Raziskovalna naloga

PITAGOREJSKE PETERICE

Avtorja: Rok Jurinčič in Patrik Mikuž

Mentor: mag. Alojz Grahor, prof. mat.

Področje: SŠ Matematika

April, 2018

Škofijska gimnazija Vipava

Zahvala

Zahvaljujeva se profesorjem Škofijske gimnazije Vipava:

- mentorju mag. Alojzu Grahorju za spodbude in usmerjanje pri izdelavi raziskovalne naloge ter za pomoč pri iskanju virov in

- prof. Sonji Matelič za pregled prevoda povzetka v angleščino.

Povzetek

Pitagorejska peterica je peterica števil (a, b, c, d, e), ki ustrezajo enačbi $a^2 + b^2 + c^2 + d^2 = e^2$. Kadar so števila $a, b, c, d\ in\ e$ naravna števila, imenujemo peterico naravna pitagorejska peterica (na primer (24,887,1520,512,1833)), če pa so $a, b, c, d\ in\ e$ cela števila, jo imenujemo cela pitagorejska peterica (na primer (-2,10,-11,20,25)).

V prvem delu raziskovalne naloge smo odkrili več različnih parametrizacij naravnih pitagorejskih peteric. Pri kreiranju nekaterih izmed njih smo uporabili analogijo s parametrizacijo pitagorejskih trojic in četveric. S pomočjo izbire parametrov dobimo pitagorejsko peterico, zato parametrizaciji pravimo tudi generator pitagorejske peterice. Odkrili smo tudi generator, ki generira vse pitagorejske peterice in to tudi dokazali.

V drugem delu raziskovalne naloge smo v množici celih pitagorejskih peteric definirali množenje s predpisom:

$$(a, b, c, d, e) \circ (\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{s}, \mathrm{t}) = (\mathrm{ap} - \mathrm{bq} - \mathrm{cr} - \mathrm{ds}, \mathrm{aq} + \mathrm{bp} + \mathrm{cs} - \mathrm{dr}, \mathrm{ar} - \mathrm{bs} + \mathrm{cp} + \mathrm{dq}, \mathrm{as} + \mathrm{br} - \mathrm{cq} + \mathrm{dp}, \mathrm{et}).$$

Dokazali smo, da obstaja enota za množenje ter da je množenje asociativno, ni pa komutativno. V množici neničelnih racionalnih pitagorejskih peteric obstaja k vsakemu elementu inverzni element, tako da je množica neničelnih racionalnih pitagorejskih peteric nekomutativna grupa. Raziskovali smo tudi razstavljanje pitagorejskih peteric. Dokazali smo trditev, da v množici celih pitagorejskih peteric ne velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice, kjer je nerazcepna tista pitagorejska peterica, ki jo ne moremo zapisati kot produkt dveh pitagorejskih peteric. Izrek velja tudi v podmnožici naravnih pitagorejskih peteric.

Ključne besede: Pitagorov izrek, pitagorejske trojice, pitagorejske četverice, pitagorejske peterice, parametrizacija pitagorejskih peteric, množenje pitagorejskih peteric, razstavljanje pitagorejskih peteric

Abstract

The Pythagorean quintuple is a quintuple of numbers (a, b, c, d, e) corresponding to the equation $a^2 + b^2 + c^2 + d^2 = e^2$. When the numbers are natural numbers, they are named a natural Pythagorean quintuple (for example (24, 887, 1520, 512, 1833)), but if $a, b, c, d\ and\ e$ are integers, it is called the whole Pythagorean quintuple (for example (-2,10, -11,20,25)).

In the first part of the research, several different parametrizations of natural Pythagorean quintuples were discovered. Some of them were created using the analogy of the parameterization of Pythagorean triples and quadruples. Using the parameter selection, a Pythagorean quintuple is obtained, so the generator of Pythagorean pentacles is also called parametrization. The generator that generates all Pythagorean pentacles was discovered and also proved.

In the second part of the research, in the set of the whole Pythagorean quintuple the multiplication was defined by the rule:

$$(a, b, c, d, e) \circ (\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{s}, \mathrm{t}) = (\mathrm{ap} - \mathrm{bq} - \mathrm{cr} - \mathrm{ds}, \mathrm{aq} + \mathrm{bp} + \mathrm{cs} - \mathrm{dr}, \mathrm{ar} - \mathrm{bs} + \mathrm{cp} + \mathrm{dq}, \mathrm{as} + \mathrm{br} - \mathrm{cq} + \mathrm{dp}, \mathrm{et}).$$

It was proved that there is a multiplication unit, and that the multiplication is associative but not commutative. The dismantling of Pythagorean quintuples was also explored. It was proved that in the set of entire Pythagorean quintuples the theorem on a unipolar split is not applicable to the inseparable Pythagorean pentacles, which cannot be written as the product of two Pythagorean quintuples. The theorem does also apply to the subset of natural Pythagorean quintuples.

Key words: Pythagorean Theorem, Pythagorean triples, Pythagorean Quartuples, Pythagorean quintuples, parametrization of Pythagorean quintuples, multiplication of Pythagorean quintuples, dismantling Pythagorean quintuples.

Kazalo

1 UVOD

1.1 OSNOVNE DEFINICIJE

Definicija 1: *Naravna pitagorejska trojica* (a, b, c) je nabor treh naravnih števil a, b, c za katere velja

$$a^2 + b^2 = c^2 \ . \tag{1}$$

Definicija 2: *Naravna pitagorejska* četverica (a, b, c, d) je nabor štirih naravnih števil $a, b, c \ in \ d$, za katere velja

$$a^2 + b^2 + c^2 = d^2. \tag{2}$$

Definicija 3: *Naravna pitagorejska peterica* (a, b, c, d, e) je nabor petih naravnih števil $a, b, c, d \ in \ e$, za katere velja

$$a^2 + b^2 + c^2 + d^2 = e^2. \tag{3}$$

Pitagorejska peterica je *primitivna*, če je $D(a, b, c, d) = 1$, sicer je *neprimitivna.* Za neprimitvno $(a_1, \ b_1, c_1, d_1, e_1)$ pitagorejsko peterico velja, da je večkratnik primitivne pitagorejske peterice (a, b, c, d, e): $(a_1, \ b_1, c_1, d_1, e_1) = k(a, b, c, d, e)$. Analogno velja za pitagorejske trojice in četverice.

Po analogiji s Pitagorovim izrekom imenujemo števila na levi strani enakosti (1), (2) in (3) katete, na desni pa je hipotenuza. Pri trojicah gre za običajni Pitagorov izrek v pravokotnem trikotniku, pri četvericah so katete osnovni robovi kvadra in hipotenuza diagonala kvadra.

Če v gornjih definicijah dopustimo, da so katete cela števila, imenujemo pitagorejsko n-terico (n = 3,4,5) *cela pitagorejska n-terica* (n = 3,4,5), če pa so komponente racionalna števila, dobimo racionalno pitagorejsko peterico.

1.2 OSNOVNE LASTNOSTI

Če je (a, b, c) pitagorejska peterica, potem je tudi (ka, kb, kc, kd, ke) pitagorejska trojica, saj je $(ka)^2 + (kb)^2 + (kc)^2 + (kd)^2 = k^2(a^2 + b^2 + c^2 + d^2) = (ke)^2$. Analogno velja za pitagorejske trojice in četverice.

Poglejmo, katere pitagorejske peterice lahko nastopijo glede na sodost ali lihost katet.

Izrek[1] 1: Naj bo (a, b, c, d, e) naravna pitagorejska peterica. Potem so vsaj tri izmed števil a, b, c in d soda števila ali pa so vsa štiri števila a, b, c in d liha števila.

Dokaz: Pri dokazovanju se bomo sklicevali na ostanke pri deljenju naravnega števila s 4. Če je $n = 2m$ sodo število, potem je ostanek pri deljenju s 4 njegovega kvadrata $n^2 = 4m^2$ enak 0. Če pa je je $n = 2m + 1$, potem je ostanek pri deljenju s 4 njegovega kvadrata $n^2 = 4m^2 + 4m + 1$ enak 1.

Preverimo vse možnosti.

- Vsa števila a, b, c in d so soda števila. V tem primeru je tudi hipotenuza e sodo število. Leva stran enakosti $a^2 + b^2 + c^2 + d^2 = e^2$ ima pri deljenju s 4 ostanek 0, desna tudi. Taka peterica obstaja.
- Natanko tri izmed števil a, b, c in d so soda števila. V tem primeru je hipotenuza e liho število. Leva stran enakosti $a^2 + b^2 + c^2 + d^2 = e^2$ ima pri deljenju s 4 ostanek 1, desna tudi. Taka peterica obstaja.
- Natanko dve izmed števil a, b, c in d sta sodi števili. V tem primeru je hipotenuza e sodo število. Leva stran enakosti $a^2 + b^2 + c^2 + d^2 = e^2$ ima pri deljenju s 4 ostanek 2, desna pa 0. Taka peterica ne obstaja.
- Natanko eno izmed števil a, b, c in d je sodo število. V tem primeru je hipotenuza e liho število. Leva stran enakosti $a^2 + b^2 + c^2 + d^2 = e^2$ ima pri deljenju s 4 ostanek 3, desna pa 1. Taka peterica ne obstaja.
- Vsa števila a, b, c in d so liha števila. V tem primeru je tudi hipotenuza e sodo število. Leva stran enakosti $a^2 + b^2 + c^2 + d^2 = e^2$ ima pri deljenju s 4 ostanek 0, desna tudi. Taka peterica obstaja. QED

[1] V nalogi z *Izreki* označujemo trditve, ki so avtorske.

Pitagorejska trojica (a, b, c) obstaja, kadar je vsaj eno izmed števil a in b sodo število, pitagorejska četverica (a, b, c, d) pa, kadar sta vsaj dve izmed števil a, b in c sodi števili.

V nalogi obravnavamo pitagorejske peterice. Elemente te množice dobimo z računalniškim programom, ki generira vse pitagorejske peterice z določeno lastnostjo (na primer z omejitvijo velikosti katet in hipotenuze ali vse peterice z dano hipotenuzo). Prav tako lahko dobimo pitagorejske peterice s parametrizacijo katet in hipotenuze. V nalogi imenujemo posamezno parametrizacijo *generator*, saj s tem dobimo peterice. Ker smo ideje za generatorje (to je parametrizacijo) dobili tudi iz znanih generatorjev (parametrizacij) pitagorejskih trojic in četveric, v uvodu naštejemo nekaj generatorjev pitagorejskih trojic in četveric. Prvi del naloge vsebuje generatorje pitagorejskih peteric, v drugem delu naloge pa v množici celih pitagorejskih peteric definiramo množenje in raziskujemo lastnosti množenja.

1.3 GENERATORJI PITAGOREJSKIH TROJIC

1.3.1 Prvi generator pitagorejskih trojic (Python)

S pomočjo ustreznega programa lahko enostavno generiramo pitagorejske trojice. Uporabili smo programski jezik Python (glej slilo 1).

```
x = 2
while True:
    for a in range(1,x):
        for b in range(1,x):
            c = x
            if a**2 + b**2 == c**2:
                print "(%(aa)d,%(bb)d,%(cc)d)" % {"aa" : a, "bb" : b, "cc" : c}

    x += 1
```

Slika 1 Program za generiranje pitagorejskih trojic v Pythonu

1.3.2 Drugi generator pitagorejskih trojic

Znana je Evklidova metoda generiranja (parametrizacije) pitagorejskih trojic.

Trditev[2]: Naj bosta m in n naravni števili, $m > n$. Potem števila $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ sestavljajo naravno pitagorejsko trojico (a, b, c).

Primitivno pitagorejsko trojico dobimo, kadar sta m in ni tuji si števili različne parnosti. Z gornjimi formulami dobimo vsako pitagorejsko trojico (Vidav, 1972, str. 145-146).

Do enakega generatorja (enake parametrizacije) pridemo tudi preko kompleksnih števil. Naj bo $\alpha = (m + ni)^2$. Izračunajmo $|\alpha|$ na dva načina.

$$|\alpha| = |(m + ni)^2| = |m + ni|^2 = \left(\sqrt{m^2 + n^2}\right)^2 = m^2 + n^2.$$

$|\alpha| = |(m + ni)^2| = |m^2 - n^2 + 2mni| = \sqrt{(m^2 - n^2)^2 + (2mn)^2}$. Tako imamo

[2] V nalogi pod *Trditvami* navajamo že znana splošna dejstva ali izreke iz literature in ne navajamo dokazov.

$\sqrt{(m^2-n^2)^2+(2mn)^2}=m^2+n^2$ oziroma $(m^2-n^2)^2+(2mn)^2=(m^2+n^2)^2$. S tem smo dokazali, da je $(m^2-n^2, 2mn, m^2+n^2)$ pitagorejska trojica.

1.3.3 Tretji generator pitagorejskih trojic

Znani sta tudi Pitagorova in Platova metoda generiranja pitagorejskih trojic.

Trditev: Naj bo a naravno število. Potem obstajata takšni naravni števili b in c, da je (a, b, c) naravna pitagorejska trojica in sicer:

a) če je število $a \geq 3$ liho število, potem sta $b=\frac{a^2-1}{2}$, $c=\frac{a^2+1}{2}$ (Pitagorova metoda, glej Posamentier, 2010, stran 130).

b) če je število $a \geq 4$ sodo število, potem sta $b=\frac{a^2}{4}-1$, $c=\frac{a^2}{4}+1$ (Platova metoda, glej Posamentier, 2010, stran 131).

1.3.4 Četrti generator pitagorejskih trojic[3]

Trditev: Trojica $\left(m-n, 2\sqrt{mn}, m+n\right)$, $m, n \in N$ je pitagorejska trojica, ko je mn popoln kvadrat.

Utemeljitev: $(m+n)^2=(m-n)^2+4mn$

[3] Te parametrizacije nismo zasledili v nam dostopni literaturi

1.4 GENERATORJI PITAGOREJSKIH ČETVERIC¸

1.4.1 Prvi generator pitagorejskih četveric

Podobno kot pitagorejske trojice lahko poiščemo pitagorejske četverice s pomočjo programskih orodij, na primer s pomočjo programa v Pythonu (glej sliko 2).

```
x = 2
while True:
    for a in range(1,x):
        for b in range(1,x):
            for c in range(1,x):
                d = x
                if a**2 + b**2 + c**2 == d**2:
                    print "(%(aa)d,%(bb)d,%(cc)d,%(dd)d)" % {"aa" : a, "bb" : b, "cc" : c, "dd" : d}

    x += 1
```

Slika 2 Program v Pythonu, ki generira pitagorejske četverice

1.4.2 Drugi generator pitagorejskih četveric

Idejo, ki smo jo uporabili za generiranje pitagorejskih trojic (glej razdelek 1.3.4) nekoliko dopolnimo in dobimo generator pitagorejskih četveric.

Trditev: Naj bosta števili m in n naravni števili ter $2mn$ popolni kvadrat. Tedaj je četverica $(m, \sqrt{2mn}, n, m+n)$ pitagorejska četverica.

Utemeljitev: $(m+n)^2 = m^2 + 2mn + n^2$,

Očitno je, da s tem generatorjem ne dobimo vseh pitagorejskih četveric, temveč le tiste, kjer je število $2mn$ popoln kvadrat.

Ta generator pa lahko nekoliko preoblikujemo. Naj bo $mn = \frac{p^2}{2}$. Očitno mora biti p^2 sodo število, torej je tudi p sodo število. Tako lahko sistematično poiščemo pitagorejske četverke te oblike: izberemo sodo število p in potem vse možne m in n, ki jih dobimo z razcepom $mn = \frac{p^2}{2}$ na dva faktorja.

1.4.3 Tretji generator pitagorejskih četveric

Tudi Platovo in Pitagorovo metodo generiranja pitagorejskih trojic lahko razširimo na generator pitagorejskih četveric.

Trditev: Naj bosta a in b naravni števili različne parnosti ali obe sodi števili. Potem obstajata takšni naravni števili c in d, da je (a, b, c, d) naravna pitagorejska četverka. Če sta števili a in b obe lihi števili, naravna pitagorejska četverka ne obstaja.

a) Če sta števili a in b sta različne parnosti, sta potem $c = \frac{a^2+b^2-1}{2}$, $d = \frac{a^2+b^2+1}{2}$.

b) Če sta števili a in b obe sodi števili, sta potem:
$c = \frac{a^2+b^2}{4}$ -1, $d = \frac{a^2+b^2}{4} + 1$.

c) Števili a in b sta obe lihi števili. Iščemo števili c in d, da bo veljalo

$$a^2 + b^2 + c^2 = d^2.$$

Če je število c liho število, je tudi število d liho. Ostanek pri deljenju leve strani s 4 je enak 3, desne pa 1, kar je protislovje. Če pa je število c sodo število, je število d sodo. Ostanek pri deljenju leve strani s 4 je enak 2, desne pa 0. Spet je protislovje (Sierpinski, 2003, stran 98).

1.4.4 Četrti generator pitagorejskih četveric

Tudi Evklidovo metodo generiranja pitagorejskih trojic lahko razširimo na genrrator pitagorejskih četveric.

Trditev: Naj bodo m, n, p in q naravna števila. Tedaj števila

$$a = m^2 + n^2 - p^2 - q^2$$

$$b = 2(mq + np)$$

$$c = 2(nq - mp)$$

$$d = m^2 + n^2 + p^2 + q^2$$

sestavljajo pitagorejsko četverico (a, b, c, d).

Dokaz:

$$(m^2 + n^2 + p^2 + q^2)^2 = (2mq + 2np)^2 + (2nq - 2mp)^2 + (m^2 + n^2 - p^2 - q^2)^2.$$

(glej vir https://en.wikipedia.org/wiki/Pythagorean_quadruple)

1.4.5 Peti generator pitagorejskih četveric

V viru, dostopnem na naslovu http://mathworld.wolfram.com/PythagoreanQuadruple.html je omenjena parametrizacija pitagorejskih četveric. Idejo smo priredili in sestavili dva generatorja.

Trditev: Naj bodo m, n in p naravna števila. Tedaj števila

$$a = m^2 + n^2 - p^2$$

$$b = 2mp$$

$$c = 2np$$

$$d = m^2 + n^2 + p^2$$

sestavljajo pitagorejsko četverko (a, b, c, d).

Dokaz je preprost.

Trditev: Naj bodo m, n in p naravna števila. Tedaj števila

$$a = m^2 - n^2 - p^2$$

$$b = 2mn$$

$$c = 2mp$$

$$d = m^2 + n^2 + p^2$$

sestavljajo pitagorejsko četverko (a, b, c, d).

Dokaz je preprost.

1.4.6 Šesti generator pitagorejskih četveric

Idejo, opisano v razdelku 1.4.5, smo preoblikovali in dokazali naslednji izrek:

Izrek 2: Naj bodo m, n in p naravna števila. Tedaj števila

$$a = 2m^2$$
$$b = 2mn$$
$$c = n^2$$
$$d = 2m^2 + n^2$$

sestavljajo pitagorejsko četverico (a, b, c, d).

Dokaz: $(2m^2)^2 + (2mn)^2 + (n^2)^2 = (2m^2 + n^2)^2$

QED

1.4.7 Sedmi generator pitagorejskih četveric

Sierpinski (glej Sierpinski, 2003, stran 98) navaja še eno parametrizacijo, ki jo povzemamo tukaj v naslednji trditvi.

Trditev: Če je x liho število, potem za vsako naravno število n sestavljajo števila a,b,c,d pitagorejsko četverico

$$\boldsymbol{a = x}$$

$$\boldsymbol{b = 2n}$$

$$\boldsymbol{c = \frac{x^2 - 1}{2} + 2n^2}$$

$$\boldsymbol{d = \frac{x^2-1}{2} + 2n^2 + 1.}$$

Če je x sodo število, potem za vsako naravno število n sestavljajo števila a, b, c, d pitagorejsko četverico

$$\boldsymbol{a = x}$$

$$\boldsymbol{b = 2n + 1}$$

$$\boldsymbol{c = \frac{x^2}{2} + 2n^2 + 2n}$$

$$\boldsymbol{d = \frac{x^2}{2} + 2n^2 + 2n + 1.}$$

Dokaz je v Sierpinski, 2003, stran 98.

1.4.8 Osmi generator pitagorejskih četveric

Sierpinski navaja generator, ki generira vse pitagorejske četverice (Sierpinski, 2003, stran 102). Na istem mestu je tudi dokaz.

Trditev: Naravna števila a, b, c in d zadoščajo enakosti $a^2 + b^2 + c^2 = d^2$ natanko tedaj, ko obstajajo takšna naravna števila m, n in l, kjer je n delitelj števila $l^2 + m^2$ in manjši od $\sqrt{l^2 + m^2}$ ter

$$a = \frac{l^2+m^2-n^2}{n}.$$

$$b = 2l$$

$$c = 2m$$

$$d = \frac{l^2 + m^2 + n^2}{n}.$$

1.5 CILJI IN METODE DELA

Cilj naloge je raziskovati pitagorejske peterice in sicer:

- odkriti čim več parametrizacij pitagorejskih peteric,
- odkriti parametrizacijo, ki opiše vse pitagorejske peterice,
- v množici celih pitagorejskih peteric definirati množenje in
- preveriti ter dokazati, ali velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice.

Metoda dela, ki smo jo uporabili, je sklepanje in matematično dokazovanje. Pri formulaciji nekaterih izrekov smo si pomagali z analogijo k obstoječim izrekom pri pitagorejskih trojicah in četvericah. Pri preiskovanju in računanju smo uporabljali programski jezik Python.

2 GENERATORJI PITAGOREJSKIH PETERIC

2.1 Prvi generator pitagorejskih peteric

Podobno kot pitagorejske trojice in pitagorejske četverice lahko generiramo s programom. Program za generiranje pitagorejskih četveric smo dopolnili (glej sliko 3). Na sliki 4 je tudi nekaj primerov pitagorejskih peteric.

```
x = 2
while True:
    for a in range(1,x):
        for b in range(1,x):
            for c in range(1,x):
                for d in range(1,x):
                    e = x
                    if a**2 + b**2 + c**2 + d**2 == e**2:
                        print "(%(aa)d,%(bb)d,%(cc)d,%(dd)d,%(ee)d)" % {"aa" : a, "bb" : b, "cc" : c, "dd" : d, "ee" : e}

    x += 1
```

Slika 3 Program v Pythonu, ki generira pitagorejske peterice

```
(1,1,1,1,2)
(2,2,2,2,4)
(1,2,2,4,5)
(1,2,4,2,5)
(1,4,2,2,5)
(2,1,2,4,5)
(2,1,4,2,5)
(2,2,1,4,5)
(2,2,4,1,5)
(2,4,1,2,5)
(2,4,2,1,5)
(4,1,2,2,5)
(4,2,1,2,5)
(4,2,2,1,5)
(27,15,49,3,58)
(27,21,13,45,58)
(27,21,45,13,58)
(27,23,9,45,58)
(27,23,45,9,58)
(27,27,15,41,58)
(27,27,41,15,58)
(27,33,5,39,58)
(27,33,39,5,58)
(27,39,5,33,58)
(27,39,33,5,58)
(27,41,15,27,58)
(27,41,27,15,58)
(27,45,9,23,58)
(4,10,51,98,111)
(4,10,98,51,111)
(4,10,109,18,111)
(4,12,56,95,111)
(4,12,95,56,111)
(4,13,6,110,111)
(4,13,30,106,111)
(4,13,106,30,111)
(4,13,110,6,111)
(4,14,3,110,111)
(4,14,110,3,111)
(4,16,32,105,111)
(4,16,105,32,111)
(4,18,10,109,111)
```

Slika 4 Nekaj primerov pitagorejskih peteric

2.2 Drugi generator pitagorejskih peteric

Do preprostega generatorja pitagorejskih peteric pridemo z uporabo enakosti:

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

Trditev: Naj bosta m in n naravni števili. Potem je peterica naravnih števil $(m, \sqrt{mn}, \sqrt{mn}, n, m+n)$ pitagorejska peterica.

Očitno je, da s tem generatorjem ne dobimo vseh pitagorejskih četverk, temveč le tiste, kjer je število mn popoln kvadrat.

2.3 Tretji generator pitagorejskih peteric

Nekatere pitagorejske peterice lahko dobimo iz naravnih pitagorejskih trojic: Če obstaja med naravnima pitagorejskima trojicama $a^2 + b^2 = x^2$,

$c^2 + d^2 = y^2$ zveza $x^2 + y^2 = e^2$, potem je (a, b, c, d, e) naravna pitagorejska peterica.

Primer: Velja: $24^2 + 32^2 = 40^2$, $21^2 + 72^2 = 75^2$ in $40^2 + 75^2 = 85^2$, torej je $24^2 + 32^2 + 21^2 + 72^2 = 85^2$. Zato je $(21, 24, 32, 72, 85)$ naravna pitagorejska peterica.

Lahko pa naravne peterice generiramo tudi iz naravne pitagorejske trojice in naravne pitagorejske četverice:

Če obstajata naravna pitagorejska četverka $a^2 + b^2 + x^2 = e^2$ in naravna pitagorejska trojica $c^2 + d^2 = x^2$, potem je (a, b, c, d, e) naravna pitagorejska peterica.

Primer 1: Iz $(8, 15, 17)$ in $(2,10,11,15)$ dobimo $(2, 8, 10, 11, 17)$

Primer 2: Iz $(2,10,25,27)$ in $(7, 24, 25)$ dobimo $(2, 7, 10, 24, 27)$

2.4 Četrti generator pitagorejskih peteric

Platovo in Pitagorovo metodo smo razširili tudi ma generator pitagorejskih peteric (glej izrek 3).

Izrek 3: Naj bodo a, b in c naravna števila, med katerimi nista natanko dve lihi in eno sodo število. Potem obstajata takšni naravni števili d in e, da je (a, b, c, d, e) naravna pitagorejska peterka. Če sta med števili a, b in c natanko dve lihi in eno sodo število, potem naravna pitagorejska peterka ne obstaja.

Dokaz:

a) Števila a, b in c so ali vsa tri liha ali natanko eno liho in dve sodi.

Tedaj naj bo $d = \frac{a^2+b^2+c^2-1}{2}$, $e = \frac{a^2+b^2+c^2+1}{2}$.

Izračunajmo:

$$a^2 + b^2 + c^2 + \left(\frac{a^2 + b^2 + c^2 - 1}{2}\right)^2 = \cdots = \left(\frac{a^2 + b^2 + c^2 + 1}{2}\right)^2$$

QED

b) Števila a, b in c so vsa tri soda. V tem primeru vzemimo:

$c = \frac{a^2+b^2+c^2}{4} - 1$, $d = \frac{a^2+b^2+c^2}{4} + 1$.

Preverimo:

$$a^2 + b^2 + c^2 + \left(\frac{a^2 + b^2 + c^2}{4} - 1\right)^2 = \cdots = \left(\frac{a^2 + b^2 + c^2}{4} + 1\right)^2$$

QED

c) Med števili a, b in c sta natanko dve lihi in eno sodo število. Iščemo števili d in e, da bo veljalo

$$a^2 + b^2 + c^2 + d^2 = e^2.$$

Če je d sodo število, je število $a^2 + b^2 + c^2 + d^2$ oblike $4k + 2$, če pa je d liho število, je število $a^2 + b^2 + c^2 + d^2$ oblike $4l + 3$. Desna stran e^2 je oblike $4m + 1$ ali $4n$. V vsakem primeru je protislovje.

QED

Lahko sklepamo tudi takole:

Kvadrat lihega števila je enak $(2k+1)^2 = 4k^2 + 4k + 1$. Torej je ostanek pri deljenju lihega števila s 4 enak 1.
Kvadrat sodega števila je večkratnik števila 4, zato je ostanek pri deljenju s 4 enak 0.
Sklepamo torej, da je ostanek pri deljenju dveh izmed števil a^2, b^2 in c^2 s 4 vedno enak 1, enega izmed njih pa enak 0. Število $a^2 + b^2 + c^2$ ima pri deljenju s 4 ostanek 2. Ostanek pri deljenju števil d^2 in e^2 s 4 pa je bodisi 0 bodisi 1.
Vzemimo najprej, da je d liho število. Tako je ostanek pri deljenju s 4 leve strani enakosti $a^2 + b^2 + c^2 + d^2 = e^2$ enak 3, kar je protislovje.
Če pa je c sodo število, je ostanek pri deljenju s 4 leve strani iste enakosti enak 2, kar je tudi protislovje.

Sklep: Če sta med števili a, b in c natanko dve lihi in eno sodo število, potem naravna pitagorejska peterka ne obstaja. QED

2.5 Peti generator pitagorejskih peteric

Podobno kot smo v izreku 3 sestavili generator pitagorejskih četveric, smo sestavili tudi dva generatorja pitagorejskih peteric (glej izreka 4a in 4b).

Izrek 4. a: Naj bodo m, n, p in q naravna števila. Tedaj števila

$$\boldsymbol{a = m^2 - n^2 - p^2 - q^2}$$
$$\boldsymbol{b = 2mn}$$
$$\boldsymbol{c = 2mp}$$
$$\boldsymbol{d = 2mq}$$
$$\boldsymbol{e = m^2 + n^2 + p^2 + q^2}$$

sestavljajo pitagorejsko peterico (a, b, c, d, e).

Dokaz:

$$(m^2 - n^2 - p^2 - q^2)^2 + (2mn)^2 + (2mp)^2 + (2mq)^2 = \cdots = (m^2 + n^2 + p^2 + q^2)^2$$

QED

Izrek 4. b: Naj bodo m, n, p in q naravna števila. Tedaj števila

$$\boldsymbol{a = m^2 + n^2 + p^2 - q^2}$$
$$\boldsymbol{b = 2mq}$$
$$\boldsymbol{c = 2nq}$$
$$\boldsymbol{d = 2pq}$$
$$\boldsymbol{e = m^2 + n^2 + p^2 + q^2}$$

sestavljajo pitagorejsko peterko $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e})$.

Dokaz:

$$(m^2 + n^2 + p^2 - q^2)^2 + (2mq)^2 + (2nq)^2 + (2pq)^2 = \cdots = (m^2 + n^2 + p^2 + q^2)^2$$

QED

2.6 Šesti generator pitagorejskih peteric

Tudi idejo iz izreka 2 smo nadgradili in dobili generator pitagorejskih peteric (glej izrek 5).

Izrek 5. Naj bodo m, n in p poljubna naravna števila. Tedaj števila

$$\boldsymbol{a = 2m^2}$$

$$\boldsymbol{b = 2mn}$$

$$\boldsymbol{c = 2mp}$$

$$\boldsymbol{d = n^2 + p^2}$$

$$\boldsymbol{e = 2m^2 + n^2 + p^2}$$

sestavljajo pitagorejsko peterico $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e})$.

Dokaz:

$$(2m^2)^2 + (2mn)^2 + (2mp)^2 + (n^2 + p^2)^2 = \cdots = (2m^2 + n^2 + p^2)^2$$

QED

Primeri so zbrani v tabeli 1.

m	n	p	Pitagorejska peterica
1	1	1	$(2,2,2,2,4) = 2(1,1,1,1,2)$
1	1	2	$(2,2,4,5,7)$
1	2	1	$(2,4,2,5,7)$
2	1	1	$(8,4,4,2,10) = 2(4,2,2,1,5)$
1	2	2	$(2,4,4,8,10) = (1,2,2,4,5)$
2	1	2	$(8,4,8,5,13)$
2	2	1	$(8,8,4,5,13)$
2	2	2	$(8,8,8,8,16) = 8(1,1,1,1,2)$

Tabela 1 Nekaj primerov pitagorejskih peteric, dobljenih s šestim generatorjem

2.7 Sedmi generator pitagorejskih peteric

Idejo iz razdelka 1.4.7 smo razširili in dobili generator pitagorejskih peteric, ki je opisan v izrekih 6a in 6b.

Izrek 6a. Če je x liho število, potem za vsako naravno število n sestavljajo števila a,b,c,d, e pitagorejsko peterico

$$\boldsymbol{a = x}$$

$$\boldsymbol{b = 2n}$$

$$\boldsymbol{c = 2m}$$

$$\boldsymbol{d = \frac{x^2 - 1}{2} + 2n^2 + 2m^2}$$

$$\boldsymbol{e = \frac{x^2-1}{2} + 2n^2 + 2m^2 + 1.}$$

Dokaz:

$$a^2 + b^2 + c^2 + d^2 = x^2 + (2n)^2 + (2m)^2 + \left(\frac{x^2-1}{2} + 2n^2 + 2m^2\right)^2 = \frac{\left(x^2+4n^2+4m^2+1\right)^2}{4} = \left(\frac{x^2-1}{2} + 2n^2 + 2m^2 + 1\right)^2 = e^2$$

QED

Izrek 6b. Če sta x in y sodi števili, potem za vsako naravno število n sestavljajo števila a,b,c,d, e pitagorejsko peterico

$$\boldsymbol{a = x}$$

$$\boldsymbol{b = y}$$

$$\boldsymbol{c = 2n + 1}$$

$$\boldsymbol{d = \frac{x^2}{2} + \frac{y^2}{2} + 2n^2 + 2n}$$

$$\boldsymbol{e = \frac{x^2}{2} + \frac{y^2}{2} + 2n^2 + 2n + 1.}$$

Dokaz:

$$a^2 + b^2 + c^2 + d^2 = x^2 + y^2 + (2n+1)^2 + \left(\frac{x^2}{2} + \frac{y^2}{2} + 2n^2 + 2n\right)^2 =$$

$$= \cdots = \left(\frac{x^2}{2} + \frac{y^2}{2} + 2n^2 + 2n + 1\right)^2 = e^2$$ QED

2.8 Osmi generator pitagorejskih peteric

Izrek 7a: Naravna števila a, b, c in d, kjer so vsaj tri izmed njih soda števila, zadoščajo enakosti $\boldsymbol{a^2 + b^2 + c^2 + d^2 = e^2}$ natanko tedaj, ko obstajajo takšna naravna števila k, l, m in n, kjer je n delitelj števila $\boldsymbol{k^2 + l^2 + m^2}$ in je n manjši od $\boldsymbol{\sqrt{k^2 + l^2 + m^2}}$ ter

$$\boldsymbol{a = \frac{k^2 + l^2 + m^2 - n^2}{n}.}$$

$$\boldsymbol{b = 2k}$$

$$\boldsymbol{c = 2l}$$

$$\boldsymbol{d = 2m}$$

$$\boldsymbol{e = \frac{k^2 + l^2 + m^2 + n^2}{n}.}$$

Dokaz (⟹)Naj števila a, b, c in d zadoščajo enačbi (2)

$$a^2 + b^2 + c^2 + d^2 = e^2.$$

Vsaj tri izmed števil a, b, c in d so soda števila. Potem obstajajo naravna števila k, l in m, da velja b=2k, c=2l in d = 2m. Ker je $a^2 < e^2$ (glej enačbo (3)), je tudi e > a.

Tako je število u = e-a naravno število.

Upoštevajmo e = a+u ter razvijmo:

$$e^2 = (a+u)^2 = a^2 + 2au + u^2$$

Po drugi strani je

$$e^2 = a^2 + b^2 + c^2 + d^2 = a^2 + 4k^2 + 4l^2 + 4m^2.$$

Ko izraza izenačimo, dobimo: $u^2 = 4k^2 + 4l^2 + 4m^2 - 2au.$

Ker je na desni strani vsota sodih števil, je u^2 sodo število, kar pomeni, da je u sodo število. Torej obstaja naravno število n, da je u = 2n. Tako sledi

$n^2 = k^2 + l^2 + m^2 - an$ oziroma

$k^2 + l^2 + m^2 = n(a+n)$, torej velja $n|(k^2 + l^2 + m^2)$.

Če iz enakosti $n^2 = k^2 + l^2 + m^2 - an$ izrazimo a, dobimo

$$a = \frac{k^2+l^2+m^2-n^2}{n}.$$

Ker velja $n|(k^2 + l^2 + m^2)$, je a naravno število. Število a je naravno število, zato je njegov števec pozitiven, torej je $n^2 < k^2 + l^2 + m^2$.

Izračunamo še

$$e^2 = a^2 + b^2 + c^2 + e^2 = \frac{k^2+l^2+m^2+n^2}{n}.$$

Dokaz (⟸): Vzemimo naravna števila k, l in m ter število n, ki naj bo delitelj $k^2 + l^2 + m^2$, manjši od $\sqrt{k^2 + l^2 + m^2}$ ter števila

$$a = \frac{k^2+l^2+m^2-n^2}{n}.$$

$$b = 2k$$

$$c = 2l$$

$$d = 2m$$

$$e = \frac{k^2 + l^2 + m^2 + n^2}{n}.$$

Ker je $a^2 + b^2 + c^2 + d^2 = \left(\frac{\boldsymbol{k^2+l^2+m^2-n^2}}{\boldsymbol{n}}\right)^{\boldsymbol{2}} + (\boldsymbol{2k})^{\boldsymbol{2}} + (\boldsymbol{2l})^{\boldsymbol{2}} + (\boldsymbol{2m})^{\boldsymbol{2}} = \cdots = \left(\frac{\boldsymbol{k^2+l^2+m^2+n^2}}{\boldsymbol{n}}\right)^{\boldsymbol{2}} = e^2,$ sestavljajo števila a, b, c, d in e pitagorejsko peterko.

QED

Primeri so prikazani v tabeli 2.

V primerih, ko je število a sodo število, so potem vsi členi peterice soda števila. Pitagorejska peterica takrat ni primitivna

k	l	m	$k^2+l^2+m^2$	n	a	(a,b,c,d,e)
1	1	1	3	1	2	$(2,2,2,2,4)=2(1,1,1,1,2)$
1	1	2	6	1	5	$(2,2,4,5,7)$
				2	1	$(1,2,2,4,5)$
1	2	2	9	1	8	$(2,4,4,8,10)=2(1,2,2,4,5)$
2	2	2	12	1	13	$(4,4,4,11,13)$
				2	4	$(4,4,4,4,8)=4(1,1,1,1,2)$
				3	1	$(1,4,4,4,7)$
1	2	3	14	1	13	$(2,4,6,13,15)$
				2	5	$(2,4,5,6,9)$
1	3	5	35	1	34	$(2,6,10,34,36)$ $=2(1,3,5,17,18)$
				5	2	$(2,2,6,10,12)$ $=2(1,1,3,5,6)$
3	4	5	50	1	49	$(6,8,10,49,51)$
				2	23	$(6,8,10,23,27)$
				5	5	$(5,6,8,10,15)$

Tabela 2 Primeri pitagorejskih peteric, dobljenih z osmim generatorjem (po izreku 7a)

Izrek 7b: Naravna števila a, b, c in d, kjer so vsa štiri liha števila, zadoščajo enakosti $a^2+b^2+c^2+d^2=e^2$ natanko tedaj, ko obstajajo takšna liha naravna števila k, l, m in n, kjer je n delitelj števila $k^2+l^2+m^2$ in je n manjši od $\sqrt{k^2+l^2+m^2}$ ter

$$a=\frac{k^2+l^2+m^2-n^2}{2n}.$$

$$b=k$$

$$c=l$$

$$d=m$$

$$e=\frac{k^2+l^2+m^2+n^2}{2n}.$$

Dokaz (⟹)Naj liha števila a, b, c in d zadoščajo enačbi (3) $a^2 + b^2 + c^2 + d^2 = e^2$, se pravi, da je (a, b, c, d, e) pitagorejska peterica. Potem je pitagorejska peterica tudi $(2a, 2b, 2c, 2d, 2e)$. Ta pitagorejska peterica ustreza pogojem iz izreka 7a. Torej obstajajo naravna števila k, l, m in n, kjer je n delitelj števila $k^2 + l^2 + m^2$ in je n manjši od $\sqrt{k^2 + l^2 + m^2}$ ter

$2a = \frac{k^2+l^2+m^2-n^2}{n}$.

$$2b = 2k$$

$$2c = 2l$$

$$2d = 2m$$

$$2e = \frac{k^2 + l^2 + m^2 + n^2}{n}.$$

Ker so b, c in d liha števila, so k, l, m liha števila. Ker je $2a = \frac{k^2+l^2+m^2-n^2}{n}$ in je a liho število, je $2a = \frac{nx-n^2}{n} = x - n$. Število nx je liho število, zato sta tako x in n lihi števili ter $x - n$ sodo število, zato sta $a = \frac{k^2+l^2+m^2-n^2}{2n}$. Iz podobnih razlogov je tudi $e = \frac{k^2+l^2+m^2+n^2}{2n}$ naravno število. Tako smo za pitagorejsko peterico (a, b, c, d, e), kjer so a,b,c in d liha števila, poiskali takšna liha naravna števila k, l, m in n, kjer je n delitelj števila $k^2 + l^2 + m^2$ in je n manjši od $\sqrt{k^2 + l^2 + m^2}$ ter

$$a = \frac{k^2+l^2+m^2-n^2}{2n}.$$

$$b = k$$

$$c = l$$

$$d = m$$

$$e = \frac{k^2 + l^2 + m^2 + n^2}{2n}.$$

Dokaz (⟸): Vzemimo liha naravna števila k, l in m ter število n, ki naj bo delitelj $k^2 + l^2 + m^2$, manjši od $\sqrt{k^2 + l^2 + m^2}$ ter števila

$$\boldsymbol{a = \frac{k^2+l^2+m^2-n^2}{2n}}.$$

$$b = 2k$$

$$c = 2l$$

$$d = 2m$$

$$e = \frac{k^2 + l^2 + m^2 + n^2}{2n}.$$

Ker je $a^2 + b^2 + c^2 + d^2 = \left(\frac{k^2+l^2+m^2-n^2}{2n}\right)^2 + (k)^2 + (l)^2 + (m)^2 = \cdots =$ $\left(\frac{k^2+l^2+m^2+n^2}{2n}\right)^2 = e^2$, sestavljajo števila a, b, c, d in e pitagorejsko peterko.

QED

V tabeli 3 navajamo nekaj primerov.

k	l	m	$k^2+l^2+m^2$	n	(a,b,c,d,e)
1	1	1	3	1	(1,1,1,1,2)
1	1	3	11	1	(1,1,3,5,6)
1	3	5	35	1	(1,3,5,17,18)
				5	(1,1,3,5,6)
1	3	3	19	1	(1,3,3,9,10)
1	5	5	51	1	(1,5,5,25,26)
				3	(1,5,5,7,10)
1	5	7	75	1	(1,5,7,37,38)
				3	(1,5,7,11,14)
				5	(1,5,5,7,10)
1	1	7	51	1	(1,1,7,25,26)
				3	(1,1,7,7,10)
3	9	27	819	1	(3,9,27,409,410)
				3	(3,9,27,135,138)
				7	(3,9,27,55,62)
				9	(3,9,27,41,50)
				13	(3,9,27,25,38)
				21	(3,9,27,9,30)

Tabela 3 Primeri pitagorejskih peteric, dobljenih z osmim generatorjem (po izreku 7b)

3 MNOŽENJE CELIH PITAGOREJSKIH PETERIC

3.1 Definicija množenja

Vzemimo množico celih pitagorejskih peteric. Če zamenjamo vrstni red prvih štirih komponent v peterici, dobimo drugo peterico. Množico pitagorejskih peteric si predstavljamo kot podmnožico v štirirazsežnem vektorskem prostoru.

V množici pitagorejskih trojic uvedemo množenje tako, da vzamemo idejo množenja dveh kompleksnih števil $z_1 = a + bi$ ter $z_2 = d + ei$. Potem je $z_1 \cdot z_2 = ad - be + (ae + bd)i$. Množenje dveh pritagorejskih trojic definiramo kot

$$(a, b, c) \circ (d, e, f) = (ad - be, ae + bd, cf).$$

Če sta (a, b, c) in (d, e, f) pitagorejski trojici, je pitagorejska trojica tudi $(ad - be, ae + bd, cf)$ (Križnič, Miklavčič, 2013). Ker ima pitagorejska peterica štiri katete, poskusimo definirati množenje pitagorejskih peteric s pomočjo množenja kvaternionov. Naj bosta $z_1 = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ ter $z_2 = p + q\boldsymbol{i} + r\boldsymbol{j} + s\boldsymbol{k}$ kvaterniona. Za množenje imaginarnih enot kvaternionov veljajo naslednja pravila:

$$\boldsymbol{i} \cdot \boldsymbol{j} = \boldsymbol{k} \qquad \boldsymbol{j} \cdot \boldsymbol{i} = -\boldsymbol{k} \qquad \boldsymbol{k} \cdot \boldsymbol{i} = \boldsymbol{j}$$

$$\boldsymbol{i} \cdot \boldsymbol{k} = -\boldsymbol{j} \qquad \boldsymbol{k} \cdot \boldsymbol{j} = -\boldsymbol{i} \qquad \boldsymbol{j} \cdot \boldsymbol{k} = \boldsymbol{i}$$

$$\boldsymbol{i} \cdot \boldsymbol{i} = \boldsymbol{j} \cdot \boldsymbol{j} = \boldsymbol{k} \cdot \boldsymbol{k} = \mathbf{1}$$

Zmnožimo:

$$z_1 \cdot z_2 = (a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}) \cdot (p + q\boldsymbol{i} + r\boldsymbol{j} + s\boldsymbol{k}) =$$

$$ap + aq\boldsymbol{i} + ar\boldsymbol{j} + as\boldsymbol{k} + bp\boldsymbol{i} + bq\boldsymbol{i}^2 + br\boldsymbol{ij} + bs\boldsymbol{ik} + cp\boldsymbol{j} + cq\boldsymbol{ji} + cr\boldsymbol{j}^2 + cs\boldsymbol{jk} + dp\boldsymbol{k} + dq\boldsymbol{ki} + dr\boldsymbol{kj} + ds\boldsymbol{k}^2 =$$

$$ap + aq\boldsymbol{i} + ar\boldsymbol{j} + as\boldsymbol{k} + bp\boldsymbol{i} - bq + br\boldsymbol{k} - bs\boldsymbol{j} + cp\boldsymbol{j} - cq\boldsymbol{k} - cr + cs\boldsymbol{i} + dp\boldsymbol{k} + dq\boldsymbol{j} - dr\boldsymbol{i} - ds =$$

$$ap - bq - cr - ds + (aq + bp + cs - dr)\boldsymbol{i} + (ar - bs + cp + dq)\boldsymbol{j} + (as + br - cq + dp)\boldsymbol{k}$$

Na osnovi te ideje definiramo množenje pitagorejskih peteric s pravilom:

$$(a,b,c,d,e)\circ(p,q,r,s,t)=(ap-bq-cr-ds, aq+bp+cs-dr, ar-bs+cp+dq, as+br-cq+dp, et). \quad (4)$$

Dokazati moramo, da je množenje pitagorejskih peteric (4) dobro definirano, torej, da je dobljena peterica pitagorejska(glej izrek 8).

Izrek 8: Naj bosta dani celi pitagorejski peterici $(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d},\boldsymbol{e})$; $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d},\boldsymbol{e}\in\boldsymbol{Z}$ in $(\boldsymbol{p},\boldsymbol{q},\boldsymbol{r},\boldsymbol{s},\boldsymbol{t})$; $\boldsymbol{p},\boldsymbol{q},\boldsymbol{r},\boldsymbol{s},\boldsymbol{t}\in\boldsymbol{Z}$. Potem je peterica $(\boldsymbol{ap}-\boldsymbol{bq}-\boldsymbol{cr}-\boldsymbol{ds}, \boldsymbol{aq}+\boldsymbol{bp}+\boldsymbol{cs}-\boldsymbol{dr}, \boldsymbol{ar}-\boldsymbol{bs}+\boldsymbol{cp}+\boldsymbol{dq}, \boldsymbol{as}+\boldsymbol{br}-\boldsymbol{cq}+\boldsymbol{dp}, \boldsymbol{et})$ cela pitagorejska peterica.

Dokaz:

$$(ap-bq-cr-ds)^2+(aq+bp+cs-dr)^2+(ar-bs+cp+dq)^2 + (as+br-cq+dp)^2 =$$

$$\begin{aligned}a^2p^2+b^2q^2+c^2r^2+d^2s^2-2apbq-2apcr-2apds+2bqcr+2bqds+2crds\\ +a^2q^2+b^2p^2+c^2s^2+d^2r^2+2aqbp+2aqcs-2aqdr+2bpcs\\ -2bpdr-2csdr+\ a^2r^2+b^2s^2+c^2p^2+d^2q^2-2arbs+arcp+2ardq\\ -2bscp-2bsdq+2cpdq+a^2s^2+b^2r^2+c^2q^2+d^2p^2+2asbr-2ascq\\ +2asdp-2brcq+2brdp-2cqdp=\end{aligned}$$

$$\begin{aligned}a^2p^2+b^2q^2+c^2r^2+d^2s^2+a^2q^2+b^2p^2+c^2s^2+d^2r^2+\ a^2r^2+b^2s^2+c^2p^2+d^2q^2\\ +a^2s^2+b^2r^2+c^2q^2+d^2p^2=\end{aligned}$$

$$a^2(p^2+q^2+r^2+s^2)+b^2(p^2+q^2+r^2+s^2)+c^2(p^2+q^2+r^2+s^2) + d^2(p^2+q^2+r^2+s^2)=$$

$$a^2t^2+b^2t^2+c^2t^2+d^2t^2=\ t^2(a^2+b^2+c^2+d^2)=e^2t^2$$

QED

Da smo si olajšali množenje pitagorejskih peteric, smo napisali program v programskem jeziku Python (glej sliko 5). Navajamo nekaj primerov množenja:

$$
\begin{aligned}
&(1,1,1,1,2) \circ (1,2,2,4,5) \\
&\qquad = (1 \cdot 1 - 1 \cdot 2 - 1 \cdot 2 - 1 \cdot 4, 1 \cdot 2 + 1 \cdot 1 + 1 \cdot 4 - 1 \cdot 2, 1 \cdot 2 - 1 \cdot 4 + 1 \cdot 1 \\
&\qquad + 1 \cdot 2, 1 \cdot 4 + 1 \cdot 2 - 1 \cdot 2 + 1 \cdot 1, 2 \cdot 5) \\
&\qquad = (1 - 2 - 2 - 4, 2 + 1 + 4 - 2, 2 - 4 + 1 + 2, 4 + 2 - 2 + 1, 10) \\
&\qquad = (-7,5,1,5,10)
\end{aligned}
$$

$$
\begin{aligned}
&(4,2,2,1,5) \circ (8,2,2,7,11) \\
&\qquad = (4 \cdot 8 - 2 \cdot 2 - 2 \cdot 2 - 1 \cdot 7, 4 \cdot 2 + 2 \cdot 8 + 2 \cdot 7 - 1 \cdot 2, 4 \cdot 2 - 2 \cdot 7 + 2 \cdot 8 \\
&\qquad + 1 \cdot 2, 4 \cdot 7 + 2 \cdot 2 - 2 \cdot 2 + 1 \cdot 8, 5 \cdot 11) \\
&\qquad = (32 - 4 - 4 - 7, 8 + 16 + 14 - 2, 8 - 14 + 16 + 2, 28 + 4 - 4 + 8, 55) \\
&\qquad = (17,36,12,36,55)
\end{aligned}
$$

$$
\begin{aligned}
&(1,5,5,7,10) \circ (14,28,22,55,67) \\
&\qquad = (1 \cdot 14 - 5 \cdot 28 - 5 \cdot 22 - 7 \cdot 55, 1 \cdot 28 + 5 \cdot 14 + 5 \cdot 55 - 7 \cdot 22, 1 \cdot 22 \\
&\qquad - 5 \cdot 55 + 5 \cdot 14 + 7 \cdot 28, 1 \cdot 55 + 5 \cdot 22 - 5 \cdot 28 + 7 \cdot 14, 10 \cdot 67) \\
&\qquad = (14 - 140 - 110 - 385, 28 + 70 + 275 - 154, 22 - 275 + 70 + 196, 55 \\
&\qquad + 110 - 140 + 98, 670) = (-621,219,13,123,670)
\end{aligned}
$$

Kot zanimivost navajamo primer, da produkt dveh naravnih pitagorejskih peteric ni vedno naravna pitagorejska peterica, na primer:

(4, 2, 1, 2, 5) ∘ (1, 1, 1, 1, 2) = (-1, 5,5,7,10).

Množica naravnih pitagorejskih peteric torej ni zaprta za množenje, definirano s (4).

```
pet1 = input("Vnesi prvo peterko v formatu [a,b,c,d,e]: ")
pet2 = input("Vnesi drugo peterko v formatu [a,b,c,d,e]: ")

a1 = pet1[0]
b1 = pet1[1]
c1 = pet1[2]
d1 = pet1[3]
e1 = pet1[4]

a2 = pet2[0]
b2 = pet2[1]
c2 = pet2[2]
d2 = pet2[3]
e2 = pet2[4]

at = a1 * a2 - b1 * b2 - c1 * c2 - d1 * d2
bt = a1 * b2 + b1 * a2 + c1 * d2 - d1 * c2
ct = a1 * c2 - b1 * d2 + c1 * a2 + d1 * b2
dt = a1 * d2 + b1 * d2 - c1 * b2 + d1 * a2
et = e1 * e2

print "Produkt peterk " + str(pet1) + " in " + str(pet2) + " je " + str([at,bt,ct,dt,et]) + "."
```

Slika 5 Program za množenje pitagorejskih peteric (Python)

3.2 Lastnosti množenja

V množici celih pitagorejskih peteric smo definirali množenje s pravilom (4). Preverimo, ali za to operacijo velja katera izmed osnovnih lastnosti:

- Ali obstaja enota za množenje?
- Ali za množenje velja komutativnostni zakon: A∘B = B∘A, kjer sta A in B pitagorejski peterici)
- Ali za množenje velja asociativnostni zakon: (A∘B) ∘C = A∘ (B∘C), kjer so A,B in C pitagorejske peterice?

Najprej predpostavimo, da bi enota lahko bila peterica (1,0,0,0,1).

Izrek 9: Množenje celih pitagorejskih peteric, definirano v (4), je množenje z enoto. Enota za množenje je element $(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$.

Dokaz:

$(a,b,c,d,e) \circ (1,0,0,0,1) = (a \cdot 1 + b \cdot 0 + c \cdot 0 + d \cdot 0), (a \cdot 0 + b \cdot 1 + c \cdot 0 + d \cdot 0),$
$(a \cdot 0 + b \cdot 0 + c \cdot 1 + d \cdot 0), (a \cdot 0 + b \cdot 0 + c \cdot 0 + d \cdot 1), e \cdot 1 = (a,b,c,d,e).$

Ker ne vemo, ali je množenje komutativno, preverimo še množenje z enoto z leve:

$(1,0,0,0,1) \circ (a,b,c,d,e) = \cdots = (a,b,c,d,e)$. QED

Naj bosta z_1 in z_2 pitagorejski peterici. Dokažimo izrek 10.

Izrek 10: Množenje celih pitagorejskih peteric ni komutativno.

Dokaz: Naj bosta $z_1 = (a,b,c,d,e)$ in $z_2 = (p,q,r,s,t)$ pitagorejski peterici.

$$z_1 \circ z_2 = (a,b,c,d,e) \circ (p,q,r,s,t) =$$

$$(ap - bq - cr - ds, aq + bp + cs - dr, ar - bs + cp + dq, as + br - cq + dp, et)$$

$$z_2 \circ z_1 = (p,q,r,s,t) \circ (a,b,c,d,e)$$
$$= (ap - bq - cr - ds, aq + bp - cs + dr, ar + bs + cp - dq, as - br + cq + dp, te)$$

Ugotovili smo, da $z_1 \circ z_2 \neq z_2 \circ z_1$, torej množenje, definirano s (4), ni komutativno.

QED

Preverimo še asociativnostni zakon. Vzemimo tri pitagorejske peterice: (a,b,c,d,e), (p,q,r,s,t) in (x,y,z,u,v) ter dokažimo izrek 11.

Izrek 11: Množenje celih pitagorejskih peteric je asociativno.

Dokaz:

$$\big((a,b,c,d,e)\circ(p,q,r,s,t)\big)\circ(x,y,z,u,v)=$$

$$=(ap-bq-cr-ds,aq+bp+cs-dr,ar-bs+cp+dq,as+br-cq+dp,et)\circ(x,y,z,u,v)=$$

$$\begin{aligned}&(ap-bq-cr-ds)x-(aq+bp+cs-dr)y-(ar-bs+cp+dq)z\\&-(as+br-cq+dp)u,(aq+bp+cs-dr)x\\&+(ap-bq-cr-ds)y-(as+br-cq+dp)z\\&+(ar-bs+cp+dq)u,(ar-bs+cp+dq)x\\&+(as+br-cq+dp)y+(ap-bq-cr-ds)z\\&-(aq+bp+cs-dr)u,(as+br-cq+dp)x\\&-(ar-bs+cp+dq)y+(aq+bp+cs-dr)z\\&+(ap-bq-cr-ds)u,etv)=\end{aligned}$$

$$\begin{aligned}=(&apx-dsx-bqx-crx-arz-dqz-cpz+bsz-aqy+dry-bpy\\&-csy-asu-dpu+cqu-bru,aqx-drx+bpx+csx-asz\\&-dpz+cqz-brz+apy-dsy-bqy-cry+aru+dqu\\&+cpu-bsu,arx+dqx+cpx-bsx+apz-dsz-bqz-crz\\&+asy+dpy-cqy+bry-aqu+dru-bpu-csu,asx+dpx\\&-cqx+brx+aqz-drz+bpz+csz-ary-dqy-cpy\\&+bsy+apu-dsu-bqu-cru,etv)\end{aligned}$$

$$(a,b,c,d,e)\circ\big((p,q,r,s,t)\circ(x,y,z,u,v)\big)=$$

$$(a,b,c,d,e)\circ(px-qy-rz-su,qx+py-sz+ru,rx+sy+pz-qu,sx-ry+qz+pu,tv)=$$

$$\begin{aligned}=(&a(px-qy-rz-su)-b(qx+py-sz+ru)-c(rx+sy+pz-qu)-\\&d(sx-ry+qz+pu),a(qx+py-sz+ru)+b(px-qy-rz-su)+\\&c(sx-ry+qz+pu)-d(rx+sy+pz-qu),a(rx+sy+pz-qu)-\end{aligned}$$

$b(sx - ry + qz + pu) + c(px - qy - rz - su) + d(qx + py - sz + ru), a(sx - ry + qz + pu) + b(rx + sy + pz - qu) - c(qx + py - sz + ru) + d(px - qy - rz - su), e(tv))=$

$$= (apx - dsx - bqx - crx - aqy + dry - bpy - csy - arz - dqz - cpz + bsz - asu - dpu + cqu - bru, aqx - drx + bpx + csx + apy - dsy - bqy - cry - asz - dpz + cqz - brz + aru + dqu + cpu - bsu, arx + dqx + cpx - bsx + asy + dpy - cqy + bry + apz - dsz - bqz - crz - aqu + dru - bpu - csu, asx + dpx - cqx + brx - ary - dqy - cpy + bsy + aqz - drz + bpz + csz + apu - dsu - bqu - cru, etv)$$

Enakost velja. Tako smo dokazali, da za množenje pitagorejskih peteric velja asociativnostni zakon. QED

Naj bo $\alpha = (a, b, c, d, e)$ cela pitagorejska peterica. Potem je $\beta = \frac{1}{k}(a, b, c, d, e) = (\frac{a}{k}, \frac{b}{k}, \frac{c}{k}, \frac{d}{k}, \frac{e}{k})$ racionalna peterica za vsak $k \in Z, k \neq 0$. Dokaz je očiten. Množica celih pitagorejskih peteric je za operacijo množenja, definirano s (4), asociativna, obstaja leva in desna enota (1,0,0,0,1) ter ni komutativna. Vse to velja tudi v množici neničelnih racionalnih peteric. Vprašajmo se o obstoju inverzne pitagorejske peterice, Pokazali bomo, da obstajata levi in desni inverz, ki sta enaka. V se to povzemimo v naslednjem izreku:

Izrek 12: Množica neničelnih racionalnih peteric je nekomutativna grupa za operacijo množenja, definirano v (4).

Dokaz: V izreku 9 smo dokazali obstoj enote, v izreku 10, da množenje ni komutativno ter v izreku 11, da je množenje asociativno. Množica z operacijo je grupa, če je

operacija asociativna, če obstaja enota in za vsak neničelni element obstaja inverz. Manjka nam torej le inverz. Naj bo

$\alpha = (a, b, c, d, e)$ neničelna racionalna pitagorejska peterica. Poiščimo desni inverz $\alpha^{-1} = (x, y, z, u, v)$:

$\alpha \circ \alpha^{-1} = (a, b, c, d, e) \circ (x, y, z, u, v) = (1,0,0,0,1)$.

Ko zmnožimo levo stran, dobimo:

$$(ax - by - cz - du, bx + ay - dz + cu, cx + dy + az - bu, dx - cy + bz + au, ev) = (1,0,0,0,1)$$

Zapišimo sistem petih enačb s petimi neznankami:

$$ax - by - cz - du = 1$$

$$bx + ay - dz + cu = 0$$

$$cx + dy + az - bu = 0$$

$$dx - cy + bz + au = 0$$

$$ev = 1$$

Rešitev sistema je:

$$x = \frac{a}{a^2 + b^2 + c^2 + d^2}$$

$$y = -\frac{b}{a^2 + b^2 + c^2 + d^2}$$

$$z = -\frac{c}{a^2 + b^2 + c^2 + d^2}$$

$$u = -\frac{d}{a^2 + b^2 + c^2 + d^2}$$

$$v = \frac{1}{e}$$

Peterica $\alpha^{-1} = \left(\frac{a}{a^2+b^2+c^2+d^2}, -\frac{b}{a^2+b^2+c^2+d^2}, -\frac{c}{a^2+b^2+c^2+d^2}, -\frac{d}{a^2+b^2+c^2+d^2}, \frac{1}{e}\right)$ je torej desni inverz.

Dokažimo še, da je ista peterica tudi levi inverz:

$\alpha^{-1} \circ \alpha = \left(\frac{a}{a^2+b^2+c^2+d^2}, -\frac{b}{a^2+b^2+c^2+d^2}, -\frac{c}{a^2+b^2+c^2+d^2}, -\frac{d}{a^2+b^2+c^2+d^2}, \frac{1}{e}\right) \circ (a,b,c,d,e) =$ $(1,0,0,0,1)$.

Ker je $\alpha^{-1} = \left(\frac{a}{a^2+b^2+c^2+d^2}, -\frac{b}{a^2+b^2+c^2+d^2}, -\frac{c}{a^2+b^2+c^2+d^2}, -\frac{d}{a^2+b^2+c^2+d^2}, \frac{1}{e}\right)$ levi in desni inverz, obstaja torej k vsaki neničelni pitagorejski peterici inverzni element. Element α^{-1} lahko tudi krajše zapišemo:

$$\alpha^{-1} = \left(\frac{a}{e^2}, -\frac{b}{e^2}, -\frac{c}{e^2}, -\frac{d}{e^2}, \frac{1}{e}\right)$$

Opomba:

Levi inverz bi lahko poiskali tudi iz enakosti:

$\alpha^{-1} \circ \alpha = (x,y,z,u,v) \circ (a,b,c,d,e) = (1,0,0,0,1)$.

Pripadajoči sistem

$$ax - by - cz - du = 1$$

$$bx + ay + dz - cu = 0$$

$$cx - dy + az + bu = 0$$

$$dx + cy - bz + au = 0$$

$$ve = 1$$

se razlikuje od sistema, s katerim smo iskali desni inverz, a imata oba enako rešitev.

QED

Oglejmo si še nekaj primerov inverznih peteric:

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

$$(97,20,20,20,103)^{-1} = \left(\frac{97}{10609}, \frac{-20}{10609}, \frac{-20}{10609}, \frac{-20}{10609}, \frac{1}{103}\right)$$

4 RAZSTAVLJANJE PITAGOREJSKIH PETERIC

V množici celih pitagorejskih peteric se vprašamo tudi, ali je možno dano celo pitagorejsko peterico zapisati kot produkt dveh celih pitagorejskih peteric. Temu procesu bomo rekli, da celo pitagorejsko peterico razcepimo na produkt nerazcepnih pitagorejskih peteric. Pitagorejska peterica je nerazcepna tedaj, ko je ne moremo zapisati kot produkt dveh celih pitagorejskih peteric. Pri tem seveda razcepa večkratnika primitivne pitagorejske trojice na $k(a, b, c, d, e)$ ne štejemo z razcep. Očitno je, da pitagorejske peterice s praštevilsko hipotenuzo ni mogoče razcepiti. Program v Pythonu, ki razcepi dano pitagorejsko peterico, je v prilogi.

Navajamo nekaj primerov nerazcepnih pitagorejskih peteric.

- (16,10,14,17,29)
- (5,10,8,10,17)
- (14,34,4,1,37)
- (7,2,8,2,11)
- (22,16,11,10,31)
- (11,20,62,26,71)
- (7,4,2,10,13)
- (38,8,2,13,41)
- (10,40,10,7,43)
- (26,16,11,34,47)
- (1,2,2,4,5)
- (14,28,22,55,67)

Naštete pitagorejske peterice so vse s praštevilsko hipotenuzo. Obstajajo pa tudi nerazcepne pitagorejske peterice, ki nimajo za hipotenuzo praštevila. To so na primer:

(9,1,3,3,10), (33, 31, 15, 15, 50), (1,7,5,5,109).

Nerazcepnost takšnih peteric smo ugotavljali s programom v Pythonu (glej prilogo).

Nerazcepne pitagorejske peterice imajo podobno vlogo kot praštevila v množici naravnih števil. V množici naravnih števil velja izrek o enoličnem razcepu na praštevila. Podobno smo se vprašali tudi tukaj, ali velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice. Dokazali smo, da ne velja (glej izrek 13).

Izrek 13: V množici celih pitagorejskih peteric ne velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice.

Dokaz: Teoretično se tega dokaza nismo niti lotili. S pomočjo programa za razcep smo (po dolgem preizkušanju) našli celo pitagorejsko peterico, ki jo lahko zapišemo kot produkt dveh različnih nerazcepnih pitagorejskih peteric.

(-28, 64, 64, 32, 100) = (9, 1, 3, 3, 10) o (1, 7, 5, 5, 10)

(-28, 64, 64, 32, 100) = (1, 1, 1, 1, 2) o (33, 31, 15, 15, 50)

Program za razstavljanje pitagorejskih peteric nam je vrnil dve enaki pitagorejski peterici, razstavljeni na dva različna načina. Pokazali smo, da so dobljene peterice v razcepu nerazcepne (s pomočjo programa v prilogi).

Izrek 14: V množici naravnih pitagorejskih peteric ne velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice.

Podobno kot pri celih pitagorejskih petericah smo tudi tu opustili teoretično dokazovanje in se lotili iskanja protiprimera. Program v prilogi smo dopolnili tako, da je iskal samo naravne pitagorejske peterice. Po res zelo zelo dolgem času iskanja (program je tekel več ur) smo našli naravno pitagorejsko peterico, ki jo lahko zapišemo kot produkt dveh naravnih nerazcepnih pitagorejskih trojic na dva različna načina.

(52, 494, 715, 494, 1001) = (8, 2, 2, 7, 11) o (52, 65, 26, 26, 91)

(52, 494, 715, 494, 1001)= (4, 2, 2, 5, 7) o (104, 91, 26, 26, 143) =

= 13 (4,2,2,5,7) o (8,7,2,2,11).

Pitagorejski peterici (8, 2, 2, 7, 11) ter (8,7,2,2,11) sta kot elementa podmnožice vektorskega prostora seveda različni.

Poiskali smo še drug primer, pri katerem pa so vsi faktorji nerazcepne pitagorejske peterice.

(686, 468, 359, 718, 1155) = (10, 4, 1, 2, 11) ∘ (87, 16, 40, 40, 105)

(686, 468, 359, 718, 1155) = (4, 2, 1, 2, 5) ∘ (219, 20, 50, 50, 231).

Dobljeni protiprimeri dokazujejo, da v množici naravnih pitagorejskih peteric ne velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice. QED

5 ZAKLJUČEK

V nalogi smo si zastavili štiri cilje in sicer odkriti čimveč parametrizacij (generatorjev) pitagorejskih peteric, odkriti parametrizacijo, ki opiše vse pitagorejske peterice,v množici celih pitagorejskih peteric definirati množenje in preveriti ter dokazati, ali velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice.

Opisali smo osem paranetrizacij (generatorjev) pitagorejskih peteric. Odkrili in dokazali smo tudi generator, s katerim generiramo vse pitagorejske peterice. V množici celih pitagorejskih peteric smo definirali množenje pitagorejskih peteric. Dokazali smo, da obstaja enota za množenje, da je množenje asociativno in da ni komutativno. Kot povezavo povejmo, da je množenje pitagorejskih trojic komutativno in asociativno. Zastavili smo si tudi problem razstavljanja in dokazali, da nti v množici celih pitagorejskih peteric niti v množici naravnih pitagorejskih peteric ne velja izrek o enoličnem razcepu na nerazcepne pitagorejske peterice.

V nam dostopnih virih smo zasledili zelo mali omemb in člankov o pitagorejskih petericah in še tisti so bili na visokem znanstvenem nivoju, ki ga nismo razumeli. O pitagorejskih trojicah in četvericah pa je več znanega. Tako smo nekaj lastnosti dobili iz idej o pitagorejskih trojicah in četvericah, nekaj pa je plod našega lastnega ustvarjanja.

Nadaljnje raziskovanje pitagorejskih peteric bi se lahko usmerilo v iskanje pogojev, kdaj so pitagorejske peterice nerazcepne. Zanimivo bi bilo raziskati, kako so pitagorejske peterice razporejene znotraj štirirazsežnega vektorskega prostora. Predvidevamo pa, da bi bilo zelo težko ugotoviti, saj je pitagorejskih peteric zelo veliko. Z določeno hipotenuzo dobimo zelo veliko število pitagorejskih peteric. Izdelati bi bilo potrebno seveda računalniško simulacijo. Ker so pitagorejske trojice razporejene po parabolah, bi bilo zanimivo videti, ali so mogoče tudi pitagorejske peterice razporejene samo na določenih »predelih.«

6 VIRI IN LITERTURA

[1] Križnič, J. in Miklavčič R.: Množenje in razstavljanje pitagorejskih trojic. Raziskovalna naloga. Škofijska gimnazija Vipava, Vipava, 2013.

[2] Posamentier, A. S: The Pythagorean Theorem: The Story of its Power and Beauty. Prometheus Books, 2010.

[3] Sierpinski, W.: *Pythagorean Triangles.* Dover Publications, Meneola, New York, 2003.

[4] Vidav, I.: Algebra, Mladinska knjiga, Ljubljana, 1972.

7 Kazalo slik

8 Kazalo tabel

PRILOGA

Program za razstavljanje pitagorejskih peteric

```
peterka = input("Vnesi peterico v obliki [a,b,c,d,e]: ")
el = 2
while el <= int(peterka[4]**0.5):
    e2 = int(peterka[4] / el)
    if el * e2 == peterka[4]:
        for a1 in range(el):
            for b1 in range(el):
                for c1 in range(el):
                    for d1 in range(el):
                        if a1**2 + b1**2 + c1**2 + d1**2 == el**2:
                            for a2 in range(e2):
                                for b2 in range(e2):
                                    for c2 in range(e2):
                                        for d2 in range(e2):
                                            if  a2**2 + b2**2 + c2**2 + d2**2 == e2**2:
                                                at = a1 * a2 - b1 * b2 - c1 * c2 - d1 * d2
                                                bt = a1 * b2 + b1 * a2 + c1 * d2 - d1 * c2
                                                ct = a1 * c2 - b1 * d2 + c1 * a2 + d1 * b2
                                                dt = a1 * d2 + b1 * d2 - c1 * b2 + d1 * a2
                                                et = el * e2
                                                if peterka == [at,bt,ct,dt,et]:
                                                    print str([at,bt,ct,dt,et]) + " = " + str([a1,b1,c1,d1,e1]) + " o " + str([a2,b2,c2,d2,e2])
    el += 1
ex = input("Done! Press enter to exit!")
```