PREDAVANJE 5

Marija Mia

ZAD. 1.14.

$$\left(\frac{51}{71}\right) = -\left(\frac{71}{51}\right)^{*}$$

$$= -\left(\frac{20}{51}\right) \quad \rightarrow 71-51$$

$$= -\left(\frac{2}{51}\right)\left(\frac{2}{51}\right)\left(\frac{5}{51}\right)$$

$$\underbrace{\left(\frac{2}{51}\right)\left(\frac{2}{51}\right)}_{1}$$

$$= -\left(\frac{51}{5}\right) = -\left(\frac{1}{5}\right)$$

$$* \left(\frac{51}{71}\right)\left(\frac{71}{51}\right) = (-1)^{\frac{50\cdot 70}{4}} = -1$$

$$\left(\frac{5}{51}\right)\left(\frac{51}{5}\right) = (-1)^{\frac{4\cdot 50}{4}} = 1$$

PR. 1.26. a) odredite sve proste brojeve p takve da je -2 kvadratni ostatak modulo p

b) dokazati da postoji beskonačno mnogo prostih brojeva oblika $8k+3$

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

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

1° $\left(\frac{-1}{p}\right) = 1 = (-1)^{\frac{p-1}{2}} \Rightarrow p \equiv 1 \pmod 4$ → propozicija 1.38. 4)

$\frac{p-1}{2} = 2k \Rightarrow p = 4k+1$

$\left(\frac{2}{p}\right) = 1 \Rightarrow p \equiv 1, 7 \pmod 8$ → osnovna svojstva Jacobijevog simbola (str. 32)

$$\left.\begin{array}{l} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 8 \end{array}\right\} p \equiv 1 \pmod 8$$

$$\left.\begin{array}{l} p \equiv 1 \pmod 4 \\ p \equiv 7 \pmod 8 \Rightarrow p \equiv 3 \pmod 4 \end{array}\right\} \text{nema rješenja}$$

$\hookrightarrow p \equiv 7 \pmod 4 \Rightarrow p \equiv 3 \pmod 4$

2° $\left(\frac{-1}{p}\right) = -1 = (-1)^{\frac{p-1}{2}} \implies p \equiv 3 \pmod 4$

$\left(\frac{2}{p}\right) = -1 \implies p \equiv 3, 5 \pmod 8$

$$\left.\begin{array}{l} p \equiv 3 \pmod 4 \\ p \equiv 3 \pmod 8 \end{array}\right\} \quad p \equiv 3 \pmod 8$$

$$\left.\begin{array}{l} p \equiv 3 \pmod 4 \\ p \equiv 5 \pmod 8 \implies p \equiv 1 \pmod 4 \end{array}\right\} \quad \text{nema rješenja}$$

$\hookrightarrow p \equiv 5 \pmod 4 \to p \equiv 1 \pmod 4$

b) pretpostavimo suprotno tj. $p_1, p_2, \dots, p_n$ su svi prosti brojevi oblika $8k+3$

$m = p_1^2 p_2^2 p_3^2 \dots p_n^2 + 2$

$x^2 \equiv -2 \pmod m \implies x^2 \equiv -2 \pmod{q_i}$

q_i – bilo koji prosti faktor od m

$\hookrightarrow q_i$ mora biti oblika $8k+1$ ili $8k+3$

$\hookrightarrow$ postoji barem jedan prosti faktor od m oblika $8k+3$

$\Downarrow$

jedan prosti faktor od m je p_1

$p_i \equiv 3 \pmod 8$

$p_i^2 \equiv 1 \pmod 8$

$m \equiv 3 \pmod 8$

$\implies m = p_1 \cdot m'$

$p_1 \cdot m' = p_1^2 p_2^2 \cdots p_n^2 + 2$

$p_1 \cdot m' - p_1^2 p_2^2 \cdot p_n^2 = 2$

$p_1 (\dots) = 2$

$\hookrightarrow$ desna strana nije djeljiva s p_1

~~ZADATAK~~ Odredite $\left(\frac{3}{p}\right)$ za sve neparne proste brojeve p

$p = 3 \rightarrow \left(\frac{3}{3}\right) = 0$

$(p,3) = 1 \qquad \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)(3-1)}{4}}$

$= (-1)^{\frac{p-1}{2}}$ *

1° $\left(\frac{3}{p}\right) = 1 \qquad \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$

$p \equiv 1, 2 \pmod 3$ ⟶ ostatak može biti samo 1 ili 2 (dijeljenje s 3)

I) $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1 = (-1)^{\frac{p-1}{2}} \qquad p = 4k+1$

$p \equiv 1 \pmod 4$

$\left.\begin{matrix} p \equiv 1 \pmod 3 \\ p \equiv 1 \pmod 4 \end{matrix}\right\} p \equiv 1 \pmod{12}$

II) $p \equiv 2 \pmod 3$

$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1) = (-1)^{\frac{p-1}{2}} \qquad p = 4k+3$

$p \equiv 3 \pmod 4$

$p \equiv 2 \pmod 3 \qquad (3,4) = 1$

$p \equiv 3 \pmod 4 \qquad$ KIN TEOREM:

$4 = 1 \cdot 3 + 1 \qquad 4 - 1 \cdot 3 = 1$

$p \equiv 2 \cdot 4 \cdot 1 - 3 \cdot 3 \pmod{12}$

$p \equiv -1 \pmod{12}$

$p \equiv 11 \pmod{12}$

NAPOMENA !

$$X \equiv a_1 \pmod{m_1}$$
$$X \equiv a_2 \pmod{m_2}$$

Euklid: $um_1 + vm_2 = 1$

$$X = um_1 a_2 + vm_2 a_1 \pmod{m_1 m_2}$$

$\cancel{p \equiv 0 \pmod{12}}$

$\boxed{p \equiv 1 \pmod{12}}$ ✓

$\cancel{p \equiv 2 \pmod{12}}$

$\cancel{p \equiv 3 \pmod{12}}$

$\cancel{p \equiv 4 \pmod{12}}$

$p \equiv 5 \pmod{12} \to ?$

$\cancel{p \equiv 6 \pmod{12}}$

$p \equiv 7 \pmod{12} \to ?$

$\cancel{p \equiv 8 \pmod{12}}$

$\cancel{p \equiv 9 \pmod{12}}$

$\cancel{p \equiv 10 \pmod{12}}$

$\boxed{p \equiv 11 \pmod{12}}$ ✓

$p \equiv 5 \pmod{12} \Rightarrow p \equiv 2 \pmod 3 \Rightarrow \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$

$\Rightarrow \frac{p-1}{2} \in 2\mathbb{N}$ $\Rightarrow \left(\frac{3}{p}\right) = -1$ *

$p \equiv 7 \pmod{12} \Rightarrow p \equiv 1 \pmod 3 \Rightarrow \left(\frac{p}{3}\right) = 1 \Rightarrow \left(\frac{3}{p}\right) = -1$

$\Rightarrow \frac{p-1}{2} \in 2\mathbb{N} - 1$

$$\left(\frac{3}{p}\right) = \begin{cases} 0, & p = 3 \\ 1, & p = 1, 11 \pmod{12} \\ -1, & p = 5, 7 \pmod{12} \end{cases}$$

~~ZADATAK~~ Odredite sve neparne proste brojeve tako da

$x^2 + 20 \equiv 0 \pmod p$ ima rješenje

$x^2 \equiv -20 \pmod p$

$\left(\frac{-20}{p}\right) = 1$

$\boxed{\left(\frac{-20}{p}\right) = 0 \quad p \mid -20 \quad p = 5}$

$-20 = -1 \cdot 4 \cdot 5$

$$\left(\frac{-20}{p}\right) = \underbrace{\left(\frac{-1}{p}\right)}_{(-1)^{\frac{p-1}{2}}} \underbrace{\left(\frac{-2^2}{p}\right)}_{1} \left(\frac{5}{p}\right) = 1 \quad *$$

NAPOMENA!

$\left(\frac{a^2}{p}\right) = 1 \quad (a,p) = 1$

- odredimo $\left(\frac{5}{p}\right)$ za sve neparne proste brojeve $\neq 5$

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

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

$p \equiv 1 \pmod 5 \longrightarrow \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$ ▲

1^* $\begin{cases} p \equiv 2 \pmod 5 \longrightarrow \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1 \\ p \equiv 3 \pmod 5 \longrightarrow \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \end{cases}$

$p \equiv 4 \pmod 5 \longrightarrow \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$ ▲

$* \quad \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right) = 1$

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

$1^\circ \quad \left(\frac{-1}{p}\right) = 1 \qquad \left(\frac{5}{p}\right) = 1$

$p \equiv 1 \pmod 4 \qquad p \equiv 1, 4 \pmod 5$ ▲

I) $\left.\begin{array}{l} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 5 \end{array}\right\} p \equiv 1 \pmod{20}$

II) $p \equiv 1 \pmod 4$

$p \equiv 4 \pmod 5$

KIN TEOREM $\rightarrow$ $5 = 1 \cdot 4 + 1$

$5 - 1 \cdot 4 = 1$

$p \equiv \underbrace{5 \cdot 1 \cdot 1 + 4 \cdot 4 \cdot (-1)}_{-11} \pmod{20}$

$p \equiv 9 \pmod{20}$

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

$\downarrow$ $\downarrow 1^*$

$p \equiv 3 \pmod 4$ $p \equiv 2, 3 \pmod 5$

I) $p \equiv 3 \pmod 4$

$p \equiv 2 \pmod 5$

II) $\left.\begin{array}{l} p \equiv 3 \pmod 4 \\ p \equiv 3 \pmod 5 \end{array}\right\} p \equiv 3 \pmod{20}$

KIN.: $5 = 1 \cdot 4 + 1$

$5 - 1 \cdot 4 = 1$

$p \equiv 15 - 8 \pmod{20}$

$p \equiv 7 \pmod{20}$

Rj: $p \equiv 1, 3, 7, 9 \pmod{20}$

$p = 5$

$\left(\frac{a}{p}\right) = 1 \Rightarrow x^2 \equiv a \pmod p$

PROPOZICIJA 1.39. $p \equiv 3 \pmod 4$ onda je $x = a^{\frac{p+1}{4}}$ rješenje kongruencije $x^2 \equiv a \pmod p$

DOKAZ: $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ Eulerov kriterij

$$x^2 \equiv \left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \cdot 1 \equiv a \pmod p$$

PROPOZICIJA 1.40. $p \equiv 5 \pmod 8$

jedan od brojeva $a^{\frac{p+3}{8}}$ i $2^{\frac{p-1}{4}} \cdot a^{\frac{p+3}{8}}$ rješenje kongruencije $x^2 \equiv a \pmod p$

$$p = 8k+5 \overset{E.K.}{\Longrightarrow} a^{\frac{p-1}{2}} \equiv a^{4k+2} \equiv 1 \pmod p$$

$$(a^{2k+1})^2 \equiv 1 \pmod p$$

$$a^{2k+1} \equiv \pm 1 \pmod p$$

$$a^{2k+2} \equiv \pm a \pmod p$$

Ako imamo $+$ $\rightarrow$ $x \equiv a^{k+1} = a^{\frac{p+3}{8}}$

je rješenje kongruencije

Ako imamo $-$ $\rightarrow$ $\left(\frac{2}{p}\right) = -1$

$$2^{\frac{p-1}{2}} \equiv 2^{4k+2} \overset{E.K.}{\equiv} -1 \pmod p$$

$$x \equiv 2^{\frac{p-1}{4}} \cdot a^{\frac{p+3}{8}}$$

$$x^2 \equiv 2^{\frac{p-1}{2}} \cdot a^{\frac{p+3}{4}} \equiv 2^{4k+2} \cdot a^{2k+2} \equiv (-1)(-a) \equiv a \pmod p$$

$p \equiv 1 \pmod 8$

Tonelijev algoritam

1.4. DIOFANTSKE JEDNADŽBE

$ax+by=c$ – lin. diof. jedn.

TM. 1.41. $a,b,c \in \mathbb{Z}$ $\quad d=(a,b)$

(1) Ako $d \nmid c \Rightarrow ax+by=c$ nema rj.

(2) Ako $d \mid c$ onda $ax+by=c$ ima beskonačno rj.

Ako je (x_1, y_1) jedno rješenje onda su sva rješenja dana sa

$$x = x_1 + \frac{b}{d}\cdot t \qquad t\in\mathbb{Z}$$
$$y = y_1 - \frac{a}{d}\cdot t$$

Ako $ax+by=c$ ima rješenja onda $d \mid c$

$$\Downarrow$$

$$ax \equiv c \pmod{b}$$

x_1 neko rješenje

$$x \equiv x_1 + \frac{b}{d}\cdot k \pmod{b} \qquad k=0,1,\ldots,d-1$$

$$x = x_1 + \frac{b}{d}\cdot t, \quad t\in\mathbb{Z}$$

$$by = c-ax = c-a\left(x_1+\frac{b}{d}\cdot t\right) = \underbrace{c-ax_1}_{by_1} - \frac{ab}{d}\cdot t \quad /\cdot b$$

$$= by_1 - \frac{ab}{d}\cdot t$$

$$y = y_1 - \frac{a}{d}\cdot t$$

DEFINICIJA 1.19. PITAGORINA TROJKA $(x,y,z) \in \mathbb{N}^3$

$$x^2+y^2=z^2$$

x,y,z relativno prosti

↳ primitivna Pitagorina trojka

$3^2+4^2=5^2$ $/\cdot 2$ ili $/\cdot 5$

$6^2+8^2=10^2$

(3,4,5)

↳ prim. Pit. trojka

$15^2+20^2=25^2$ (beskonačno mnogo)

$\vdots$

VAŽNO!!! U bilo kojoj prim. Pit. trojki točno jedan od x,y je paran a drugi je neparan!

DOKAZ:

$\Rightarrow$ $x,y \in 2\mathbb{N}$ $\rightarrow$ $z \in 2\mathbb{N}$ $\rightarrow$ nije primitivno (svi su parni)

$\Rightarrow$ $x,y \in 2\mathbb{N}-1$

$$\left.\begin{aligned} x^2 &\equiv 1 \pmod 4 \\ y^2 &\equiv 1 \pmod 4 \end{aligned}\right\} +$$

$$\overline{z^2 \equiv 2 \pmod 4}$$

kontradikcija

TM. 1.42. Sve primitivne Pitagorine trojke (x,y,z) u kojima je y paran, dane su formulama:

$$x=m^2-n^2, \quad y=2mn, \quad z=m^2+n^2$$

$m>n$, $(m,n)=1$

↳ različite parnosti

DOKAZ: $x^2+y^2=z^2$ $\qquad (z+x) = (z-x)+2x$

$$y^2 = z^2-x^2 = (z-x)(z+x)$$

$$y=2c$$

$$z+x=2a, \quad z-x=2b$$

$$4c^2 = 2a2b \Rightarrow c^2 = ab \Rightarrow a=m^2,\ b=n^2$$

$$z=a+b \qquad x=a-b \quad \Rightarrow \quad (a,b)=1 \longrightarrow \text{da nisu } \underbrace{d|z \quad d|x}_{d|y}$$

$$\Rightarrow z=m^2+n^2 \qquad y^2=(m^2+n^2)^2-(m^2-n^2)^2$$

$$x=m^2-n^2 \qquad\qquad = 4m^2n^2$$

$$y=2mn$$

m,n različite parnosti

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

Dokazati da su x,y,z relativno prosti

pretp. $(x,z)=d>1$

$$\left.\begin{array}{l} d\,|\,x+z = d\,|\,2m^2 \\ d\,|\,x+z = d\,|\,2n^2 \end{array}\right\} \Rightarrow \begin{array}{c}\text{BSO } d\\ \text{prost}\end{array} \Rightarrow \begin{array}{l} d|m \\ d|n \end{array} \Rightarrow \Leftarrow$$

→ sve Pitagorine trojke

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

VAŽNO !!!

(1) neparan broj k se može prikazati kao:

$k = m^2 + n^2 \quad (m,n) = 1 \iff$ svaki prosti faktor p od k vrijedi:

$p \equiv 1 \pmod 4$

(2) bilo koji prirodni broj k

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

(3) Ne postoji Pitagorin trokut sa stranicom duljine 1

$x^2 + y^2 = 1^2 \qquad z^2 - x^2 = 1 \qquad \left.\begin{array}{l} z - x = 1 \\ z + x = 1 \end{array}\right\} \Rightarrow x = 0$

$1^2 + y^2 = z^2 \qquad (z-x)(z+x) = 1 \qquad \Rightarrow \Leftarrow$

$\boxed{\text{PR. 1.28.}}$ Odredite sve Pitagorine trokute kojima je jedna stranica a) 39 b) 2003

$1^\circ \quad d = 1$

$m^2 + n^2 = 39 \qquad m^2 - n^2 = 39$

$= 3 \cdot 13$

$\not\equiv 1 \pmod 4$

nema rješenja

$m^2 - n^2 = (m-n)(m+n) = 1 \cdot 39 = 3 \cdot 13$

$\left.\begin{array}{l} m - n = 1 \\ m + n = 39 \end{array}\right\} \qquad \left.\begin{array}{l} m - n = 3 \\ m + n = 13 \end{array}\right\}$

$m = 20 \quad n = 19 \qquad m = 8,\ n = 5$

$d(m^2 - n^2),\ 2dmn,\ d(m^2 + n^2) \longrightarrow (39, 760, 761),\ (39, 80, 89)$

2° $d=3$

$m^2+n^2=13$

$13 \equiv 1 \pmod 4$

$m=3,\ n=2 \quad [m>n]$

$(15, 36, 39)$

$m^2-n^2=13$

$(m-n)(m+n)=13\cdot 1$

$m-n=1$

$m+n=13$

$m=7,\ n=6,\ d=3$

$(39, 252, 255)$

3° $d=13 \quad m^2+n^2=3$

nema rješenja

$m^2-n^2=3$

$(m-n)(m+n)=1\cdot 3$

$m-n=1$

$m+n=3$

$m=2 \quad n=1$

$(39, 52, 65)$

b) $d \mid 2003$

↳ prost broj

$d=1,\ \cancel{d=2003}$

$m^2+n^2=2003$

$2003 \equiv 3 \pmod 4$

nema rješenja

$m^2-n^2=2003$

$(m+n)(m-n)=2003$

$m-n=1$

$m+n=2003$

$m=1002,\ n=1001$

$(2003, 2006004, 2006035)$

VELIKI FERMATOV TEOREM

Jedn. $x^n + y^n = z^n$ nema rješenja u cijelim brojevima za $n \geq 3$

ZADATAK Pitagorini trokuti str. 99

$d \mid 99$ $\quad d = 1, 3, 9, 11, 33, 99$

1° $d = 1$

$m^2 + n^2 = 99$

nema rješenja

$m^2 - n^2 = 99$

$(m-n)(m+n) = 1 \cdot 99 = \cancel{3 \cdot 33} = 9 \cdot 11$

!!! (m,n) rel. prosti

$m+n$ rel. prosti

$m-n$ rel. prosti

$m - n = 1$

$m + n = 99$

$m = 50$

$n = 49$

$(99, 4900, 4901)$

$m - n = 9$

$m + n = 11$

$m = 10$

$n = 1$

$(99, 20, 101)$

2° $d = 3$

$m^2 + n^2 = 33$

nema rješenja

$m^2 - n^2 = 33 = 1 \cdot 33 = 3 \cdot 11$

$m - n = 1$

$m + n = 33$

$(99, 1632, 1635)$

$m - n = 3$

$m + n = 11$

$(99, 168, 195)$

3° $d = 9$

$m^2 + n^2 = 11$

$m^2 - n^2 = 1 \cdot 11$

$(99, 540, 549)$

$d = 11$ $\quad m^2 + n^2 = 9$ $\quad m^2 - n^2 = 9$

nema rješenja

$(m-n)(m+n) = 9 \cdot 1$

$m + n = 9$

$m - n = 1$

$(99, 440, 451)$

$d = 33$ $\quad m^2 + n^2 = 3$ $\quad m^2 - n^2 = 3 = 1 \cdot 3$

nema rješenja

$(m-n)(m+n) = 1 \cdot 3$

$(99, 132, 165)$

Powered by Marija Mia