{1829}$$

$$59m + 31n = 1$$

$59 = 31 \cdot 1 + 28$
$31 = 28 \cdot 1 + 3$
$28 = 3 \cdot 9 + \underline{1}$
$3 = 1 \cdot 3$

i	-1	0	1	2	3	
q_i			1	1	9	
m_i	1	0	1	-1	10	$\Rightarrow m = 10$
n_i	0	1	-1	2	-19	$\Rightarrow n = -19$

$$x \equiv \pm 19 \cdot 59 \cdot 10 \pm 16 \cdot 31 \cdot 19 \pmod{1829}$$

$$x \equiv \pm 11210 \pm 9424 \pmod{1829}$$

$$\boxed{x \equiv 515, 1786, 43, 1314 \pmod{1829}}$$

$\cancel{(515)_{10} = (\ldots 0011)_2}$
$\cancel{(1786)_{10} = (\ldots 1010)_2}$
$\cancel{(43)_{10} = (\ldots 1011)_2}$
$\cancel{(1314)_{10} = (\ldots 0010)_2}$

Otvoreni tekstovi: 43, 515, 1314, 1786.

$\boxed{\text{ZIR } 14./15.\ 2.}$

(b) Odredite preostale primitivne korjene modulo 43.

3 je najmanji primitivni korijen modulo 43, a ima $\varphi(43-1)=12$ primitivnih korjena modulo 43.

Ovo je iz $\boxed{\text{MI } 14./15.\ 3.}$.

Ostali primitivni korjeni su oblika $3^i \pmod{43} : (i,42)=1$.

$\varphi(42)=12$

reducirani sustav ostataka modulo 42:

$\{1,5,11,13,17,19,23,25,29,31,37,41\}$

$\Rightarrow 3^1, 3^5, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{25}, 3^{29}, 3^{31}, 3^{37}, 3^{41} \pmod{43}$

tj. $3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34$

$\boxed{\text{ZIR } 14./15.\ 3.}$

$$\left(\frac{1333}{1597}\right)=\underbrace{(-1)^{\frac{1596\cdot 1332}{4}}}_{=1}\left(\frac{1597}{1333}\right)=\left(\frac{264}{1333}\right)=\left[\left(\frac{2}{1333}\right)\right]^3\cdot\left(\frac{33}{333}\right)=$$

$$=\left((-1)^{\frac{1333^2-1}{8}}\right)^3\cdot\left(\frac{33}{333}\right)=(-1)\cdot\underbrace{(-1)^{\frac{332\cdot 32}{4}}}_{=1}\cdot\left(\frac{333}{33}\right)=$$

$$=-1\left(\frac{3}{33}\right)=-1\cdot(-1)^{\frac{32\cdot 2}{4}}\cdot\left(\frac{33}{3}\right)=0$$

ZIR 14./15. 3.

(a)
$$\left(\frac{1333}{1597}\right) = \left(\frac{31}{1597}\right)\cdot\left(\frac{43}{1597}\right) = (-1)^{\frac{30\cdot 1596}{4}}\left(\frac{1597}{31}\right)\cdot(-1)^{\frac{42\cdot 1596}{4}}\left(\frac{1597}{43}\right) =$$

$$= \left(\frac{1597}{31}\right)\cdot\left(\frac{1597}{43}\right) = \left(\frac{16}{31}\right)\cdot\left(\frac{6}{43}\right) = \left(\frac{2^4}{31}\right)\cdot\left(\frac{2}{43}\right)\cdot\left(\frac{3}{43}\right) =$$

$$\left(\frac{2^4}{31}\right) = 1$$

$$= \underbrace{(-1)^{\frac{43^2-1}{8}}}_{=-1} \cdot \underbrace{(-1)^{\frac{42\cdot 2}{4}}}_{=-1} \cdot \left(\frac{43}{3}\right) = \left(\frac{1}{3}\right) = 1$$

(b)
$$\left(\frac{99}{101}\right) = \underbrace{\left(\frac{3}{101}\right)\cdot\left(\frac{3}{101}\right)}_{1}\cdot\left(\frac{11}{101}\right) = (-1)^{\frac{100\cdot 10}{4}}\cdot\left(\frac{101}{11}\right) =$$

$$= \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1$$

$\Rightarrow$ 99 je kvadratni neostatak modulo 101 i iz tog slijedi da zadana kongruencija nema rješenja.

ZIR 14./15. 4.

(a) Ostatak pri dijeljenju broja 314^{162} s brojem 165.

$(314, 165) = (2\cdot 157, 3\cdot 5\cdot 11) = 1$

$\Rightarrow$ Euler: $314^{\varphi(165)} \equiv 1 \pmod{165}$

$\varphi(165) = \varphi(3\cdot 5\cdot 11) = 2\cdot 4\cdot 10 = 80.$

$\Rightarrow 314^{80} \equiv 1 \pmod{165}$

$314^{162} \equiv (314^{80})^2 \cdot 314^2 \equiv 314^2 \equiv 149^2 \equiv 91 \pmod{165}.$

Ostatak : $\underline{\underline{91}}$.

(b)

Dokažite da je $\varphi(9n) = \begin{cases} 9\varphi(n), & 3 \mid n \\ 6\varphi(n), & 3 \nmid n \end{cases}$

$3 \mid n \Rightarrow n = 3^{\alpha} \cdot m, \quad (m, 3) = 1$

$$\frac{\varphi(n)}{\varphi(9n)} = \frac{\varphi(3^{\alpha} \cdot m)}{\varphi(3^2 \cdot 3^{\alpha} \cdot m)} = \frac{\varphi(3^{\alpha}) \cdot \varphi(m)}{\varphi(3^{\alpha+2}) \cdot \varphi(m)} = \frac{3^{\alpha-1} \cdot \cancel{2}}{3^{\alpha+1} \cdot \cancel{2}} =$$

$$= \frac{\frac{\cancel{3^{\alpha}}}{3}}{\cancel{3^{\alpha}} \cdot 3} = \frac{1}{9} \Rightarrow \varphi(9n) = 9 \cdot \varphi(n)$$

$3 \nmid n \Rightarrow (n, 3) = 1$

$$\varphi(9n) = \varphi(3^2 \cdot n) = \varphi(3^2) \cdot \varphi(n) = 3 \cdot 2 \cdot \varphi(n) = 6\varphi(n)$$

$\boxed{\text{ZIR 14./15. 5.}}$

Pitagorini trokuti sa stranicom duljine 148.

Stranice su oblika: $d(m^2 - n^2)$, $2dmn$, $d(m^2 + n^2)$

$d \mid 148 \Rightarrow d = \{1, 2, 4, 37, 74, 148\}$ $\quad 148 = 2^2 \cdot 37$

$\underline{d = 1}$ $\quad m^2 - n^2 = 148$, $\quad 148 \equiv 0 \not\equiv 2 \pmod 4$ $\quad m^2 - n^2$ mora biti neparan broj

$2mn = 148 \Rightarrow mn = 74 = 2 \cdot 37 = 74 \cdot 1$

$\Rightarrow m = 37, n = 2, d = 1 \Rightarrow \boxed{(1365, 148, 1373)}$

$m = 74, n = 1, d = 1 \Rightarrow \boxed{(5475, 148, 5477)}$

$m^2 + n^2 = 148$, $\quad 2 \not\equiv 1 \pmod 4$

$\underline{d = 2}$

$74 \equiv 2 \pmod 4 \Rightarrow m^2 - n^2 \neq 74$ ~~$\Rightarrow (m-n)(m+n) = 74 \cdot 1 \neq 2 \cdot 37$~~

~~$m - n = 1$~~

~~$m + n = 74$~~

~~$n =$~~

$2mn = 74 \Rightarrow mn = 37$

$2 \not\equiv 1 \pmod 4 \Rightarrow m^2 + n^2 \neq 74$.

$37 \equiv 1 \pmod 4$

$\underline{d=4}$

$m^2-n^2=37$

$37 \equiv 1 \not\equiv 2 \pmod 4 \Rightarrow m^2-n^2=(m-n)(m+n)=37\cdot 1$

$m-n=1$
$m+n=37$

$n=18$
$m=19$
$d=4$
$\Rightarrow \boxed{(148, 2736, 2740)}$

$2mn=37 \Rightarrow\Leftarrow$

$m^2+n^2=37$

$37 \equiv 1 \pmod 4 \Rightarrow m=6,\ n=1,\ d=4$

$\Rightarrow \boxed{(140, 48, 148)}$

$\underline{d=37}$

$m^2-n^2=4 \Rightarrow\Leftarrow$

$2mn=4 \Rightarrow mn=2 \Rightarrow m=2, n=1, d=37$

$\Rightarrow \boxed{(111, 148, 185)}$

$m^2+n^2=4$

$4 \equiv 0 \not\equiv 1 \pmod 4 \Rightarrow m^2+n^2 \neq 4$

$\underline{d=74 \text{ i } d=148}$

$\Rightarrow\Leftarrow$

$\boxed{\text{ZIR 14./15. 9.}}$

RSA

$(n, e) = (51809, 6607)$

$n = p \cdot q$

$\sigma(n) = 52416$

$\cancel{p + q = 52416}$

$$\sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$$

$$\sigma(n) = \sigma(p \cdot q) = \frac{p^2 - 1}{p - 1} \cdot \frac{q^2 - 1}{q - 1} = \frac{\cancel{(p-1)}(p+1)}{\cancel{p-1}} \cdot \frac{\cancel{(q-1)}(q+1)}{\cancel{q-1}}$$

$$= (p+1)(q+1) = pq + p + q + 1 = 1 + p + q + n$$

$$\sigma(n) = 1 + p + q + n = 52416 \Rightarrow p + q = 52416 - n - 1 = 606$$

$p \cdot q = 51809$

$p + q = 606$

$$\Rightarrow x^2 - 606x + 51809 = 0$$

$$x_{1,2} = 503, 103$$

$$\Rightarrow p = 503, \ q = 103$$

$\varphi(n) = (p-1)(q-1) = 51204$

$e \cdot d \equiv 1 \pmod{\varphi(n)}$

$6607 d \equiv 1 \pmod{51204}$

$$d = \frac{1 + 51204k}{6607} = (k = 4) = 31 \qquad \boxed{d = 31}$$

MI 13./14. 1.

(a) $a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

$ac \equiv bd \pmod{m}$

$\cancel{ac - bd = m \cdot k}$

$a - b = m \cdot k$

$c - d = m \cdot l$

$ac - bd = a(c-d) + d(a-b) = a \cdot ml + d \cdot mk =$

$= m(al + dk) = m \cdot i \Rightarrow ac \equiv bd \pmod{m}$

(b) $2013 \equiv 213 \pmod{m}$

$\Rightarrow m \mid 2013 - 213 = 1800$

$\boxed{\tau(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \prod_{i=1}^{k} (\alpha_i + 1)}$ Broj djelitelja broja n

$\tau(1800) = \tau(2^3 \cdot 3^2 \cdot 5^2) = (3+1)(2+1)(2+1) =$

$= 4 \cdot 3 \cdot 3 = 36$

Postoji 36 takvih brojeva.

MI 13./14. 2.

$x \equiv -13 \pmod{70}$ $\quad$ $x \equiv 77 \pmod{80}$ $\quad$ $x \equiv 57 \pmod{75}$

$x \equiv -13 \pmod{7}$ $\quad$ $x \equiv 77 \pmod{5}$ $\quad$ $x \equiv 57 \pmod{3}$

$x \equiv -13 \pmod{10}$ $\quad$ $x \equiv 77 \pmod{16}$ $\quad$ $x \equiv 57 \pmod{25}$

$x \equiv 1 \pmod{7}$ $\quad$ $x \equiv 2 \pmod{5}$ $\quad$ $x \equiv 0 \pmod{3}$

$x \equiv 3 \pmod{10}$ $\quad$ $x \equiv 13 \pmod{16}$ $\quad$ $x \equiv 7 \pmod{25}$

MI 13./14. 2.

$x \equiv -13 \pmod{70}$ $\quad$ $x \equiv 77 \pmod{260}$ $\quad$ $x \equiv 57 \pmod{75}$

$70 = 7 \cdot 2 \cdot 5$ $\quad$ $260 = 4 \cdot 5 \cdot 13$ $\quad$ $75 = 3 \cdot 25$

$x \equiv -13 \pmod{7}$ $\quad$ $x \equiv 77 \pmod{4}$ $\quad$ $x \equiv 57 \pmod{3}$

$x \equiv -13 \pmod{2}$ $\quad$ $x \equiv 77 \pmod{5}$ $\quad$ $x \equiv 57 \pmod{25}$

$x \equiv -13 \pmod{5}$ $\quad$ $x \equiv 77 \pmod{13}$

$x \equiv 1 \pmod{7}$ $\quad$ $x \equiv 1 \pmod{4}$ $\quad$ $x \equiv 0 \pmod{3}$

$x \equiv 1 \pmod{2}$ $\quad$ $x \equiv 2 \pmod{5}$ $\quad$ $x \equiv 7 \pmod{25}$

$x \equiv 2 \pmod{5}$ $=$ $x \equiv 12 \pmod{13}$

$x \equiv 7 \pmod{25} \Rightarrow x \equiv 2 \pmod{5}$

$x \equiv 1 \pmod{4} \Rightarrow x \equiv 1 \pmod{2}$

Ekvivalentan sustav:

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 12 \pmod{13} \\ x &\equiv 7 \pmod{25} \end{aligned}$$

$3 \cdot 4 \cdot 7 \cdot 13 \cdot 25 = 27300$

$$x \equiv 4 \cdot 7 \cdot 13 \cdot 25 \cdot x_1 + 3 \cdot 7 \cdot 13 \cdot 25 \cdot x_2 + 3 \cdot 4 \cdot 13 \cdot 25 \cdot x_3 + 3 \cdot 4 \cdot 7 \cdot 25 \cdot x_4 + 3 \cdot 4 \cdot 7 \cdot 13 \cdot x_5 \pmod{27300}$$

$$x \equiv 9100x_1 + 6825x_2 + 3900x_3 + 2100x_4 + 1092x_5 \pmod{27300}$$

$9100x_1 \equiv 0 \pmod 3 \Rightarrow x_1 \equiv 0 \pmod 3 \Rightarrow x_1 = 0$

$6825x_2 \equiv 1 \pmod 4 \Rightarrow x_2 \equiv 1 \pmod 4 \Rightarrow x_2 = 1$

$3900x_3 \equiv 1 \pmod 7 \Rightarrow x_3 \equiv 1 \pmod 7 \Rightarrow x_3 = 1$

$2100x_4 \equiv 12 \pmod{13} \Rightarrow 7x_4 \equiv 12 \pmod{13} \Rightarrow x_4 = 11$

$1092x_5 \equiv 7 \pmod{25} \Rightarrow 17x_5 \equiv 7 \pmod{25} \Rightarrow x_5 = 21$

$x \equiv 9100 \cdot 0 + 6825 \cdot 1 + 3900 \cdot 1 + 2100 \cdot 11 + 1092 \cdot 21 \pmod{27300}$

$x \equiv 56757 \pmod{27300}$

$\boxed{x \equiv 2157 \pmod{27300}}$

MI 13./14. 3.

(a) Koliko ima primitivnih korijena modulo 43?

Ima ih $\varphi(43-1) = \varphi(42) = \varphi(2 \cdot 3 \cdot 7) = 1 \cdot 2 \cdot 6 = 12$.

Odredite najmanji među njima.

Prosti broj g je primitivan korijen modulo p akko za svaki prosti faktor q od $p-1$ vrijedi:

$$g^{\frac{p-1}{q}} \not\equiv 1 \pmod p$$

$43-1=42=2 \cdot 3 \cdot 7$

$g=2$

$2^{\frac{42}{2}} \equiv 2^{21} \equiv 42 \pmod{43}$

$2^{\frac{42}{3}} \equiv 2^{14} \equiv 1 \pmod{43}$

$\Rightarrow$ 2 nije!

$g=3$

$3^{\frac{42}{2}} \equiv 3^{21} \equiv 37^3 \equiv 42 \pmod{43}$

$3^{\frac{42}{3}} \equiv 3^{14} \equiv 36 \pmod{43}$

$3^{\frac{42}{7}} \equiv 3^6 \equiv 41 \pmod{43}$

$\Rightarrow$ 3 je najmanji primitivni korijen modulo 43.

(b)

$$28x^{33} \equiv 30 \pmod{43}$$

$$\mathrm{ind}_3(28\cdot x^{33}) \equiv \mathrm{ind}_3 30 \pmod{42}$$

$$\mathrm{ind}_3 28 + \mathrm{ind}_3 x^{33} \equiv \mathrm{ind}_3 30 \pmod{42}$$

$$\mathrm{ind}_3 28 + 33\cdot \mathrm{ind}_3 x \equiv \mathrm{ind}_3 30 \pmod{42}$$

$$3^l \equiv 28 \pmod{43}$$

$$l = 0, 1, \ldots, \underbrace{\varphi(43)-1}_{=41}$$

$$\Rightarrow l = 5$$

$$3^l \equiv 30 \pmod{43}$$

$$l = 0, 1, \ldots, \varphi(43)-1$$

$$\Rightarrow l = 11$$

$$5 + 33\cdot \mathrm{ind}_3 x \equiv 11 \pmod{42}$$

$$33\cdot \mathrm{ind}_3 x \equiv 6 \pmod{42}$$

$(33, 42) = 3 \Rightarrow 3$ rješenja

$$11\,\mathrm{ind}_3 x \equiv 2 \pmod{14}$$

$$\mathrm{ind}_3 x \equiv 4 \pmod{14}$$

$$\mathrm{ind}_3 x \equiv 4, 18, 32 \pmod{42}$$

$$\Rightarrow x \equiv 3^4, 3^{18}, 3^{32} \pmod{43}$$

$$\boxed{x \equiv 38, 35, 13 \pmod{43}}$$

$\boxed{\text{MI 13./14. 4.}}$

(a) $\varphi(n) = 98$

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_k - 1)$$

$$p_i - 1 \mid 98 \implies p_i \in \{2, 3, \cancel{8}, \cancel{15}, \cancel{50}, \cancel{99}\}$$

$98 = 2 \cdot 7^2$ $\qquad$ nisu prosti

$\underline{1^\circ}$ $n = 2^\alpha \implies \varphi(2^\alpha) = 2^{\alpha-1} \cdot 1 = 2 \cdot 7^2 \implies \Leftarrow$

$\underline{2^\circ}$ $n = 3^\beta \implies \varphi(3^\beta) = 3^{\beta-1} \cdot 2 = 2 \cdot 7^2 \implies \Leftarrow$

$\underline{3^\circ}$ $n = 2^\alpha 3^\beta \implies \varphi(2^\alpha 3^\beta) = 2^{\alpha-1} \cdot 3^{\beta-1} \cdot 2 = 2 \cdot 7^2 \implies \Leftarrow$

$\boxed{\text{MI 13./14. 5.}}$

(a) $$\left(\frac{-24}{437}\right) = \left(\frac{-1}{437}\right)\left(\frac{2^3}{437}\right)\left(\frac{3}{437}\right) = \underbrace{(-1)^{\frac{437-1}{2}}}_{=1} \cdot \left(\frac{2^3}{437}\right) \cdot \left(\frac{3}{437}\right) =$$

$$= \underbrace{(-1)^{\frac{437^2-1}{8}}}_{=-1}\left(\frac{3}{437}\right) = -1 \cdot \underbrace{(-1)^{\frac{436 \cdot 2}{4}}}_{=1}\left(\frac{437}{3}\right) =$$

$$= -1 \cdot \left(\frac{2}{3}\right) = (-1) \cdot (-1)^{\frac{3^2-1}{8}} = 1$$

MI 13./14. 6.

Svi Pitagorini trokuti kojima je jedna stranica duljine 68.

Stranice su oblika: $d(m^2-n^2)$, $2dmn$, $d(m^2+n^2)$

$d|68 \Rightarrow d = \{1, 2, 4, 17, 34, 68\}$ $\quad 68 = 2\cdot 2\cdot 17$

<u>d=1</u>

$m^2-n^2 = 68 \Rightarrow\Leftarrow$ m^2-n^2 mora biti neparan broj

$2mn = 68 \Rightarrow mn = 34 = 2\cdot 17 = 34\cdot 1$

$\Rightarrow m = 17, n = 2, d = 1 \Rightarrow \boxed{(285, 68, 293)}$

$\Rightarrow m = 34, n = 1, d = 1 \Rightarrow \boxed{(1155, 68, 1157)}$

$m^2+n^2 = 68 = 2\cdot 2\cdot 17$

Mora vrijediti: $2 \equiv 1 \pmod 4 \wedge 17 \equiv 1 \pmod 4$

Međutim $2 \not\equiv 1 \pmod 4 \Rightarrow m^2+n^2 \neq 68$.

<u>d=2</u>

$2mn = 34 \Rightarrow mn = 17 \Rightarrow\Leftarrow$ m i n moraju biti različitih parnosti.

$m^2-n^2 = 34 \Rightarrow\Leftarrow$

$m^2+n^2 = 34 = 2\cdot 17 \Rightarrow\Leftarrow$

<u>d=4</u>

$m^2-n^2 = 17 \Rightarrow (m-n)(m+n) = 17 \Rightarrow$ $m-n=1$, $m+n=17$

$n=8$, $m=9$, $d=4$ $\Rightarrow \boxed{(68, 576, 580)}$

$2mn = 17 \Rightarrow\Leftarrow$

$m^2+n^2 = 17 \Rightarrow m=4, n=1, d=4 \Rightarrow \boxed{(60, 32, 68)}$

<u>d=17</u>

$m^2-n^2 = 4 \Rightarrow\Leftarrow$

$2mn = 4 \Rightarrow mn = 2 \Rightarrow m=2, n=1, d=17 \Rightarrow \boxed{(51, 68, 85)}$

$m^2+n^2 = 4 \Rightarrow\Leftarrow$

<u>d=34</u> $\Rightarrow\Leftarrow$

<u>d=68</u> $\Rightarrow\Leftarrow$

Eulerov teorem:

$$(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

Mali Fermatov teorem:

$$p \nmid a,\ p \text{ prost} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$\forall a \in \mathbb{Z} \quad a^p \equiv a \pmod{p}$$
