1. Odredite $g = \text{nzd}(a, b)$ i nađite cijele brojeve x, y takve da je $ax + by = g$ ako je

   a) $a = 777, \quad b = 629$;
   b) $a = 1643, \quad b = 901$;
   c) $a = 1105, \quad b = 481$.

2. Odredite s koliko nula završavaju brojevi 713! i 1713! .

3. Riješite kongruenciju:

   a) $311x \equiv 7 \pmod{401}$;
   b) $153x \equiv 71 \pmod{391}$;
   c) $213x \equiv 75 \pmod{333}$.

4. Riješite sustav kongruencija:

   a) $x \equiv 1 \pmod{5}, \ x \equiv 2 \pmod{6}, \ x \equiv 3 \pmod{7}$;
   b) $x \equiv 5 \pmod{7}, \ x \equiv 9 \pmod{13}, \ x \equiv 8 \pmod{11}$;
   c) $x \equiv 1 \pmod{4}, \ x \equiv 7 \pmod{9}, \ x \equiv 22 \pmod{25}$.

5. Nađite sva rješenja jednadžbe $\varphi(n) = 30$.

6. Nađite sva rješenja jednadžbe $\varphi(n) = 58$.

7. a) Nađite najmanji primitivni korijen modulo 61.
   b) Riješite (pomoću indeksa) kongruenciju: $x^7 \equiv 24 \pmod{61}$.

8. a) Nađite najmanji primitivni korijen modulo 67.
   b) Riješite (pomoću indeksa) kongruenciju: $x^5 \equiv 61 \pmod{67}$.

9. Izračunajte Legendreove simbole:

   a) $(\frac{51}{97})$;
   b) $(\frac{321}{901})$;
   c) $(\frac{-31}{101})$;
   d) $(\frac{58}{269})$.

10. Odredite sve proste brojeve p takve da je $\left(\frac{6}{p}\right) = 1$.

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

1. $g = nzd(a,b)$, $ax + by = g$, $x, y = ?$

a) $nzd(777, 629) = 37$

$777 = 629 \cdot 1 + 148$
$629 = 148 \cdot 4 + 37$
$148 = 37 \cdot 4$

i	-1	0	1	2
q_i			1	4
x_i	1	0	1	-4
y_i	0	1	-1	5

$777 \cdot (-4) + 629 \cdot 5 = 37$

b) $nzd(1643, 901) = 53$

$1643 = 901 \cdot 1 + 742$
$901 = 742 \cdot 1 + 159$
$742 = 159 \cdot 4 + 106$
$159 = 106 \cdot 1 + 53$
$106 = 53 \cdot 2$

i	-1	0	1	2	3	4
q_i			1	1	4	1
x_i	1	0	1	-1	5	-6
y_i	0	1	-1	2	-9	11

$1643 \cdot (-6) + 901 \cdot 11 = 53$

c) $nzd(1105, 481) = 13$

$1105 = 481 \cdot 2 + 143$
$481 = 143 \cdot 3 + 52$
$143 = 52 \cdot 2 + 39$
$52 = 39 \cdot 1 + 13$
$39 = 13 \cdot 3$

i	-1	0	1	2	3	4
q_i			2	3	2	1
x_i	1	0	1	-3	7	-10
y_i	0	1	-2	7	-16	23

$1105 \cdot (-10) + 481 \cdot 23 = 13$

1zad

② 713!

$10 = 2\cdot 5 \quad 5>2$

$$\left\lfloor\frac{713}{5}\right\rfloor+\left\lfloor\frac{713}{25}\right\rfloor+\left\lfloor\frac{713}{125}\right\rfloor+\left\lfloor\frac{713}{625}\right\rfloor = 142+28+5+1 = \underline{\underline{176}}$$

1713!

$$\left\lfloor\frac{1713}{5}\right\rfloor+\left\lfloor\frac{1713}{25}\right\rfloor+\left\lfloor\frac{1713}{125}\right\rfloor+\left\lfloor\frac{1713}{625}\right\rfloor = 342+68+13+2 = \underline{\underline{425}}$$

③ a) $311x \equiv 7 \pmod{401}$

$401 = 311\cdot 1 + 90$
$311 = 90\cdot 3 + 41$
$90 = 41\cdot 2 + 8$
$41 = 8\cdot 5 + 1$
$8 = 1\cdot 8$
$1 | 7$

i	-1	0	1	2	3	4
q_i			1	3	2	5
y_i	0	1	-1	4	-9	49

$311u \equiv 1 \pmod{401}$
$u \equiv 49 \pmod{401}$
$\Rightarrow x \equiv 49\cdot 7 \pmod{401}$
$\underline{x \equiv 343 \pmod{401}}$

b) $153x \equiv 71 \pmod{391}$

$391 = 153\cdot 2 + 85$
$153 = 85\cdot 1 + 68$ $\Rightarrow 17 \nmid 71 \Rightarrow$ nema rješenja
$85 = 68\cdot 1 + 17$
$68 = 17\cdot 4$

c) $213x \equiv 75 \pmod{333}$

nzd$(333,213) = 3$, $3|75$
$\Rightarrow 71x \equiv 25 \pmod{111}$

$111 = 71\cdot 1 + 40$
$71 = 40\cdot 1 + 31$
$40 = 31\cdot 1 + 9$
$31 = 9\cdot 3 + 4$
$9 = 4\cdot 2 + 1$
$4 = 1\cdot 4$

i	-1	0	1	2	3	4	5
q_i			1	1	1	3	2
y_i	0	1	-1	2	-3	11	-25

$213u \equiv 1 \pmod{111}$
$u \equiv -25 \pmod{111}$
$u \equiv 86 \pmod{111}$
$\Rightarrow x \equiv 25\cdot 86 \pmod{111}$
$x \equiv 2150 \pmod{111}$
$x \equiv 41 \pmod{111} \Rightarrow \underline{x \equiv 41, 152, 263 \pmod{333}}$

2+3zad

4\. a) $x \equiv 1 \pmod 5$ $\quad x \equiv 2 \pmod 6$ $\quad x \equiv 3 \pmod 7$

$x_0 = 42x_1 + 35x_2 + 30x_3$

$42x_1 \equiv 1 \pmod 5$ $\quad 35x_2 \equiv 2 \pmod 6$ $\quad 30x_3 \equiv 3 \pmod 7$

$2x_1 \equiv 1 \pmod 5$ $\quad 5x_2 \equiv 2 \pmod 6$ $\quad 2x_3 \equiv 3 \pmod 7$

$\Downarrow \quad \Downarrow \quad \Downarrow$

$x_1 = 3$ $\quad x_2 = 4$ $\quad x_3 = 5$

$x_0 = 42 \cdot 3 + 35 \cdot 4 + 30 \cdot 5$

$x_0 = 416 \Rightarrow x \equiv 416 \pmod{210}$

$\underline{x \equiv 206 \pmod{210}}$

b) $x \equiv 5 \pmod 7$ $\quad x \equiv 9 \pmod{13}$ $\quad x \equiv 8 \pmod{11}$

$x_0 = 143x_1 + 77x_2 + 91x_3$

$143x_1 \equiv 5 \pmod 7$ $\quad 77x_2 \equiv 9 \pmod{13}$ $\quad 91x_3 \equiv 8 \pmod{11}$

$3x_1 \equiv 5 \pmod 7$ $\quad 12x_2 \equiv 9 \pmod{13}$ $\quad 3x_3 \equiv 8 \pmod{11}$

$\Downarrow \quad \Downarrow \quad \Downarrow$

$x_1 = 4$ $\quad x_2 = 4$ $\quad x_3 = 10$

$x_0 = 143 \cdot 4 + 77 \cdot 4 + 91 \cdot 10 = 1790$

$x \equiv 1790 \pmod{1001} \Rightarrow \underline{x \equiv 789 \pmod{1001}}$

c) $x \equiv 1 \pmod 4$ $\quad x \equiv 7 \pmod 9$ $\quad x \equiv 22 \pmod{25}$

$x_0 = 225x_1 + 100x_2 + 36x_3$

$225x_1 \equiv 1 \pmod 4$ $\quad 100x_2 \equiv 7 \pmod 9$ $\quad 36x_3 \equiv 22 \pmod{25}$

$x_1 \equiv 1 \pmod 4$ $\quad x_2 \equiv 7 \pmod 9$ $\quad 11x_3 \equiv 22 \pmod{25}$

$\Downarrow \quad \Downarrow \quad \Downarrow$

$x_1 = 1$ $\quad x_2 = 7$ $\quad x_3 = 2$

$x_0 = 225 \cdot 1 + 100 \cdot 7 + 36 \cdot 2 = 997$

$x \equiv 997 \pmod{900}$

$\underline{x \equiv 97 \pmod{900}}$

5. $\varphi(n) = 30 \quad = 5 \cdot 3 \cdot 2$ *

$1, 2, 3, 5, 6, 10, 15, 30 \mid 30 \qquad \varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$

$p \in \{2, 3, 7, 11, 31\}$

$n = 2^\alpha \cdot 3^\beta \cdot 7^\gamma \cdot 11^\delta \cdot 31^\varepsilon \quad , \gamma, \delta, \varepsilon \leq 1$

$\alpha, \beta \leq 2$ (zato što 2 i 3 dijele 30)

1.) $n = 31 \cdot k \Rightarrow \varphi(n) = 30 \cdot \varphi(k) = 30 \Rightarrow \varphi(k) = 1$

$\Rightarrow k = 1, 2 \Rightarrow \boxed{n = 31, 62}$

2.) $n = 11 \cdot k \Rightarrow \varphi(n) = 10 \cdot \varphi(k) = 30 \Rightarrow \varphi(k) = 3$ nema rj.

3.) $n = 7 \cdot k \Rightarrow \varphi(n) = 6 \cdot \varphi(k) = 30 \Rightarrow \varphi(k) = 5$ nema rj.

*) $n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$

$\Rightarrow \varphi(n) = 2^{\alpha-1} \cdot 1 \cdot 3^{\beta-1} \cdot 2 \cdot 5^{\gamma-1} \cdot 4 = 30$

$8 \cdot 2^{\alpha-1} \cdot 3^{\beta-1} \cdot 5^{\gamma-1} = 30$

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

$\alpha + 2 = 1$

$\beta - 1 = 1$

$\gamma - 1 = 1$

Postoje samo prva 3 slučaja. Ovaj označen zvjezdicom bi postojao jedino kada bi 5 bio u skupu p.

5zad

6. $f(n) = 58 = 2 \cdot 29$

$1, 2, 29, 58 \mid 58$

$p \in \{2, 3, 59\}$

$n = 2^{\alpha} \cdot 3^{\beta} \cdot 59^{\gamma}$ $\quad , \beta, \gamma \leq 1$

$\alpha \leq 2$

1.) $n = 59 \cdot k \Rightarrow f(n) = 58 \cdot f(k) = 58 \Rightarrow f(k) = 1$

$\Rightarrow k = 1, 2 \Rightarrow \boxed{n = 59, 118}$

2.) $n = 3 \cdot k \Rightarrow f(n) = 2 \cdot f(k) = 58 \Rightarrow f(k) = 29 \Rightarrow$ nema rj.

$$\boxed{n = 59, 118}$$

6zad

7\. a) $g^{(p-1)/q} \not\equiv 1 \pmod p$

$p = 61 \Rightarrow p-1 = 60 = 2^2 \cdot 3 \cdot 5$

$\Downarrow$

$q \in \{2, 3, 5\}$

$\Rightarrow g^{60/2} \not\equiv 1 \pmod{61} \Rightarrow g^{30} \not\equiv 1 \pmod{61}$

$g^{60/3} \not\equiv 1 \pmod{61} \Rightarrow g^{20} \not\equiv 1 \pmod{61}$

$g^{60/5} \not\equiv 1 \pmod{61} \Rightarrow g^{12} \not\equiv 1 \pmod{61}$

$g = 2, 3, 5, 6, 7, 10 \ldots$ (bez potencija prethodnih brojeva)

$\underline{\underline{2}}$

$2^{30} \not\equiv 1 \pmod{61} \Rightarrow 2^{30} \equiv 60 \not\equiv 1 \pmod{61}$ ✓

$2^{20} \not\equiv 1 \pmod{61} \Rightarrow 2^{20} \equiv 47 \not\equiv 1 \pmod{61}$ ✓

$2^{12} \not\equiv 1 \pmod{61} \Rightarrow 2^{12} \equiv 9 \not\equiv 1 \pmod{61}$ ✓

$\Rightarrow$ <u>2 je min prim korijen</u>

7azad

7\. b) $x^7 \equiv 24 \pmod{61}$

7.a) prim korijen od 61 je 2 $\Rightarrow$ smijemo indeksirat sa 2

$$ind_2 x^7 \equiv \underbrace{ind_2 24}\ (\text{mod } \varphi(61))$$

$ind_2 24 = ind_2(2^3 \cdot 3) = ind_2 2^3 + ind_2 3$? $\varphi(61)$

$\Rightarrow ind_2 2^3 = 3\, ind_2 2 = 3 \cdot 1 = 3 \pmod{61}$

$\Rightarrow ind_2 3 \pmod{61}$

$\hookrightarrow 2^y \equiv 3 \pmod{61} \Rightarrow y = 6 = ind_2 3 \pmod{61}$

$\Rightarrow ind_2 24 = 3 + 6 = 9$

$ind_2 x^7 \equiv 9\ (\text{mod } \varphi(61))$

$\hookrightarrow \varphi(61) = 60$

$$7\underbrace{ind_2 x}_{z} \equiv 9 \pmod{60}$$

$7z \equiv 9 \pmod{60}$

$60 = 7 \cdot 8 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3$

i	-1	0	1	2	3
q_i			8	1	1
y_i	0	1	-8	9	-17

$7u = 1 \pmod{60}$

$u = -17 \pmod{60}$

$u = 43 \pmod{60}$

$z = 9 \cdot 43 \pmod{60} = 387 \pmod{60}$

$z = 27 \pmod{60}$

$ind_2 x \equiv 27 \pmod{61}$?

$x \equiv 2^{27} \pmod{61}$

$$\boxed{x \equiv 38 \pmod{61}}$$

7bzad

8. a) $g^{(p-1)/q} \not\equiv 1 \pmod{p}$

$p = 67 \Rightarrow p-1 = 66 = 2 \cdot 3 \cdot 11$

$\Downarrow$

$q \in \{2, 3, 11\}$

$\Rightarrow g^{33} \not\equiv 1 \pmod{67}$

$g^{22} \not\equiv 1 \pmod{67}$

$g^{6} \not\equiv 1 \pmod{67}$

$\underline{2}$ $\quad 2^{33} \equiv 0 \pmod{67}$ ✓

$2^{22} \equiv 37 \pmod{67}$ ✓ $\Rightarrow$ 2 je min prim korijen

$2^{6} \equiv 64 \pmod{67}$ ✓

b) $x^5 \equiv 61 \pmod{67}$

$\operatorname{ind}_2 61 \overset{?}{(\bmod 67)}$

$\hookrightarrow 2^y = 61 \pmod{67} \Rightarrow y = 7$

$\operatorname{ind}_2 x^5 \equiv \operatorname{ind}_2 61 \pmod{\varphi(67)}$

$5 \underbrace{\operatorname{ind}_2 x}_{z} \equiv 7 \pmod{66}$

$66 = 5 \cdot 13 + 1$

$5 = 1 \cdot 5$

$5u \equiv 1 \pmod{66}$

i	-1	0	1
q_i			13
y_i	0	1	-13

$u \equiv -13 \pmod{66}$

$u \equiv 53 \pmod{66}$

$z \equiv 371 \pmod{66}$

$z \equiv 41 \pmod{66} \Rightarrow \operatorname{ind}_2 x \equiv 41 \overset{?}{(\bmod 67)}$

$x \equiv 2^{41} \pmod{67}$

$\boxed{x \equiv 12 \pmod{67}}$

8zad

9. a) $\left(\frac{51}{97}\right) = \left(\frac{97}{51}\right) \overset{\text{paran brojnik}}{=} \left(\frac{46}{51}\right) = \underbrace{\left(\frac{2}{51}\right)}_{-1}\left(\frac{23}{51}\right) = -\left(\frac{23}{51}\right) = -\left(-\frac{51}{23}\right)$

$51 \equiv 3 \pmod 4$, $97 \equiv 1 \pmod 4$

$= -\underbrace{\left(-\frac{1}{23}\right)}_{-1}\left(\frac{51}{23}\right) = \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$

b) $\left(\frac{321}{991}\right) = \left(\frac{991}{321}\right) = \left(\frac{28}{321}\right) = \underbrace{\left(\frac{2}{321}\right)}_{1}\underbrace{\left(\frac{2}{321}\right)}_{1}\left(\frac{7}{321}\right) = \left(\frac{321}{7}\right) = \left(\frac{6}{7}\right)$

$= \underbrace{\left(\frac{2}{7}\right)}_{1} \cdot \left(\frac{3}{7}\right) = \left(-\frac{7}{3}\right) = \underbrace{\left(-\frac{1}{3}\right)}_{-1} \cdot \left(\frac{7}{3}\right) = -\left(\frac{7}{3}\right) = -\underbrace{\left(\frac{1}{3}\right)}_{1} = -1$

c) $\left(-\frac{31}{101}\right) = \underbrace{\left(-\frac{1}{101}\right)}_{1}\left(\frac{31}{101}\right) = \left(\frac{31}{101}\right) = \left(\frac{101}{31}\right) = \left(\frac{8}{31}\right) = \underbrace{\left(\frac{2}{31}\right)}_{1}\left(\frac{2}{31}\right)\left(\frac{2}{31}\right)$

$= 1$

d) $\left(\frac{58}{269}\right) = \underbrace{\left(\frac{2}{269}\right)}_{-1}\left(\frac{29}{269}\right) = -\left(\frac{29}{269}\right) = -\left(\frac{269}{29}\right) = -\left(\frac{8}{29}\right) = -\underbrace{\left(\frac{2}{29}\right)}_{-1}\left(\frac{2}{29}\right)\left(\frac{2}{29}\right)$

$= 1$

9zad

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

tablica fi