1. Nađite sve Pitagorine trokute kojima je jedna stranica jednaka

   a) 15;
   b) 20;
   c) 29;
   d) 38.

2. Odredite razvoj u jednostavni verižni razlomak broja

   a) $\frac{51}{97}$;
   b) $\frac{101}{31}$;
   c) $\frac{58}{269}$.

3. Odredite razvoj u jednostavni verižni razlomak broja

   a) $\sqrt{23}$;
   b) $\sqrt{47}$;
   c) $\sqrt{57}$.

4. Nađite najmanje rješenje u prirodnim brojevima Pellove jednadžbe $x^2 - 71y^2 = 1$.

5. Nađite sva rješenja Pellove jednadžbe $x^2 - 146y^2 = 1$ za koja vrijedi $1 < x < 100000$.

6. Neka je X skup svih funkcija $f : S \to G$ sa skupa S u grupu $(G, \cdot)$. Na X je definirana binarna operacija $*$ na sljedeći način:

   $$(f * g)(s) = f(s) \cdot g(s), \quad f, g \in X,\ s \in S.$$

   Dokažite da je $(X, *)$ grupa.

7. Odredite red

   a) elementa i u grupi $(\mathbb{C}^*, \cdot)$;
   b) elementa 4 u grupi $(\mathbb{Z}_6, +_6)$;
   c) elementa 4 u grupi $(\mathbb{Z}_7, +_7)$;
   d) elementa 4 u grupi $(\mathbb{Z}_7^*, \cdot_7)$.

8. Neka je H normalna podgrupa grupe G i neka su $a, b \in G$. Dokažite da vrijedi:

   $$ab \in H \iff ba \in H.$$

9. Jesu li grupe $(\mathbb{Z}, +)$ i $(2\mathbb{Z}, +)$ izomorfne?

10. Jesu li grupe $\mathbb{Z}_{12}$ i $\mathbb{Z}_2 \times \mathbb{Z}_6$ izomorfne?

11. Neka je $(\mathbb{Q}^*, \cdot)$ multiplikativna grupa racionalnih brojeva različitih od nule, te neka je $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$ preslikavanje zadano sa $\varphi(x) = x^2$. Dokažite da je φ homomorfizam grupa, te odredite jezgru $\operatorname{Ker}\varphi$ i sliku $\operatorname{Im}\varphi$.

12. Dokažite da brojevi oblika $a + b\sqrt{5}$, $a, b \in \mathbb{Q}$, uz uobičajeno zbrajanje i množenje, čine polje. Odredite inverz, obzirom na množenje, elementa $x = 2 - 3\sqrt{5}$. Je li to polje izomorfno polju racionalnih brojeva $(\mathbb{Q}, +, \cdot)$?

13. Dokažite da matrice oblika $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$, gdje su a i b racionalni brojevi, uz uobičajeno zbrajanje i množenje matrica, čine polje.

14. Dokažite da je polinom $g(t) = t^3 + t + 1$ ireducibilan nad $\mathbb{Z}_2$. Nađite jedan generator multiplikativne grupe $\mathbb{F}_8^*$ polja $\mathbb{F}_8$ reprezentiranog kao $\mathbb{Z}_2[x]/(g(t))$. Odredite inverz elementa $a = t + 1$ u $\mathbb{F}_8^*$.

1. Nađi sve Pitagorine trojke kojima je stranica jednaka:

a) 15

15 ⇒ 1, 3, 5, 15

$\boxed{d = 1, 3, 5}$

samo za neparne

$d=1$ $m^2+n^2 \neq 15$ $(15 \bmod 4 \neq 1)$

$m^2-n^2=15$

$(m-n)(m+n)=15$

$\begin{cases} m-n=1 \\ m+n=15 \end{cases}$ ili $\begin{cases} m-n=3 \\ m+n=5 \end{cases}$

$m=8$, $n=7$ ⇓ $m=4$, $n=1$

$x=d(m^2-n^2)$

$y=2dmn$

$z=d(m^2+n^2)$

⇓

$x=15$, $y=112$, $z=113$ ⇓ $\boxed{(15,112,113)}$

$x=15$, $y=8$, $z=17$ ⇓ $\boxed{(15,8,17)}$

$d=3$ $m^2+n^2=5$ ili $m^2-n^2=5$

$m^2+n^2=5$ ⇓ $m=2, n=1$ ⇓ $x=9$, $y=12$, $z=15$ ⇓ $\boxed{(9,12,15)}$

$m^2-n^2=5$ ⇓ $(m-n)(m+n)=1\cdot 5$

$m-n=1$

$m+n=5$

$m=3, n=2$ ⇓ $x=15$, $y=36$, $z=49$ ⇓ $\boxed{(15,36,49)}$

$d=5$ $m^2+n^2 \neq 3$ / $m^2-n^2=3$

$m=2, n=1$

⇓

$x=15$

$y=20$

$z=25$

$\boxed{(15,20,25)}$

1. b) $20 \Rightarrow 1, 2, 4, 5, 10, 20$

$d = 1, 5$

$d = 1$

$m^2 + n^2 = 20$

$m = 4, n = 2$

$\Downarrow$

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

$m^2 - n^2 = 20$

$(m-n)(m+n) = 2 \cdot 10$

$m - n = 2$

$m + n = 10$

$m = 6, n = 4$

$\Downarrow$

$\boxed{(20, 48, 52)}$

$2mn = 20$

$m = 10, n = 1$

$m = 2, n = 5$

$\Downarrow$

$(99, 20, 101)$

$(21, 20, 29)$

$d = 5$

$m^2 + n^2 = 4$

$m = 2, n = 1$

$\downarrow$

$\boxed{(15, 20, 25)}$

$m^2 - n^2 = 4$

$(m-n)(m+n) = 4 \cdot 1$

$m - n = 1$

$m + n = 4$

$2mn = 4$

$m = 2, n = 1$

1_b

2. Odredite razvoj u jednostavni verižni razlomak broja:

a) $\frac{51}{97}$

$$97 = 51 \cdot 1 + 46$$
$$51 = 46 \cdot 1 + 5$$
$$46 = 5 \cdot 9 + 1$$
$$5 = 1 \cdot 5$$

$$\Rightarrow \frac{97}{51} = [1; 1, 9, 5] \Rightarrow \frac{51}{97} = [0; 1, 1, 9, 5]$$

b) $\frac{101}{31}$

$$101 = 31 \cdot 3 + 8$$
$$31 = 8 \cdot 3 + 7$$
$$8 = 7 \cdot 1 + 1$$
$$7 = 1 \cdot 7$$

$$\Rightarrow \frac{101}{31} = [3; 3, 1, 7]$$

c) $\frac{58}{269}$

$$269 = 58 \cdot 4 + 37$$
$$58 = 37 \cdot 1 + 21$$
$$37 = 21 \cdot 1 + 16$$
$$21 = 16 \cdot 1 + 5$$
$$16 = 5 \cdot 3 + 1$$
$$5 = 1 \cdot 5$$

$$\Rightarrow \frac{269}{58} = [4; 1, 1, 1, 3, 5] \Rightarrow \frac{58}{269} = [0; 4, 1, 1, 1, 3, 5]$$

3. Odredite razvoj u jednostavni verižni razlomak broja:

a) $\sqrt{23}$ $\quad a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor, \; s_{i+1} = a_i t_i - s_i, \; t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, \; a_0 = \lfloor \sqrt{d} \rfloor$

$s_0 = 0, \; t_0 = 1, \; a_0 = 4$

$s_1 = a_0 t_0 - s_0 = 4, \; t_1 = \frac{23 - 4^2}{1} = 7, \; a_1 = \left\lfloor \frac{4+4}{7} \right\rfloor = 1$

$s_2 = a_1 t_1 - s_1 = 3, \; t_2 = \frac{23 - 3^2}{7} = 2, \; a_2 = \left\lfloor \frac{3+4}{2} \right\rfloor = 3$

$s_3 = 3, \; t_3 = \frac{23 - 9}{2} = 7, \; a_3 = \left\lfloor \frac{3+4}{7} \right\rfloor = 1$

$s_4 = 4, \; t_4 = \frac{23 - 4^2}{7} = 1, \; a_4 = \left\lfloor \frac{4+4}{1} \right\rfloor = 8$

$s_5 = 4, \; t_5 = \frac{23 - 4^2}{1} = 7 \Rightarrow (s_5, t_5) = (s_1, t_1)$

$$\sqrt{23} = [4; \overline{1, 3, 1, 8}]$$

b) $\sqrt{47}$

$s_0 = 0, \; t_0 = 1, \; a_0 = 6$

$s_1 = 6, \; t_1 = 11, \; a_1 = 1$

$s_2 = 5, \; t_2 = 2, \; a_2 = 5$

$s_3 = 5, \; t_3 = 11, \; a_3 = 1$

$s_4 = 6, \; t_4 = 1, \; a_4 = 12$

$s_5 = 6, \; t_5 = 11 \Rightarrow (s_5, t_5) = (s_1, t_1)$

$$\sqrt{47} = [6; \overline{1, 5, 1, 12}]$$

4. Nađite najmanje rješenje u prirodnim brojevima Pellove jednadžbe $x^2-71y^2=1$.

$\sqrt{71}$

$s_0=0,\ t_0=1,\ a_0=8$

$s_1=8,\ t_1=7,\ a_1=2$

$s_2=6,\ t_2=5,\ a_2=2$

$s_3=4,\ t_3=11,\ a_3=1$

$s_4=7,\ t_4=2,\ a_4=7$

$s_5=7,\ t_5=11,\ a_5=1$

$s_6=4,\ t_6=5,\ a_6=2$

$s_7=6,\ t_7=7,\ a_7=2$

$s_8=8,\ t_8=1,\ a_8=16$

$s_9=8,\ t_9=7$

$\Rightarrow \sqrt{71}=[8;\overline{2,2,1,7,1,2,2,16}]$

$\Rightarrow l=8 \Rightarrow$ paran $\Rightarrow (x,y)=(p_{nl-1}, q_{nl-1})$

$\Rightarrow$ najmanje $(x,y)=(p_{l-1}, q_{l-1})=(p_7, q_7)$

n	-1	0	1	2	3	4	5	6	7
a_n		8	2	2	1	7	1	2	2
p_n	1	8	17	42	59	455	514	1483	3480
q_n	0	1	2	5	7	54	61	176	413

$\Rightarrow (3480, 413)$ ✓

* l paran $\Rightarrow x^2-dy^2=-1$ nema rj.

$\Rightarrow x^2-dy^2=1 \Rightarrow (x,y)=(p_{nl-1}, q_{nl-1})$

l neparan $\Rightarrow x^2-dy^2=-1 \Rightarrow (x,y)=(p_{(2n-1)l-1}, q_{(2n-1)l-1})$

$x^2-dy^2=1 \Rightarrow (x,y)=(p_{2nl-1}, q_{2nl-1})$

5. Nađite **sva** rješenja Pellove jednadžbe $x^2 - 146y^2 = 1$ za koja vrijedi $1 < x < 100\,000$.

$\sqrt{146}$

$s_0 = 0,\ t_0 = 1,\ a_0 = 12$

$s_1 = 12,\ t_1 = 2,\ a_1 = 12$

$s_2 = 12,\ t_2 = 1,\ a_2 = 24$

$s_3 = 12,\ t_3 = 2$ —

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

$\Rightarrow l = 2 \Rightarrow$ paran $= (x, y) = (\underline{p_{nl-1}}, \underline{q_{nl-1}})$

n	-1	0	1	2	3	4
a_n		12	12	24	12	24
p_n	1	12	145	3492	42 049	~~1012668~~
q_n	0	1	12	289	3480	83 809

$\Rightarrow (145, 12),\ (42\,049, 3480)$

7. Odredi red:

a) elementa i u grupi $(\mathbb{C}^*, \cdot)$

$\Rightarrow$ red od i je 4 jer je $i^4 = 1$ što je neutralni element za množenje

b) el. 4 u grupi $(\mathbb{Z}_6, +_6)$

$\Rightarrow$ red od 4 je 3 jer je $4+4+4=12$, a $12 \equiv 0 \pmod 6$, a nula je neutralni el. za zbrajanje

c) el. 4 u grupi $(\mathbb{Z}_7, +_7)$

$\Rightarrow$ red od 4 je 7 jer je $4+4+\dots+4$ $(4 \cdot 7) = 28 \equiv 0 \pmod 7$

d) el. 4 u grupi $(\mathbb{Z}_7^*, \cdot_7)$

$\Rightarrow$ red od 4 je 3 jer je $4 \cdot 4 \cdot 4 = 64 \equiv 1 \pmod 7$, a jedan je neutralni za množ.

9. Jesu li grupe $(\mathbb{Z}, +)$ i $(2\mathbb{Z}, +)$ izomorfne?

$\Rightarrow$ nać fju koja će sve el. iz $\mathbb{Z}$ preslikat u $2\mathbb{Z}$ tako da svakog pogodi točno jednom.

$\Rightarrow f(x) = 2x$

$\Rightarrow$ dokazat s obzirom na zbrajanje $(+,+)$

$f(x) = 2x$

$f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$

10. Jesu li grupe $\mathbb{Z}_{12}$ i $\mathbb{Z}_2 \times \mathbb{Z}_6$ izomorfne?

$0 \times 0 \rightarrow (0,0)$

$1 \times 1 \rightarrow (1,1)$

$2 \times 2 \rightarrow (0,2)$

$3 \times 3 \rightarrow (1,3)$

$4 \times 4 \rightarrow (0,4)$

$5 \times 5 \rightarrow (1,5)$

$6 \times 6 \rightarrow (0,0)$

$\left.\begin{array}{l} f(0) = (0,0) \\ f(6) = (0,0) \end{array}\right\} \Rightarrow$ nije injekcija

$\Rightarrow$ nisu izomorfne

11. Neka je $(\mathbb{Q}^*, \cdot)$ multiplikativna grupa rac. br. različitih od nule, te neka je $\rho: \mathbb{Q}^* \rightarrow \mathbb{Q}^*$ preslikavanje zadano sa $\rho(x) = x^2$. Dokažite da je ρ homomorfizam grupa, te odredite jezgru $\mathrm{Ker}\, \rho$ i sliku $\mathrm{Im}\, \rho$

$\rho(x) = x^2$, množenje $(\cdot, \cdot)$

$\Rightarrow f(x) = x^2$

$f(xy) = (xy)^2 = x^2 y^2 = f(x) f(y)$

$\mathrm{Ker}\, \rho \Rightarrow$ element koji provučen kroz fju daje neutralni element za danu operaciju (ovdje 1)

$\Rightarrow$ za x^2 su to 1 i -1

$\mathrm{Ker}\, \rho = \{1, -1\}$

$\mathrm{Im}\, \rho = x^2$

7, 9, 10, 11

8. Neka je H normalna podgrupa grupe G i neka su $a, b \in G$.
Dokaži:

$ab \in H \Leftrightarrow ba \in H$ $\quad$ $b \cdot / \, ab \in H \Rightarrow bab \in \underset{(xY = Yx, \forall x \in G)}{bH} \Rightarrow bab \in Hb / \cdot b^{-1} \Rightarrow ba \in H$ obrat analogno

12. Dokažite da brojevi oblika $a + b\sqrt{5}$, $a, b \in \mathbb{Q}$, uz uobičajeno zbrajanje i množenje, čine polje. Odredite inverz, s obzirom na množ., elementa $x = 2 - 3\sqrt{5}$. Je li to polje izomorfno polju racionalnih brojeva $(\mathbb{Q}, +, \cdot)$?

$\Rightarrow$ ako kaže zbr. onda oduzimamo, ako množ. onda dijelimo

$P = \{a + b\sqrt{5} ; a, b \in \mathbb{Q}\}$

$(a + b\sqrt{5}) - (c + d\sqrt{5}) \Rightarrow (a - c) + (b - d)\sqrt{5} \in P \Rightarrow (P, +)$ abelova grupa

$(a + b\sqrt{5}) / (c + d\sqrt{5}) \ldots \Rightarrow \frac{ac - 5bd}{c^2 - 5d^2} + \frac{bc - ad}{c^2 - 5d^2}\sqrt{5} \in P$, $\{P \setminus \{0\}, \cdot\}$ abelova grupa

Nisu izomorfni. Pretpostavimo $f : P \to \mathbb{Q}$ je izomorfizam

$f(1) = 1$; $f(3) = f(1 + 1 + 1) = f(1) + f(1) + f(1) = 3$

Neka je $f(\sqrt{3}) = a \in \mathbb{Q}$. Tada je $3 = f(3) = f(\sqrt{3} \cdot \sqrt{3}) = a^2$ slijedi da je $\sqrt{3}$ racionalan broj, što je kontradikcija.

13. Dokažite da matrice oblika $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$, a, b racionalni, uz uobičajeno zbrajanje i množ., čine polje.

$\Rightarrow$ množenje $\Rightarrow$ množenje
zbrajanje $\Rightarrow$ oduzimanje

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} - \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} a - c & (b - d) \\ 2(b - d) & a - c \end{bmatrix} \in H$$

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} ac + 2bd & bc + ad \\ 2(bc + ad) & ac + 2bd \end{bmatrix} \in H$$

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}^{-1} = \frac{1}{a^2 - 2b^2} \begin{bmatrix} a & -b \\ -2b & a \end{bmatrix} \in H$$

8, 12, 13