# 1. DZ → zadaci

① $g = \text{ucd}(a,b)$ $\quad x, y ? \Rightarrow a \cdot x + b \cdot y = g$

a) $a = 2541$, $b = 1134$

$2541 = 1134 \cdot 2 + 273$
$1134 = 273 \cdot 4 + 42$
$273 = 42 \cdot 6 + \boxed{21}$
~~$42 = 21 \cdot 2$~~

| $i$ | -1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| $q_i$ | | | 2 | 4 | 6 |
| $x_i$ | 1 | 0 | 1 | -4 | $\boxed{25}$ |
| $y_i$ | 0 | 1 | -2 | 9 | $\boxed{-56}$ |

$2541 \cdot 25 - 1134 \cdot 56 = 21$ ✓

b) $a = 4379$, $b = 3306$

$4379 = 3306 \cdot 1 + 1073$
$3306 = 1073 \cdot 3 + 87$
$1073 = 87 \cdot 12 + \boxed{29}$
~~$87 = 29 \cdot 3$~~

| $i$ | -1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| $q_i$ | | | 1 | 3 | 12 |
| $x_i$ | 1 | 0 | 1 | -3 | +37 |
| $y_i$ | 0 | 1 | -1 | 4 | -49 |

$4379 \cdot 37 - 3306 \cdot 49 = 29$ ✓

② a) $314m + 159n = 1$

$314 = 159 \cdot 1 + 155$
$159 = 155 \cdot 1 + 4$
$155 = 4 \cdot 38 + 3$
$4 = 3 \cdot 1 + \boxed{1}$
~~$3 = 1 \cdot 3$~~

| $i$ | -1 | 0 | 1 | 2 | 3 | 4 | |
|---|---|---|---|---|---|---|---|
| $q_i$ | | | 1 | 1 | 38 | 1 | |
| $m_i$ | 1 | 0 | 1 | -1 | 39 | $\boxed{-40}$ | $\rightarrow m$ |
| $n_i$ | 0 | 1 | -1 | 2 | -77 | $\boxed{79}$ | $\rightarrow n$ |

b) $1245m - 1603n = 1$

$1603 = 1245 \cdot 1 + 358$
$1245 = 358 \cdot 3 + 171$
$358 = 171 \cdot 2 + 16$
$171 = 16 \cdot 10 + 11$
$16 = 11 \cdot 1 + 5$
$11 = 5 \cdot 2 + \boxed{1}$
~~$5 = 1 \cdot 5$~~

| $i$ | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|
| $q_i$ | | | 1 | 3 | 2 | 10 | 1 | 2 |
| $m_i$ | 1 | 0 | 1 | -3 | 7 | -73 | 80 | -233 |
| $n_i$ | 0 | 1 | -1 | 4 | -9 | 94 | -103 | 300 |

✗

③ a) $654m + 822n = -12$

$822 = 654 \cdot 1 + 168$
$654 = 168 \cdot 3 + 150$
$168 = 150 \cdot 1 + 18$
$150 = 18 \cdot 8 + \boxed{6}$
~~$18 = 6 \cdot 3$~~

| $i$ | -1 | 0 | 1 | 2 | 3 | 4 | |
|---|---|---|---|---|---|---|---|
| $q_i$ | | | 1 | 3 | 1 | 8 | |
| $m_i$ | 1 | 0 | 1 | -3 | 4 | $\boxed{-35}$ | $\cdot (-2) = 70$ |
| $n_i$ | 0 | 1 | -1 | 4 | -5 | $\boxed{44}$ | $\cdot (-2) = -88$ |

✓

1DZ-1

⑪ a) nula? $2013!$

$2013! = 2^{\alpha(2)} \cdot 3^{\alpha(3)} \cdot 5^{\alpha(5)} \cdot \dots$

$\alpha(2) = \left\lfloor \frac{2013}{2} \right\rfloor + \left\lfloor \frac{2013}{2^2} \right\rfloor + \left\lfloor \frac{2013}{2^3} \right\rfloor + \dots = \text{veće}$

$\alpha(5) = \left\lfloor \frac{2013}{5} \right\rfloor + \left\lfloor \frac{2013}{25} \right\rfloor + \left\lfloor \frac{2013}{125} \right\rfloor + \left\lfloor \frac{2013}{625} \right\rfloor = \boxed{501}$

(402, 80, 16, 3)

} manji od ta dva

b) $\binom{4321}{1234}$, nula? $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{4321!}{1234!\,(3087)!} = \frac{\alpha_1(5)}{\alpha_2(5) \cdot \alpha_3(5)}$

$= \alpha_1(5) - \alpha_2(5) - \alpha_3(5)$

$= 864 + 172 + 34 + 6 + 1 - (246 + 49 + 9 + 1 + 617 + 123 + 24 + 4)$

$= 4$

⑫ a) $49 \mid \underbrace{\binom{2013}{35}}$ $\rightarrow \frac{2013!}{35!\,1978!} = \alpha_1(7) - \alpha_2(7) - \alpha(7)$

$\alpha_1(7) = \left\lfloor \frac{2013}{7} \right\rfloor + \left\lfloor \frac{2013}{49} \right\rfloor + \left\lfloor \frac{2013}{343} \right\rfloor = 287 + 41 + 5 = 333$

$\alpha_2(7) = 5$

$\alpha_3(7) = 282 + 40 + 5 = 327$

} $\Rightarrow 49 \nmid \binom{2013}{35}$

b) $\frac{2013!}{35^n} \Rightarrow n = ?$ da je prirodan broj

$\alpha(7) = 333$, $\alpha(5) = 501$ $\Rightarrow \frac{2^{\alpha(2)} \cdot 3^{\alpha(3)} \cdot 5^{\alpha(5)} \cdot 7^{\alpha(7)} \dots}{7^n \cdot 5^n}$ $\quad n \in \{1, \dots, 333\}$

# 2. DZ → zadaci

⑤ a) $175x \equiv 252 \pmod{294}$

1) $294 = 1 \cdot 175 + 119$
$175 = 1 \cdot 119 + 56$
$119 = 2 \cdot 56 + \boxed{7}$
$56 = 8 \cdot 7$

2) $\frac{175}{7}x \equiv \frac{252}{7} \pmod{\frac{294}{7}}$

$25x \equiv 36 \pmod{42}$

3)

| i | -1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| q | | | 1 | 1 | 2 |
| y-u | 0 | 1 | -1 | 2 | $\boxed{-5}$ |

4) $25(-5) = 1 \pmod{42} \quad / \cdot 36$

$25(-5 \cdot 36) = 36 \pmod{42}$

5) $x \equiv -180 \pmod{42}$ (!)

6) $x \equiv -12 \pmod{42}$ / da se rješim −

7) $x \equiv 30 \pmod{42}$

42 − 12

8) $x \equiv 30 + k \cdot 42, \quad k \in [0, 7-1]$

$x \equiv 30, 72, 114, 156, 198, 240, 282 \pmod{294}$

④ a) $159x \equiv 66 \pmod{201}$

$201 = 1 \cdot 159 + 42$
$159 = 3 \cdot 42 + 33$
$42 = 1 \cdot 33 + 9$
$33 = 3 \cdot 9 + 6$
$9 = 1 \cdot 6 + \boxed{3}$
$6 = 2 \cdot 3$

$53x \equiv 22 \pmod{67}$ →

| i | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| q | | | 1 | 3 | 1 | 3 | 1 |
| u | 0 | 1 | -1 | 4 | -5 | 19 | $\boxed{-24}$ |

$53(-24) \equiv 1 \pmod{67} \quad / \cdot 22$

$53(-24 \cdot 22) \equiv 22 \pmod{67}$

$x_0 \equiv -528 \pmod{67}$

$x_0 \equiv -59 \pmod{67}$

$x_0 \equiv 8 \pmod{67}$

$x = x_0 + k \cdot m \Rightarrow x \equiv 8, 75, 142 \pmod{201}$

b) $1100 \leq x_0 + km \leq 1400$

$1100 \leq 8 + k \cdot 67 \qquad 1400 \geq 8 + k \cdot 67$

$k \geq 17 \qquad k \leq 20$

$k = 17 \rightarrow 1147$
$k = 18 \rightarrow 1214$
$k = 19 \rightarrow 1281$
$k = 20 \rightarrow 1348$

c) $159 \equiv 66 \pmod{m} \Rightarrow m \mid 159 - 66$

$m \mid 93$

$m \mid 3 \cdot 31$

$m = \{1, 3, 31, 93\}$

⑤ a) $x \equiv 7 \pmod{17}$
$x \equiv 18 \pmod{31}$
$x \equiv 33 \pmod{37}$

1) $m = 17 \cdot 31 \cdot 37 = 19499$

2) $M_1 = \frac{m}{m_1} = 1147$
$M_2 = \frac{m}{m_2} = 629$
$M_3 = \frac{m}{m_3} = 527$

3) $1147 \cdot x \equiv 7 \pmod{17}$
$629 \cdot x \equiv 18 \pmod{31}$
$527 \cdot x \equiv 33 \pmod{37}$

4) $8 \cdot x \equiv 7 \pmod{17}$
$9 \cdot x \equiv 18 \pmod{31}$
$9 \cdot x \equiv 33 \pmod{37}$

5) $17 \mid 8x - 7 \Rightarrow x_1 = 3$
$31 \mid 9x - 18 \Rightarrow x_2 = 2$
$37 \mid 9x - 33 \Rightarrow x_3 = 16$

$37 = 9 \cdot 4 + 1$
$9 = 9 \cdot 1$

| i | -1 | 0 | 1 |
|---|---|---|---|
| q | | 4 | |
| u | 0 | 1 | -4 |

$9u \equiv 1 \pmod{37}$ $x = -4$
$9x \equiv 33 \pmod{37}$ $x = -4 \cdot 33$
$x \equiv -132 \pmod{37}$
$x \equiv 16 \pmod{37}$

6) $x_0 = M_1 \cdot x_1 + M_2 \cdot x_2 + M_3 \cdot x_3 = 13131$

7) $x \equiv 13131 \pmod{19499}$

b) $x \equiv 2 \pmod{5}$
$x \equiv 1 \pmod{6}$
$x \equiv 4 \pmod{11}$
$x \equiv 5 \pmod{17}$

1) $m = 5610$

2) $M_1 = 1122$
$M_2 = 935$
$M_3 = 510$
$M_4 = 330$

3) $1122 \cdot x \equiv 2 \pmod{5}$
$935 \cdot x \equiv 1 \pmod{6}$
$510 \cdot x \equiv 4 \pmod{11}$
$330 \cdot x \equiv 5 \pmod{17}$

4) $2x \equiv 2 \pmod{5}$
$5x \equiv 1 \pmod{6}$
$4x \equiv 4 \pmod{11}$
$7x \equiv 5 \pmod{17}$

5) $x_1 = 1$
$x_2 = 5$
$x_3 = 1$
$x_4 = 8$

6) $x_0 = 8947$

7) $x \equiv 8947 \pmod{5610}$
$x \equiv 3337 \pmod{5610}$

c) 1. korak
$5x \equiv 3 \pmod{7} \rightarrow x \equiv 2 \pmod{7}$
$16x \equiv 7 \pmod{17} \rightarrow x \equiv 10 \pmod{17}$
$25x \equiv 2 \pmod{37} \rightarrow x \equiv 6 \pmod{37}$

za $x_3$
$37 = 1 \cdot 25 + 12$
$25 = 2 \cdot 12 + 1$
$12 = 12 \cdot 1$

| i | -1 | 0 | 1 | 2 |
|---|---|---|---|---|
| q | | | 1 | 2 |
| u | 0 | 1 | -1 | 3 |

$25(3 \cdot 2) = 2 \pmod{37}$

2. korak
$m = 4403$

3. korak
$M_1 = 629$
$M_2 = 259$
$M_3 = 119$

4. korak
$629x \equiv 2 \pmod{7}$
$6x \equiv 2 \pmod{7}$
$x_1 = 5$

$259x \equiv 10 \pmod{17}$
$4x \equiv 10 \pmod{17}$
$x_2 = 11$

$119x \equiv 6 \pmod{37}$
$8x \equiv 6 \pmod{37}$
$x_3 = 10$

5. korak
$x_0 = 7184$

6. korak
$x \equiv 7184 \pmod{4403}$
$x \equiv 2781 \pmod{4403}$

$-2m \equiv 23 \pmod{49}$

⑥ a) $x \equiv 10 \pmod{15}$
$x \equiv 19 \pmod{21}$
$x \equiv 25 \pmod{60}$

1. korak →
$x \equiv 10 \pmod 3$
$x \equiv 10 \pmod 5$
$x \equiv 19 \pmod 3$
$x \equiv 19 \pmod 7$
$x \equiv 25 \pmod 3$
$x \equiv 25 \pmod 4$
$x \equiv 25 \pmod 5$

2. korak →
$x \equiv 1 \pmod 3$
$x \equiv 0 \pmod 5$
~~$x \equiv x \pmod 3$~~
$x \equiv 5 \pmod 7$
~~$x \equiv x \pmod 3$~~
$x \equiv 1 \pmod 4$
~~$x \equiv 0 \pmod 5$~~

3. korak
$M = 3 \cdot 5 \cdot 7 \cdot 4 = 420$

4. korak
$M_1 = 140$
$M_2 = 105$
$M_3 = 84$
$M_4 = 60$

5. korak
$140x \equiv 1 \pmod 3$
$105x \equiv 1 \pmod 4$
$84x \equiv 0 \pmod 5$
$60x \equiv 5 \pmod 7$

6. korak
$2x \equiv 1 \pmod 3$
$1x \equiv 1 \pmod 4$
$4x \equiv 0 \pmod 5$
$4x \equiv 5 \pmod 7$

7. korak
$x_1 = 2$
$x_2 = 1$
$x_3 = 5$
$x_4 = 3$

8 korak
$x_0 = x_1 \cdot M_1 + \ldots = 985$

9 korak
$x \equiv 985 \pmod{420}$
$x \equiv 145 \pmod{420}$

b)

⑦ $x \equiv 1 \pmod{41}$
$x \equiv 2 \pmod{42}$
$x \equiv 3 \pmod{43}$

$25 = 19 \cdot 1 + 6$
$19 = 6 \cdot 3 + 1$
$6 = 1 \cdot 6$

| i | -1 | 0 | 1 | 2 |
|---|---|---|---|---|
| q | | | 1 | 3 |
| u | 0 | 1 | -1 | 4 |

⑧ a) $5^2 \mid u$, $4^2 \mid u+1$, $5^2 \mid u+2$

$u \equiv 0 \pmod 9 \Rightarrow u \equiv 0 \pmod 9$
$u \equiv -1 \pmod{16} \Rightarrow u \equiv 15 \pmod{16}$
$u \equiv -2 \pmod{25} \Rightarrow u \equiv 23 \pmod{25}$

$\Rightarrow u \equiv 3600$

$x_1 = 400$ → $400u \equiv 0 \pmod 9$
$x_2 = 225$ → $225u \equiv 15 \pmod{16}$
$x_3 = 144$ → $144u \equiv 23 \pmod{25}$

$4u \equiv 0 \pmod 9$
$1u \equiv 15 \pmod{16}$
$19u \equiv 23 \pmod{25}$
$-2u \equiv 23 \pmod{25}$

$u_1 = 9$
$u_2 = 15$
$u_3 = 92$

$u_0 = 2023$

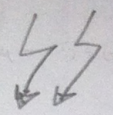
$u \equiv 2023 \pmod{3600}$
$u \equiv 2223 \pmod{3600}$

202-2

b) $n^2$

$n \equiv 0 \pmod 4$
$n \equiv -1 \pmod 9$ $\Rightarrow$
$n \equiv -2 \pmod{16}$

$n \equiv 0 \pmod 4$
$n = 8 \pmod 9$
$n = 14 \pmod{16}$



# 3. Dz → zadaci

① dokaži: $3^{105} + 4^{105}$ djeljiv sa 7 i 13, a nije s 11

mod 7

$\varphi(7) = 7 \cdot (1 - \frac{1}{7}) = 6$

$3^{\varphi(7)} \equiv 1 \pmod 7$

$3^6 \equiv 1 \pmod 7$

$105 : 6 = 17$ ostatak 3 ← $17 \cdot 6$

$3^{102} \equiv 1 \pmod 7$

ostalo 3

$3^3 \equiv 6 \pmod 7$

$4^6 \equiv 1 \pmod 7$

$4^{102} \equiv 1 \pmod 7$

$4^3 \equiv 1 \pmod 7$

uvjet da bi mogli računat

$nzd(3,7) = 1$ ✓

$nzd(4,7) = 1$ ✓

$nzd(3,13) = 1$ ✓

$nzd(4,13) = 1$ ✓

$nzd(3,11) = 1$ ✓

$nzd(4,11) = 1$ ✓

$1 + 6 = 7 \equiv \boxed{0} \pmod 7$

mod 13

$\varphi(13) = 13 \cdot (1 - \frac{1}{13}) = 12$

$3^{12} \equiv 1 \pmod{13}$

ostalo $3^9 \equiv 1 \pmod{13}$

$4^{12} \equiv 1 \pmod{13}$

$4^9 \equiv 12 \pmod{13}$

$1 + 12 = 13 \equiv \boxed{0} \pmod{13}$

mod 11

$\varphi(11) = 11 \cdot (1 - \frac{1}{11}) = 10$

$3^{10} \equiv 1 \pmod{11}$

ostalo $3^5 \equiv 1 \pmod{11}$

$4^{10} \equiv 1 \pmod{11}$

$4^5 \equiv 1 \pmod{11}$

$1 + 1 = 2 \equiv \boxed{2} \pmod{11}$

② $1111^{222} \cdot 33^{444} \mod 19 = ?$

$\varphi(19) = 19 \cdot (1 - \frac{1}{19}) = 18$

$nzd(1111, 19) = 1$ ✓

$nzd(33, 19) = 1$ ✓

$1111^{18} \equiv 1 \pmod{19}$

$222 : 18 = 12$ ostatak

$1111^{18 \cdot 12} \equiv 1 \pmod{19}$

ostatak $1111^6$ → prevelik broj za digitron pa rastavimo na dva manja

$(1111^3)^2 \rightarrow (1111^3 \bmod 19)^2 \bmod 19 = (7)^2 \bmod 19 \rightarrow 11 \pmod{19}$

$33^{18} \equiv 1 \pmod{19}$

$444 : 18 = 24$ ostatak

$33^{18 \cdot 24} \equiv 1 \pmod{19}$

ostatak $33^{12}$ → prevelikso ⇒ $(33^6)^2 \rightarrow (33^6 \bmod 19)^2 \bmod 19 \rightarrow 11 \pmod{19}$

7

Nj: $11 \cdot 11 = 121 \pmod{19} = 7 \pmod{19}$

3DZ-1

③ $73^{73} \bmod 38$

$\text{nzd}(73,38)=1$ ✓ $\Rightarrow \varphi(38)=38\cdot(1-\frac{1}{2})(1-\frac{1}{19})=18$ $\quad 73^{18}\equiv 1 \pmod{38}$

ostatak $\Rightarrow$ $\underline{73^1 \equiv 35 \pmod{38}}$ //

④ $53^{181} \pmod{105}$

$\text{nzd}(53,105)=1$ ✓ $\Rightarrow \varphi(105)=105\cdot(1-\frac{1}{3})(1-\frac{1}{5})=56$ $\quad 53^{56}\equiv 1 \pmod{105}$

$53^{168}\equiv 1 \pmod{105}$

$\left\{\left[\left((53^4 \bmod 105)^2 \bmod 105\right)\cdot 53^3\right] \bmod 105\right\} 53^2 \bmod 105$ ostatak $53^{13}=(53^4)^2 53^3\, 53^2$

$\Rightarrow \underline{X \equiv 53 \pmod{105}}$ //

⑤ $314^{162} \bmod 165$

$\text{nzd}(314,165)=1$ ✓ $\Rightarrow \varphi(165)=165\cdot(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{11})=80$

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

$314^{80\cdot 2}\equiv 1 \pmod{165}$

ostatak $\rightarrow$ $\underline{314^2 \equiv 91 \pmod{105}}$ //

⑥ $1^5+2^5+\ldots+99^5+100^5 \bmod 4 \rightarrow \varphi(4)=2$

za parne br $\bmod 4 = \emptyset$

$\rightarrow$ ostalo 50 neparnih

$\rightarrow a^2\equiv 1 \pmod 4$

$a^4\equiv 1 \pmod 4$

ostatak $\Rightarrow a^1 \equiv ? \pmod 4$

$1^1\equiv 1 \pmod 4$

$3^1\equiv 3 \pmod 4$

$5^1\equiv 1 \pmod 4$

$7^1\equiv 3 \pmod 4$

$97^1\equiv 1 \pmod 4$

$99^1\equiv 3 \pmod 4$

25. ostatak $1 \pmod 4$ } +

25. ostatak $3 \pmod 4$ }

$100 \pmod 4 = \emptyset$

$X \equiv 0 \pmod 4$

⑦ $53^{82}$, zadnje dvije znamenke? $\Rightarrow n=100$ $\quad \varphi(100)=100\cdot(1-\frac{1}{2})(1-\frac{1}{5})=40$

$\text{nzd}(53,100)=1$ ✓

$53^{40}\equiv 1 \pmod{100}$

$53^{40\cdot 2}\equiv 1 \pmod{100}$

ostatak $53^2 \equiv 09 \pmod{100}$

0 ; 9

⑧ $71^{245}$, zadnje dvije?

isto sve $\Rightarrow$ 5 ; 1

⑨ a) $14^{2012}$, zadnji dvije?

$\text{nzd}(14, 100) \neq 1 \Rightarrow$ UVJET NIJE ZADOVOLJEN PA:

$X \equiv 14^{2012} \pmod{100}$ → imamo više nj ?

4 | 25

$\boxed{14^{2012} \equiv 0 \pmod 4}$ $\quad 14^{2012} \equiv ? \pmod{25}$

$\text{nzd}(14, 25) = 1$ ✓

$\varphi(25) = 25 \cdot (1 - \frac{1}{5}) = 20 \Rightarrow 14^{20} \equiv 1 \pmod{25}$

$14^{20 \cdot 100} \equiv 1 \pmod{25}$

ostatak $14^{12} = (14^6)^2 \rightarrow (14^6 \bmod 25)^2 \bmod 25 \Rightarrow \boxed{X \equiv 21 \pmod{25}}$

$x \in [0, 99] \Rightarrow X = 21 + 25 \cdot k < 100$ → samo taj zadovoljava oba uvjeta

$X \equiv 21, 46, 71, \boxed{96} \pmod{100}$

$X \equiv 0 \pmod 4$

$X \equiv 21 \pmod{25}$

$\boxed{X \equiv 96 \pmod{100}}$

b) $14^{2012}$, zadnje tri? $\Rightarrow n = 1000$

$\text{nzd}(14, 1000) \neq 1$, $1000 = 8 \cdot 125$

$\boxed{14^{2012} \equiv 0 \pmod 8}$

$\text{nzd}(125, 14) = 1$ ✓ $\rightarrow \varphi(125) = 125 \cdot (1 - \frac{1}{5}) = 100$

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

$14^{100 \cdot 20} \equiv 1 \pmod{125}$

ostatak $14^{12} = (14^6)^2 \Rightarrow X \equiv 46 \pmod{125}$

$X \equiv 46, 171, \boxed{296}, 421, 546, 671, 796, 921 \pmod{1000}$

↳ samo taj zadovoljava oba uvjeta $\boxed{X \equiv 296 \pmod{1000}}$

⑩ ?

# 4. DZ → zadaci

② a) $f(n)=4$ → $p \mid n \Rightarrow p \mid f(n)$

svi br. djeljivi s 4 $\Rightarrow 1, 2, 4 \rightarrow \{1+1, 2+1, 4+1\} = \{2, 3, 5\} \in P$ → ako ima onih koji nisu prosti izbaci ih

1) $p=5 \rightarrow 5 \mid n$ da ako je $n = 5 \cdot k$ UVJET: $n \nmid d(5,4)=1$ ✓

$f(n) = f(5 \cdot k) = f(5) \cdot f(k) = 4$

$4 \cdot f(k) = 4 \Rightarrow f(k) = 1$

- $k=1 \Rightarrow \boxed{n=5}$
- $k=2 \Rightarrow \boxed{n=10}$

2) $p=3 \rightarrow 3 \mid n$, $n = 3 \cdot k$ UVJET: $n \nmid d(3,4)=1$ i $n \nmid d(5,4)=1$ ✓

$f(n) = f(3k) = f(3) \cdot f(k) = 4$

$f(k) = 2$

- ~~$k=3 \rightarrow n=9$~~ $n \nmid d(3,3) \neq 1$
- $k=4 \rightarrow \boxed{n=12}$
- ~~$k=6 \rightarrow n=18$~~ $n \nmid d(3,6) \neq 1$

3) $p=2 \rightarrow 2 \mid n$, $n=2k$ UVJET: $n \nmid d(2,4)=1$ i prethodna dva ✓

$f(n) = f(2k) = f(2) \cdot f(k) = 4$

$1 \cdot f(k) = 4 \Rightarrow f(k) = 4$ ← upravo to tražimo pa:

→ poništavamo sljedeći:

$\boxed{n = 2^2 \cdot k} \Rightarrow f(4) \cdot f(k) = 4$

$f(k) = 2$

- $k=3$ ← odbačeno zbog uvjeta
- $k=4$ ← odbačeno zbog uvjeta
- $k=6$ ← odbačeno zbog uvjeta

i to dijeli $f(n)$ pa tražimo opet:

$\boxed{n = 2^3 k} \Rightarrow f(8) \cdot f(k) = 4 \Rightarrow f(k) = 1$

- $k=1 \Rightarrow \boxed{n=8}$
- $k=2$ ← odbačeno zbog uvjeta

to ne dijeli $f(n)$ pa više ne tražimo ✓

Rj: $n = \boxed{5, 8, 10, 12}$

4DZ-1

e) $\ell(n) = 56$

$\rightarrow p \mid n \Rightarrow \underbrace{p-1}_{} \mid \ell(n)$ — nisu prosti

↳ 1, 2, 4, 7, 8, 14, 28, 56 $\Rightarrow p \in \{2, 3, 5, \cancel{7}, \cancel{8}, \cancel{15}, 29, \cancel{57}\}$

(1) $p = 29 \rightarrow 29 \mid n \Rightarrow n = 29 \cdot k$ uvjet: $\text{nzd}(k, 29) = 1$

$\ell(29) \cdot \ell(k) = 56$

$\ell(k) = \frac{56}{28} = 2$ → $k = 3 \Rightarrow \boxed{n = 87}$; $k = 4 \Rightarrow \boxed{n = 116}$; $k = 6 \Rightarrow \boxed{n = 174}$

(2) $p = 5 \rightarrow 5 \mid n \Rightarrow n = 5 \cdot k$ uvjet: prethodni; $\text{nzd}(5, k) = 1$

$\ell(5) \cdot \ell(k) = 56$

$\ell(k) = \frac{56}{4} = 14 \rightarrow$ ne možemo odmah pogoditi za koje $k$ vrijedi pa moramo i to računati:

$1, 2, 7, 14 \Rightarrow p \in \{\underbrace{2, 3}_{\text{obradit demo}}, \cancel{8}, \cancel{15}\}$

(3) $p = 3 \rightarrow 3 \mid n \Rightarrow n = 3 \cdot k$ uvjet: prethodni; $\text{nzd}(3, k) = 1$

$\ell(3) \cdot \ell(k) = 56$

$\ell(k) = \frac{56}{2} = 28 \rightarrow$ ne možemo pogodit pa računamo:

$1, 2, 4, 7, 14, 28 \rightarrow p \in \{\underbrace{2, 3}_{\text{hvatamo}}, \cancel{8}, \cancel{15}, 29\}$ ← obradili

(4) $p = 2 \rightarrow 2 \mid n \Rightarrow$ da; odmah računamo slijedeći

$k = 2^2 \cdot k \Rightarrow$ da; odmah računamo slijedeći

$n = 2^3 \cdot k \Rightarrow$ — " —

$n = 2^4 \cdot k \Rightarrow$ ne dijeli $\Rightarrow \ell(16) \cdot \ell(k) = 56 \rightarrow \ell(k) = 7$ ← NE MOŽE BITI JEDNAKO 7

Tj. $\boxed{n = 87, 116, 174}$

② $\varphi(n)=14 \quad p \mid n \Rightarrow p-1 \mid \varphi(n)$ — nisu prosti?

$1, 2, 7, 14 \Rightarrow p \in \{2, 3, \cancel{4}, \cancel{7}, \cancel{15}\}$

(1) $p=3 \quad 3 \mid n \Rightarrow n = 3 \cdot k$

$\varphi(3) \cdot \varphi(k) = 14 \Rightarrow \varphi(k) = 7$ ← ne može ✗

(2) $p=2 \quad 2 \mid n \Rightarrow$ da, tražimo dalje:

$n = 2^2 \cdot k \Rightarrow \varphi(4) \cdot \varphi(k) = 14$

$\varphi(k) = 7$ ← ne može ✗

} ne postoji nijedan $n$ takav da je $\varphi(n)=14$ !!

⑤ b) $\frac{\varphi(n)}{n} = \frac{4}{11}$

$\varphi(n) = n \cdot \prod (1 - \frac{1}{p})$ ⇒ $\frac{\varphi(n)}{n} = \frac{4}{11} = \prod (1 - \frac{1}{p}) \quad / \cdot 11$

($p$ — prosti brojevi)

$4 = 11 \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots$

$4 = 11 \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \frac{p_3 - 1}{p_3} \cdot \ldots$

$\boxed{p_1 = 11} \Rightarrow \cancel{4} = \cancel{11} \cdot \frac{10}{11} \cdot \frac{p_2 - 1}{p_2} \cdot \frac{p_3 - 1}{p_3} \cdot \ldots$ (2, 5)

$\boxed{p_2 = 5} \Rightarrow \cancel{2} = \cancel{5} \cdot \frac{4}{5} \cdot \frac{p_3 - 1}{p_3} \cdot \ldots$ (1, 2)

$\boxed{p_3 = 2} \Rightarrow 1 = \cancel{2} \cdot \frac{1}{\cancel{2}} \cdot \ldots$

Mj: $2, 5, 11 \mid n \Rightarrow n = 2 \cdot 5 \cdot 11 = \underline{110}$

$\boxed{n = 110 \cdot k}, \quad k = 1, 2, 3, \ldots$

a) Mj: $2, 3, 7 \mid n \Rightarrow n = 2 \cdot 3 \cdot 7 = 42$

$\boxed{n = 42 \cdot k}, \quad k = 1, 2, \ldots$

⑦ a) $\varphi(n) \mid 3n \Rightarrow \varphi(n) \cdot k = 3n$

$k \cdot \cancel{n} \cdot \prod (1 - \frac{1}{p}) = 3\cancel{n}$

$3 = k \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \ldots \cdot \frac{p_4 - 1}{p_4}$

* uzimamo $p_1 = k$ na temelju prethodnog zadatka (mora biti prosti)

$\boxed{p_1 = 7}$

$\boxed{p_2 = 2} \quad 1 = 1$ ✓

$\boxed{n = 14 \cdot i}, \quad i = 1, 2, \ldots$

$k = 2 \Rightarrow 3 = 1 \cdot \frac{p_2 - 1}{p_2} \ldots$ (ne odgovara)

$k = 3 \Rightarrow 3 = 2 \cdot \frac{p_2 - 1}{p_2} \ldots$ (ne odgovara)

$k = 5 \Rightarrow 3 = 4 \cdot \frac{p_2 - 1}{p_2} \ldots$ (ne odgovara)

$k = 7 \Rightarrow \cancel{3} = \cancel{6} \cdot \frac{p_2 - 1}{p_2} \cdot \frac{p_3 - 1}{p_3}$ ✓ (1, 2)

4DZ-2

# 5. Dt → zadaci

① a) red od 5 mod 17

→ tražimo najmanji $d \in \mathbb{N}$ koji vrijedi: $5^d \equiv 1 \pmod{17}$

$d \Rightarrow \ell(17) = 17 \cdot (1 - \frac{1}{17}) = 16 \Rightarrow d \mid 16 \Rightarrow \{1, 2, 4, 8, 16\}$

$5^1 \equiv 5 \pmod{17}$ –

$5^2 \equiv 8 \pmod{17}$ –

$5^4 \equiv 13 \pmod{17}$ –

$5^8 \equiv 16 \pmod{17}$ –

$5^{16} \equiv (5^8)^2 \equiv 1 \pmod{17}$ ✓ $\Rightarrow$ $\boxed{d = 16}$ $\Rightarrow d = \ell(n) \Rightarrow$ primitivni korijen

b) red od 7 mod 29

$\ell(29) = 28 \Rightarrow d \mid 28 \Rightarrow \{1, 2, 4, 7, 14\}$

$7^1 \equiv 7 \pmod{29}$ –

$7^2 \equiv 20 \pmod{29}$ –

$7^4 \equiv 23 \pmod{29}$ –

$7^7 \equiv 1 \pmod{29}$ ✓ $\boxed{d = 7}$ $d \neq \ell(n) \Rightarrow$ nije primitivni korijen

⑤ a) koliko ima primitivnih korijena modulo 43? odredi najmanji

postoji točno $\ell(p-1)$ p.k

$\ell(42) = 42 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = \boxed{12}$

najmanji: $p - 1 = 42 = 2 \cdot 3 \cdot 7 \Leftarrow \begin{matrix} \frac{42}{2} = 6 \\ \frac{42}{3} = 14 \\ \frac{42}{7} = 21 \end{matrix}$ } potencije

$2^6 \equiv 21 \pmod{43}$
$2^{14} \equiv 1 \pmod{43}$ } odma znamo da nije ima g dan $1 \pmod{x}$
$2^{21} =$

$3^6 \equiv 41 \pmod{43}$
$3^{14} \equiv 36 \pmod{43}$ ✓ najmanji $\boxed{3}$
$3^{21} = 42 \pmod{43}$

dodatak: odredi sve primitivne

$\text{nzd}(i, p-1) = 1$

$\text{nzd}(i, 42) = 1 \quad i = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$

najmanji $\boxed{3} \rightarrow x^i \pmod{43} = \ldots$

5) ima ih 28, najmanji 2

⑥ isto ko i 5.

⑧ i ⑨ postoj 3 tipa: $X^y \equiv$ nešto $(\mathrm{mod}$ nešto$)$ I jednostavno

$A \cdot X^y \equiv$ nešto $(\mathrm{mod}$ nešto$)$ II } malo teže

$A^X \equiv$ nešto $(\mathrm{mod}$ nešto$)$ III

I. tip

$X^5 \equiv 2 \pmod 7$

1) korak $\Rightarrow$ najmanji primitivni korijen $p-1 = 6 = 2 \cdot 3$ $\frac{6}{3} = \boxed{2}$, $\frac{6}{2} = \boxed{3}$

$\varphi(7-1) = \boxed{2}$ $\rightarrow$ ima ih $\boxed{2}$

$2^2 \equiv 4 \pmod 7$

$2^3 \equiv 1 \pmod 7$ ✗

$3^2 \equiv 2 \pmod 7$

$3^3 \equiv 6 \pmod 7$ ✓ $\Rightarrow \boxed{3}$ najmanji

2) uđesi rat po bazi najmanjeg korijena

$X^5 \equiv 2 \pmod 6 \quad / \cdot ind_3$

$ind_3 x^5 \equiv ind_3 2 \pmod 6$

$5\, ind_3 x \equiv (ind_3 2) \pmod 6$

$5\, ind_3 x \equiv 2 \pmod 6$

$\rightarrow$ sad možemo pogoditi $6 \mid 5 \cdot \overbrace{ind_3 x}^{4} - 2$ ✓

$4 = ind_3 x \Rightarrow \boxed{X = 3^4 \equiv 4 \pmod 7}$

svojstva kao i log

$\boxed{3^l \equiv 2 \pmod 7}$ to želimo dobiti i tražimo za koji $l$ to vrijedi

$3^1 \equiv 3 \pmod 7$ ✗

$3^2 \equiv 2 \pmod 7$ ✓

II. tip

$41x^9 \equiv 22 \pmod{43}$

1) korak $\Rightarrow$ primitivni korijeni i najmanji

$\varphi(43-1) = \boxed{12}$

$42 = 2 \cdot 3 \cdot 7$ $\quad \frac{42}{2} = 6$, $\frac{42}{3} = 14$, $\frac{42}{7} = 21$ $\Rightarrow$ već izračunali u ručnom od zadatka

najmanji $= \boxed{3}$

2) indeksiramo po toj bazi

$41x^9 \equiv 22 \pmod{42} \quad / ind_3$

$ind_3 41x^9 \equiv ind_3 22 \pmod{42}$

$ind_3 41 + 9\, ind_3 x \equiv ind_3 22 \pmod{42}$

$6 \qquad\qquad 15$

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

$3^4 \equiv 38 \pmod{43}$

$3^5 \equiv 28 \pmod{43}$

$\boxed{3^6 \equiv 41 \pmod{43}}$

$3^7 \equiv 37 \pmod{43}$

$3^8 \equiv 25 \pmod{43}$

$3^9 \equiv 32 \pmod{43}$

$3^{15} \equiv 22 \pmod{43}$

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

$9\, ind_3 x \equiv 9 \pmod{42}$

$\text{nzd}(9, 42) = 3$

$3\, ind_3 x \equiv 3 \pmod{14}$

$\text{nzd}(3, 14) = 1$

$ind_3 x \equiv 1 \pmod{14}$ $\Rightarrow$ $ind_3 x \equiv 1, 15, 29 \pmod{42}$

$x \equiv 3^1 \equiv 3 \pmod{43}$

$x \equiv 3^{15} \equiv 22 \pmod{43}$

$x \equiv 3^{29} \equiv 18 \pmod{43}$

5dt-2

III. typ

$28^x \equiv 27 \pmod{43}$

1) najmniejszy pierwiastek liczący $\Rightarrow$ $\boxed{3}$

2) wdelsirować p tej bazi

$28^x \equiv 27 \pmod{42} \quad / \mathrm{ind}_3$

$\mathrm{ind}_3 28^x \equiv \mathrm{ind}_3 27 \pmod{42}$

$x \cdot \mathrm{ind}_3 28 \equiv \mathrm{ind}_3 27 \pmod{42}$

$3^l \equiv 27 \pmod{43}$

$3^3 = 27 \pmod{43}$

$3^5 = 28 \pmod{43}$

$x \cdot 5 \equiv 3 \pmod{42} \Rightarrow 42 \mid 5x-3 \Rightarrow x = 9$

$x \equiv 9 \pmod{43}$

# 6. Dz → zadaci

① svi kvadratni ostaci mod 29

↓

$\{-14,-13,\dots,-1,1,2,3,\dots,13,14\}$

kvadratni ostaci su: $\{1^2,2^2,3^2,4^2,5^2,6^2,7^2,8^2,9^2,10^2,11^2,12^2,13^2,14^2\} \pmod{29}$

→ $[1,4,5,6,7,9,13,16,20,22,23,24,25,28]$

③;④ Legendreovi simboli:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & ; \ a \text{ je kvadratni ostatak mod } p \\ -1 & ; \ \text{--11--} \quad \text{neostatak} \quad \text{--11--} \\ 0 & ; \ p \mid a \end{cases}$$

* razlika između Legendreovih i Jacobijevih simbola je u tome što je kod Legendreovih $\left(\frac{a}{p}\right)$, $p \to$ prost broj!

→ ostalo je sve isto, pa vrijede i ista SVOJSTVA:

(1) $a \equiv b \pmod p \to \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(2) $\left(\frac{a\cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(3) $\left(\frac{a^2}{p}\right) = 1 \Rightarrow$ ako vrd $(a,p)=1$

(4) $\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{p}\right) = \begin{cases} -1 & , p \equiv 3 \pmod 4 \\ 1 & , p \equiv 1 \pmod 4 \end{cases}$

(5) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} -1 & , m \equiv 3,5 \pmod 8 \\ 1 & , m \equiv 1,7 \pmod 8 \end{cases}$

Gauss (6) $\left(\frac{m}{n}\right)\cdot\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} = \begin{cases} -1 & , m \equiv n \equiv 3 \pmod 4 \\ 1 & , m \equiv 1 \pmod 4 \text{ ili } n \equiv 1 \pmod 4 \end{cases}$

* $m \equiv n \equiv 3 \pmod 4 \Rightarrow \left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$

* $m$ ili $n \equiv 1 \pmod 4 \Rightarrow \left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$

6Dz-1

② a) bez svojstva koristimo $97 \bmod 35$

$$\left(\frac{-35}{97}\right) \overset{(2)}{=} \left(\frac{-1}{97}\right)\cdot\left(\frac{35}{97}\right) = (1)\cdot\left(\frac{35}{97}\right) \overset{(6)}{=} \left(\frac{97}{35}\right) \overset{\downarrow}{=} \left(\frac{27}{35}\right) \overset{(6)}{=} \left(-\frac{35}{27}\right) = \left(-\frac{1}{27}\right)\left(\frac{35}{27}\right) = (-1)\cdot\left(\frac{8}{27}\right)$$

prost = Legendre

$97 \equiv 1 \pmod 4$ (4) $\Rightarrow 1$

$35 \equiv 3 \pmod 4$, $97 \equiv 1 \pmod 4$ } (6)

$27 \equiv 3 \pmod 4$, $35 \equiv 3 \pmod 4$

$= (-1)\cdot\left(\frac{2}{27}\right)^3 \overset{(5)}{=}$

$27 \equiv 3 \pmod 8$

$= (-1)\cdot(-1)^3 = \boxed{1}$

④ $$\left(\frac{40}{403}\right) \overset{(2)}{=} \left(\frac{10}{403}\right)\cdot\left(\frac{2}{403}\right)^2 \overset{(5)}{=} (-1)^2\cdot\left(\frac{2}{403}\right)\cdot\left(\frac{5}{403}\right) \overset{(6)}{=} (-1)^2\cdot(-1)\cdot\left(\frac{403}{5}\right) = (-1)\left(\frac{3}{5}\right) = (-1)\left(\frac{2}{3}\right)$$

$= 1$

wg prost = Jacobijev

⑤ a) $$\left(\frac{-60}{377}\right) = \left(-\frac{1}{377}\right)\left(\frac{60}{377}\right) = \left(\frac{2}{377}\right)^2\cdot\left(\frac{15}{377}\right) = 1^2\left(\frac{2}{15}\right) = 1$$

$1 \pmod 4$ $\quad$ $1 \pmod 8$

b) $\bmod 377 \Rightarrow \quad 377 = 13\cdot 29$

$\left(\frac{-60}{13}\right) = \left(-\frac{8}{13}\right) = \left(-\frac{1}{13}\right)\left(\frac{2}{13}\right)^3 = (1)\cdot(-1)^3 = (-1)$ → odma znamo da nije 8 jer oba moraju biti

$\boxed{1}$

$\left(\frac{-60}{29}\right) = \dots$

a) $$\left(\frac{-60}{323}\right) = \left(-\frac{1}{323}\right)\left(\frac{60}{323}\right) = (-1)\left(\frac{2}{323}\right)^2\left(\frac{15}{323}\right) = (-1)\cdot\left(-\frac{323}{15}\right) = (-1)\left(-\frac{1}{15}\right)\left(\frac{7}{15}\right)$$

$3 \pmod 4$ $\quad$ $3 \pmod 8 \Rightarrow (-1)^2$ $\quad$ $3 \pmod 4$ $\quad$ $(-1)$

$= \left(\frac{2}{15}\right)^3 = (1)^3 = 1$

c) $\bmod 323 \Rightarrow \quad 323 = 19\cdot 17$

$\left(\frac{-60}{19}\right) = \dots = 1$ } $-60$ i kvadratni ostatak mod 323

$\left(\frac{-60}{17}\right) = \dots = 1$

⑥ sv. neparni prosti:

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

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

$p\equiv 1 \pmod 4 \to \left(\frac{p}{3}\right)$ : $p\equiv 1 \pmod 3 \Rightarrow 1$; $p\equiv 2 \pmod 3 \Rightarrow -1$

$p\equiv 3 \pmod 4 \to \left(-\frac{p}{3}\right)$ : $p\equiv 1 \pmod 3 \Rightarrow -1$; $p\equiv 2 \pmod 3 \Rightarrow 1$

$p\equiv 1,7 \pmod 8$ (1) $\quad p\equiv 3,5 \pmod 8$ (−1)

tražimo parove da zadovoljimo uvjet:

$\left(\frac{6}{p}\right)=1$ $\begin{cases} p\equiv 1 \pmod 8 \\ p\equiv 1 \pmod 3 \end{cases}$ nemoguće, $\begin{cases} p\equiv 7 \pmod 8 \\ p\equiv 2 \pmod 3 \end{cases}$ ① $\Rightarrow$ rj: 23

$\begin{cases} p\equiv 3 \pmod 8 \\ p\equiv 1 \pmod 3 \end{cases}$ ② $\qquad \begin{cases} p\equiv 5 \pmod 8 \\ p\equiv 2 \pmod 3 \end{cases}$ ③

→ ima 3 sustava kongruencija (kineski teorem o ostacima)

① $m=8\cdot 3=24$

$m_1=\frac{24}{8}=3$ $\quad m_1\cdot p\equiv 7 \pmod 8 \Rightarrow 8 \mid 3p-7$ $\quad \boxed{p_1=5}$

$m_2=\frac{24}{3}=8$ $\quad m_2\cdot p\equiv 2 \pmod 3 \Rightarrow 3 \mid 8p-2$ $\quad \boxed{p_2=1}$

$p_0=m_1\cdot p_1+m_2\cdot p_2=\boxed{23} \pmod{24}$

② $m=8\cdot 3=24$

$m_1=3$ $\quad m_1\cdot p_3\equiv 3 \pmod 8 \Rightarrow 8 \mid 3p_3-3$ $\quad \boxed{p_3=1}$

$m_2=8$ $\quad m_2\cdot p_4\equiv 1 \pmod 3 \Rightarrow 3 \mid 8p_4-1$ $\quad \boxed{p_4=2}$

$p_0=19 \pmod{24}$

③ $m=24$

$m_1=3$ $\quad m_1\cdot p_5\equiv 5 \pmod 8 \Rightarrow 8 \mid 3p_5-5$ $\quad \boxed{p_5=7}$

$m_2=8$ $\quad m_2\cdot p_6\equiv 2 \pmod 3 \Rightarrow 3 \mid 8p_6-2$ $\quad \boxed{p_6=1}$

$p_0=29 \pmod{24}$

rj: $p\equiv 19, 23, 5 \pmod{24}$

607-2

③

$x^2+45 \equiv 0 \pmod p$

$x^2 \equiv -45 \pmod p$ → $p \neq 3, 5$ → jer onda kongruencija nema rj

$(-45) \to 3^2$, $5$ ; $\left(\frac{-45}{p}\right) = 1$

$1 \pmod 4 \Rightarrow \left(\frac{p}{5}\right)$

- $p \equiv 1 \pmod 5 \Rightarrow 1$
- $p \equiv 2 \pmod 5 \Rightarrow -1$
- $p \equiv 3 \pmod 5 \Rightarrow -1$
- $p \equiv 4 \pmod 5 \Rightarrow 1$

$\left(-\frac{1}{p}\right) \cdot \underbrace{\left(\frac{3}{p}\right)^2}_{\text{uvijek } 1} \cdot \left(\frac{5}{p}\right) = \left(-\frac{1}{p}\right)\left(\frac{5}{p}\right)$

| $p \equiv 1 \pmod 4$ | $p \equiv 3 \pmod 4$ |
|---|---|
| 1 | -1 |

SUSTAV:

$\left(\frac{-45}{p}\right) = 1$ $\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 5 \end{cases}$ ✗

$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 4 \pmod 5 \end{cases} \Rightarrow$ $m = 20$, $m_1 = 5$, $m_2 = 4$

$4 \mid 5p_1 - 1 \Rightarrow \boxed{p_1 = 1}$

$5 \mid 4p_2 - 4 \Rightarrow \boxed{p_2 = 1}$

$\Rightarrow p_0 \equiv 9 \pmod{20}$

$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 2 \pmod 5 \end{cases} \Rightarrow$

$4 \mid 5p_3 - 3 \Rightarrow \boxed{p_3 = 3}$

$5 \mid 4p_4 - 2 \Rightarrow \boxed{p_4 = 3}$

$\Rightarrow p_0 \equiv 27 \pmod{20} \equiv 7 \pmod{20}$

$\begin{cases} p \equiv 3 \pmod 4 \\ p \equiv 3 \pmod 5 \end{cases}$ ✗

Rj $p \equiv 7, 9 \pmod{20}$