Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Anita Kopecki

Diofant i diofantske jednadžbe

Diplomski rad

Osijek, 2011.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Anita Kopecki

Diofant i diofantske jednadžbe

Diplomski rad

Voditelj: Doc. dr. sc. Ivan Matić

Osijek, 2011.

Sadržaj

1. Uvod

U početku su se algebarski problemi pisali riječima, a ne simbolima pa je bilo jako teško formulirati probleme. Diofant radi drastične promjene u algebri, uvodeći simboliku te time omogućuje jasan i uniforman zapis te formalizaciju ove discipline. Iz tog razloga ga se naziva *ocem algebre.*
Osim toga, proučavao je algebarske jednadžbe i njihova racionalna rješenja koje su dobile ime njemu u čast jer je prvi koji ih je zapisivao simbolički. Također, bavio se aproksimacijama iracionalnih brojeva racionalnima, otvorivši time drugim istraživačima područje teorije brojeva danas poznato pod nazivom *diofantske aproksimacije.*

On je najveći matematičar postklasičnog razdoblja grčke matematike i zadnji veliki europski matematičar prije Fibonaccija.
Međutim, poznat je i po utjecaju na druge značajne matematičare, npr. Fermat je u svojoj verziji Diofantove knjige Arithmetica na marginama stranice postavio svoj veliki teorem koji je dokazan tek 1994. godine.

U Diofantovo vrijeme matematičari su se bavili geometrijom, trigonometrijom i mehanikom. Diofant je svojim radom o algebarskim jednadžbama bio ispred svog vremena te je prošlo mnogo stoljeća dok matematičari nisu shvatili veličinu njegova rada. Za primjer se može navesti da se u Europi u srednjem vijeku koristila Diofantova notacija, ali se nije znalo da je on zaslužan.

U poglavlju *Diofantova biografija i doprinos* opisan je Diofantov život, te ukratko njegov doprinos u matematici, dok je u poglavlju *Diofantov utjecaj na druge matematičare* opisan njegov utjecaj na Vietea, Fermata, Pella, Eulera.
U sljedeća dva poglavlja, *Problem 8 knjiga II* i *Problem 16 knjiga V* navedeni su Diofantovi problemi koji se bave rješavanjem neodređenih kubnih jednadžbi.
Nakon toga su u poglavljima *Diofantske jednadžbe* i *Metode rješavanja diofantskih jednadžbi* opisane diofantske jednadžbe i neke klasične, te metode rješavanja diofantskih jednadžbi.
Posljednje poglavlje, *Hilbertov 10. problem* bavi se najnovijim razmišljanjima o diofantskim jednadžbama.

2. Diofantova biografija i doprinos

Diofant je živio u Aleksandriji (danas egipatski grad) te se još naziva i *Diofant Aleksandrijski* (eng. Diophantus of Alexandria).

Slika 2.1 *Diofant Aleksandrijski*

Diofant je najveći matematičar postklasičnog razdoblja grčke matematike i zadnji veliki europski matematičar prije Fibonaccija (13.st.). Postklasično razdoblje traje od 2. stoljeća pr. Kr. kada Rimljani zauzimaju grčko kopno pa sve do 5. stoljeća kada pada Rimsko Carstvo.
O Diofantu se jako malo zna, postoji više podataka o njegovim radovima nego o životu. Postoji jedna zagonetka u stihovima o dužini Diofantova života koju je napisao grčki lingvist Metrodor oko 500. godine.
"Diofantovo djetinjstvo trajalo je šestinu njegova života, oženio se sedminu godina kasnije, brada mu je narasla kada je prošla još dvanaestina, a sin mu se rodio 5 godina kasnije. Sin je živio polovinu očevih godina, a otac je umro 4 godine poslije sina. Koliko godina je živio Diofant?"
Jednadžba ove zagonetke gdje je x broj Diofantovih godina glasi

$$\frac{1}{6}x + \frac{1}{7}x + \frac{1}{12}x + 5 + \frac{1}{2}x + 4 = x.$$

Rješavanjem se dobije $x = 84$, što znači da je Diofant živio 84 godine. Ne postoje nikakvi zapisi kad je točno živio, ali istraživanja pokazuju da je rođen između 200. i 214. godine, a umro između 284. i 298. godine.
U to vrijeme Aleksandrija je bila znanstveno i kulturno središte antičkog svijeta jer je imala *Akademiju znanosti* u kojoj su radili učenjaci koji su poučavali studente. Jedan od njih bio je i Diofant.
Najpoznatiji je po svojoj knjizi *Arithmetica* koja se sastoji od 13 knjiga od kojih je pronađeno samo šest.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
AVCTORE CLAVDIO GASPARE BACHETO
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Slika 2.2 *Arithmetica na latinskom jeziku, izdanje 1621. godine*

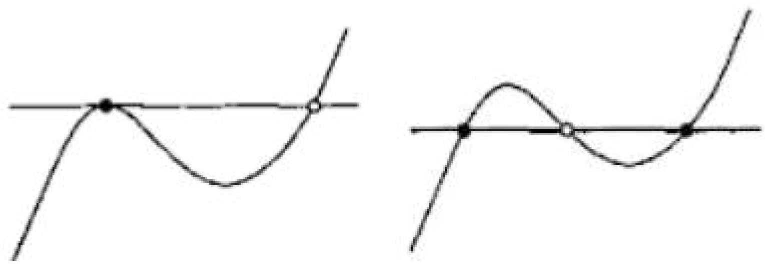
Arithmetica se uvelike razlikuje po stilu i sadržaju od ostalih antičkih knjiga koje su se bavile teorijom brojeva i algebrom zbog simboličkog zapisivanja problema i samih problema (vidjeti [4], str. 3).
Knjiga se bavi rješavanjem algebarskih problema, određenih i neodređenih jednadžbi i sustava jednadžbi, u skupu pozitivnih racionalnih brojeva. U ovih šest knjiga nalazi se 150 problema. Također, knjiga je najstariji sačuvani zapis koji se bavi proučavanjem neodređenih jednadžbi (jednadžbe koje imaju beskonačno mnogo rješenja). Danas se dio matematike koji se bavi rješavanjem neodredenih jednadžbi naziva *diofantska analiza*.

Što se tiče metoda rješavanja, Diofant ih nije navodio u općem obliku, ali je na jednaki način rješavao probleme iste vrste što znači da je na jednake probleme primjenjivao jednake metode. Kasnije su diofantske jednadžbe promatrane pomoću algebarske geometrije, te je nastala grana matematike pod nazivom *diofantska geometrija* (vidjeti [15], str. 824).
Algebarska geometrija znači da se jednadžbe rješavaju pomoću geometrijskih tehnika, tj. ako se neodređena jednadžba promatra kao krivulja, tada se za rješenje traže sve racionalne točke koje leže na krivulji.

Tako su Diofantove metode rješavanja neodređenih kubnih jednadžbi promatrane pomoću algebarske geometrije i nazvane su *Diofantova metoda tangente* i *Diofantova metoda sekante*.

Diofantova metoda tangente glasi: *ako racionalna točka leži na krivulji, tada tangenta krivulje na tu točku siječe krivulju u još jednoj racionalnoj točki*, a metoda sekante: *ako dvije*

racionalne točke leže na krivulji, pravac koji ih spaja siječe krivulju u još jednoj racionalnoj točki.
Na sljedećim slikama prikazane su ove situacije.



Slika 2.3 *Diofantove metode tangente i sekante*

Stvarno je začuđujuće kako je Diofant znao rješavati ovakve jednadžbe. Pomoću spretnog izbora nepoznanica i domišljatih supstitucija izbjegavao je mnoge probleme koje ne bi znao riješiti. Također, u nekim problemima je iracionalne brojeve aproksimirao pomoću racionalnih brojeva - *diofantske aproksimacije*.

Osim Arithmetice, Diofant je napisao i knjigu *Porizmi*, koja nije pronađena. u toj knjizi nalazila su se svojstva brojeva i propozicije na koje se pozivao u Arithmetici. Budući da se u grčko vrijeme ništa nije zapisivalo ako se nije znalo dokazati, pretpostavlja se da je Diofant znao dokazati svaku propoziciju.

Međutim, Diofant je ipak najpoznatiji po svojoj simbolici i utjecaju na druge matematičare. Stoga će u nastavku biti više riječi o tome.

2.1. Simbolizam

Na početku prve knjige Arithmetice Diofant navodi osnovne definicije i opis simbola koji će koristiti, te tako postaje prvi u povijesti koji je simbolički zapisivao algebarske izraze.
Dotad se algebra pisala u prozi pa je bilo komplicirano rješavati jednadžbe. Diofant je uvođenjem simbola za nepoznanice, koeficijente, potencije i računske operacije uvelike olakšao postavljanje i rješavanje jednadžbi te je na taj način pokrenuo veliki razvoj algebre. Neki ga stoga nazivaju *ocem algebre*.

U klasičnoj grčkoj matematici, razlomci i iracionalni brojevi nisu smatrani brojevima, a nisu postojali ni negativni brojevi. Diofant je uveo negativne brojeve, i još više od toga, racionalne brojeve.
Osim toga, uveo je oznaku za jednakost ἴσ koja je nastala tako da je uzeo prva dva slova

riječi *jednako* na grčkom jeziku ἴσος. Za operaciju zbrajanja samo je nadopisivao brojeve, dok za operaciju oduzimanja (kao i znak za negativan broj) koristi oznaku $\pitchfork$.
Također, uveo je neke elemente teorije brojeva, npr. simbole do šeste potencije, kao i za negativne potencije oznaku χ koji se mogu vidjeti u sljedećoj tablici (vidjeti [4], str 5, [3], str 82).

Suvremena oznaka	**Diofantova oznaka**
x^0	$\mathring{M}$
x	ζ
x^2	$\Delta^{\tilde{v}}$
x^3	$K^{\tilde{v}}$
x^4	$\Delta^{\tilde{v}}\Delta$
x^5	$\Delta K^{\tilde{v}}$
x^6	$K^{\tilde{v}}K$
x^{-1}	$\Delta^{\tilde{v}\chi}$
x^{-2}	$K^{\tilde{v}\chi}$

Tablica 1: Diofantovi simboli za nepoznanice i njezine potencije (do šeste)

Međutim, pogriješio je što nije uveo oznaku za drugu nepoznanicu, te nekad s ζ označava više od jednog nepoznatog broja.
U nekim problemima je kao oznake koristio geometrijske likove, npr. oznaka za nepoznati kvadrat je $\square$, za nepoznati kub .Pomoću njih zapisivao je i kub kvadrata, kvadrat kvadrata i ostale kombinacije.
Osim toga, Diofant je formulirao pravila za trasformaciju jednadžbi koja uključuju dodavanje ili oduzimanje istog izraza na obje strane, pravila za množenje brojeva s predznakom, pravila za množenje i dijeljenje potencija (vidjeti [4], str 7).

Navedimo jedan primjer jednadžbe u Diofantovoj izvornoj notaciji.

$$202x^2 + 13 - 10x = 13$$

$$x^2 202 + x^0 13 - x10 = x^0 13$$

$$\Delta^{\tilde{v}}\overline{\sigma\beta}\circ\overline{\iota\gamma} \pitchfork \zeta\overline{\iota}\,\acute{\iota}\sigma\mathring{M}\overline{\iota\gamma}\ ,$$

gdje je $\overline{\sigma\beta} = 202, \overline{i\gamma} = 13, \bar{i} = 10$. Grci su brojeve označavali kao slova, samo s povlakom iznad njih.

Zanimljivo je spomenuti da se u Europi u srednjem vijeku koristila Diofantova notacija, ali se nije znalo da je on zaslužan.

2.2. Diofant i teorija brojeva

Diofant nije proučavao teoriju brojeva, ali se u njegovom rješavanju jednadžbi pojavljuju neki elementi iz teorije brojeva. Na primjer, prilikom postavljanja problema ili njegova rješavanja, Diofant je ponekad promatrao uvjete u kojima je problem rješiv ili ne, ili navodi neka svojstva brojeva koja koristi u rješavanju.
Osim toga, Diofant se u Arithmetici pozivao na neke primjedbe vezane uz teoriju brojeva koje su navedene u knjizi Porizmi.
Navedimo neke primjere iz Arithmetice gdje se vidi Diofantov doticaj s teorijom brojeva:
Problem 28 u prvoj knjizi glasi:
"Pronaći dva broja čija je suma jednaka zadanom broju, i suma njihovih kvadrata jednaka nekom drugom zadanom broju".
U modernoj algebarskoj notaciji, potrebno je pronaći brojeve koji x, y koji zadovoljavaju $x + y = a, x^2 + y^2 = b$, gdje su a, b unaprijed zadani brojevi.
Diofant je odmah poslije postavljenog problema napisao nužan uvjet:
"Dvostruki zbroj kvadrata traženih brojeva mora biti veći od kvadrata njihova zbroja za neki kvadrat", tj.

$$2(x^2 + y^2) - (x + y)^2 = \square.$$

Budući da je bio običaj antičkih matematičara navoditi samo one tvrdnje koje znaju dokazati, pretpostavlja se da je Diofant znao dokazati svaku svoju navedenu tvrdnju.

3. Diofantov utjecaj na druge matematičare

Poslije pada Rimskog Carstva (4. st.), arapski matematičari su preuzeli Diofantov princip simbolike. Također su koristili riječi za označavanje potencija nepoznanice (vidjeti [4], str 47.).

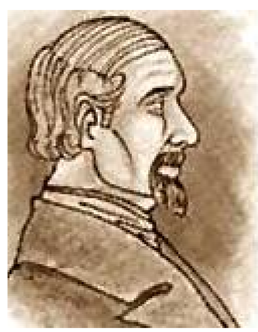
U srednjem vijeku su skoro svi algebraičari koristili Diofantova pravila za operacije s polinomima i jednadžbama (vidjeti [4], str 48.) dok negativni brojevi nisu bili prihvaćeni. Arapski matematičari ih nisu uopće koristili, a europski su ih prihvatili sa sumnjom (trudili su se izbjegavati njihovo korištenje).

Paradoksalno je to da se u Europi u 15 i 16 stoljeću koristi Diofantova algebra sa simbolima, ali se nije znalo da je Diofant zaslužan. Čak ni poznati algebraičari tog doba, kao Cardano i Tartaglia, nisu znali ništa o Diofantu.

3.1. Diofant i matematičari 16. stoljeća

U 16. stoljeću rimski matematičar Pacci pronašao je Diofantov rukopis u knjižnici u Vatikanu. Zajedno s Rafaelom Bombelli preveo je Diofantovu knjigu, ali je njihov prijevod izgubljen.

Rafael Bombelli (1526 – 1572) bio je profesor na sveučilištu u Bologni (Italija) 1572. godine.



Slika 3.1 *Rafael Bombelli*

Najpoznatiji je po svojoj knjizi *Algebra* objavljenoj 1572. godine u kojoj je naveo probleme iz Diofantove Arithmetice. Za Diofanta je rekao da je ”vrlo obrazovan u znanosti o brojevima”.

Slika 3.2 *Bombellijeva Algebra*

Bombellijeva Algebra je bitan rad jer sadrži poboljšanu notaciju za potencije nepoznanica. Prvi put se pojavljuju i kompleksni brojevi $a + bi, i^2 = -1$, uključujući precizna pravila za operacije između kompleksnih brojeva. Može se zaključiti da je Arithmetica utjecala na cijelu Bombellijevu knjigu.

Tri godine nakon objavljivanja Bombellijeve Algebre, Holtzman je napisao prvu verziju Diofantove Arithmetice na latinskom jeziku.

1585. godine matematičar i mehaničar Simon Stevin u svojoj knjizi proučava probleme prve 4 knjige Diofantove Arithmetice, a drugo izdanje ove knjige izdao je algebraist Albert Girard, koji je uključio probleme ostale dvije knjige.

Ali, Diofantove metode su imale najveću primjenu u radovima dvojice velikih francuskih matematičara 16. i 17. stoljeća, Francois Viete i Pierre Fermat.

3.2. Francois Viete

Francois Viete (1540. – 1603.) bio je francuski matematičar koji je najpoznatiji po svojim formulama koje povezuju rješenja i koeficijente algebarske jednadžbe i koje se njemu u čast i zovu *Vieteove formule.* Najpoznatija njegova knjiga je *Zetetics* u kojoj se bavio algebarskim problemima, uključujući i probleme iz Diofantove Arithmetice.

Slika 3.3 *Francois Viete*

Prije njega nije se znalo mnogo o algebri. On je prvi nakon Diofanta koji se bavio algebrom. Proširio je Diofantovu notaciju uvođenjem simbola za poizvoljne konstantne veličine (parametre) u problemima te ga se često naziva *ocem moderne algebarske notacije* (vidjeti [4], str 51). Osim toga, Diofant je imao više oznaka za potencije nepoznanica što je zbunjivalo. Viete je uveo jedinstvene oznake: A *quadratum* ili kraće A q za kvadrat i A *cubum*, tj. A c za kub. Iako ovo nije notacija koju danas koristimo, pomoću ovih jedinstvenih oznaka bilo je puno lakše razumjeti što je kvadrat, a što kub (vidjeti [13]).

3.3. Pierre de Fermat

Pierre de Fermat (1601 – 1665) bio je francuski matematičar koji je značajno doprinio u nekoliko matematičkih grana kao što su algebra, analitička geometrija, geometrija, teorija brojeva, teorija vjerojatnosti.

Slika 3.4 *Pierre de Fermat*

Za ovaj rad bitno je spomenuti da je proučavao Diofantske i Pellove jednadžbe. Pri rješavanju je koristio Diofantove metode, ali je ipak bilo neke razlike.
Dok je Diofant bio zadovoljan pronalaskom jednog rješenja, čak i racionalnog, Fermat je tražio

cjelobrojna rješenja, i to sva moguća opća rješenja.

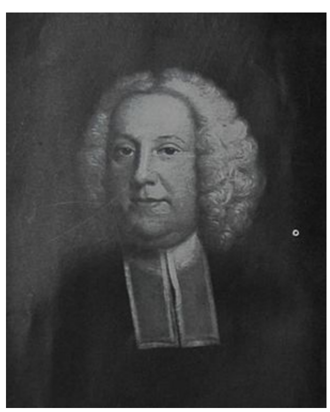
1621. Bachet de Meziriac preveo je Diofantovu Arithmeticu i ovaj prijevod je bio puno bolji od Holtzmanova. Ovo izdanje je postalo poznato, ne samo zbog kvalitete prijevoda i detaljnih komentara, već zato što je Fermat u svojoj kopiji ovog prijevoda bilježio svoje misli i rezultate koji se odnose na teoriju brojeva.

Ranije smo spomenuli Diofantov problem traženja Pitagorinih trojki koji je postao poznat zahvaljujući Fermatu.
U svojoj kopiji Diofantove Arithmetice, na margini na strani 62 u knjizi II, Fermat je 1637. godine napisao da ne postoje prirodni brojevi x, y, z i broj $n > 2$ koji zadovoljavaju jednadžbu: $x^n + y^n = z^n$ te dodao "Imam zaista sjajan dokaz ove tvrdnje, ali je margina za njega preuska". Fermat je dokazao ovu tvrdnju za $n = 4$ pomoću metode beskonačnog spusta koju je sam uveo. O tome će biti riječi kasnije.
Ovaj teorem naziva se *Fermatov veliki teorem* i izazvao je pravu pomutnju jer ga nitko preko više od 300 godina nije uspjevao dokazati, sve do engleskog matematičara John Wiles koji ga je dokazao 1994. godine.

Osim toga, Fermat je poznat i po teoremu naziva *Mali Fermatov teorem* koji se bavi djeljivošću prostim brojem.

3.4. John Pell

John Pell (1611. — 1685.) je bio engleski matematičar koji se bavio algebrom i teorijom brojeva.



Slika 3.5 *John Pell*

Poznat je po tome što je 1672. godine izdao tablicu kvadratnih brojeva do deset tisuća i po Pellovim jednadžbama o kojima će biti riječi kasnije.

3.5. Leonhard Euler

Leonhard Euler (1707 – 1783) bio je švicarski matematičar koji se bavio proučavanjem elementarne i diferencijalne geometrije, teorije grafova, infinitezimalnog računa, trigonometrije, algebre, teorije brojeva. Za svoju inspiraciju navodio je djela Fermata, Diofanta, Goldbacha i Pella.

Slika 3.6 *Leonhard Euler*

Najpoznatiji je po tome što je definirao eksponencijalnu funkciju, logaritme negativnih i kompleksnih brojeva. Također, mnogi elementi matematike nose njegovo ime: Eulerova formula, Eulerova konstanta, Eulerov broj.
Rješavao je mnoge diofantske i Pellove jednadžbe (vidjeti [4], str 59), te tako postoji i Eulerova metoda kojom se rješavaju linearne diofantske jednadžbe drugog reda.

Napisao je knjigu *Algebra* gdje je u skupu racionalnih brojeva rješavao jednadžbe oblika

$$y^2 = ax^2 + bx + c$$

i

$$y^2 = ax^3 + bx^2 + cx + d.$$

Pri rješavanju je koristio Diofantove metode sekante i tangente.
Osim toga, Euler je koristeći Fermatovu metodu beskonačnih spusta dokazao Fermatov teorem za $n = 3, 4$.

Navedimo sada dva Diofantova problema koji se bave rješavanjem neodređenih jednadžbi.

4. Problem 8 knjiga II

Jedan od najpoznatijih Diofantovih problema je onaj u kojem je Pitagorin teorem promatrao na drukčiji način nego Pitagora (vidjeti [8]), a naveden je u Arithmetici kao problem 8 u knjizi II.

Teorem 4.1. ***Pitagorin teorem***
U pravokutnom trokutu vrijedi da je kvadrat hipotenuze jednak zbroju kvadrata kateta.

Spomenimo još i sljedeću definiciju.

Definicija 4.1. *Uređenu trojku prirodnih brojeva* (x, y, z) *zovemo* Pitagorina trojka *ako vrijedi* $x^2 + y^2 = z^2$.

Diofant je promatrao sljedeći problem: "Zadani kvadrat rastaviti na sumu dva kvadrata".
U modernoj algebarskoj notaciji, Diofantov problem je u biti traženje Pitagorinih trojki rješavanjem neodređene kvadratne jednadžbe.

Ovaj problem je postao poznat jer je Fermat u svojoj kopiji Diofantove Arithmetike upravo pored ovog primjera postavio svoj veliki teorem koji se naziva *Fermatov veliki teorem.* O tome će biti riječi kasnije.

4.1. Diofantovo rješenje

Diofant pretpostavlja da je zadani kvadrat broj 16, te traži dva kvadrata koja u sumi daju 16. Budući da je imao oznaku samo za jednu nepoznanicu, prvi pribrojnik je označio s x^2, a drugi s $16 - x^2$. Diofant je znao da Pitagorinih trojki ima beskonačno mnogo, te je drugi kvadrat lukavo zapisao kao $(mx - 4)^2$, gdje je $m \in \mathbb{Z}$. Za umanjitelj je uzeo broj 4 kako bi se poslije poništio sa 16 na lijevoj strani da ne bude slobodnih koeficijenata. Uočimo da ova supstitucija vodi samo do racionalnih rješenja i da se za različite vrijednosti koeficijenta m dobiju različita rješenja.
Diofant je uzeo $m = 2$, te dobio

$$16 - x^2 = (2x - 4)^2 = 4x^2 - 16x + 16,$$

tj.

$$5x^2 = 16x.$$

Sada je podijelio obje strane s x (budući da ne poznaje 0 kao broj) te dobio

$$5x = 16$$

iz čega slijedi $x = \frac{16}{5}$, pa je prvi kvadrat jednak $\left(\frac{16}{5}\right)^2 = \frac{256}{25}$, a drugi $\left(2 \cdot \frac{16}{5} - 4\right)^2 = \left(\frac{12}{5}\right)^2 = \frac{144}{25}$.
Dobiveni kvadrati u sumi daju

$$\frac{256}{25} + \frac{144}{25} = \frac{400}{25} = 16.$$

Dakle, rješenje problema je

$$16 = 4^2 = \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2.$$

4.2. Generalizacija Diofantova rješenja

U problemu se promatra neodređena kvadratna jednadžba oblika $x^2+y^2 = a^2$, gdje je a zadani pozitivan racionalan broj.
Diofantova ideja bilo je uvesti supstituciju $y = mx - a$, iz čega se dobije

$$a^2 = x^2 + (mx - a)^2 = x^2 + m^2x^2 - 2amx + a^2,$$

odnosno

$$x(x(1 + m^2) - 2am) = 0.$$

Rješavanjem ove jednadžbe dobije se $x = 0$ i $x = \frac{2am}{m^2+1}$.
Da je Diofant koristio supstituciju $mx + a$, za rezultat bi dobio negativan broj, a on je tražio samo pozitivna rješenja.

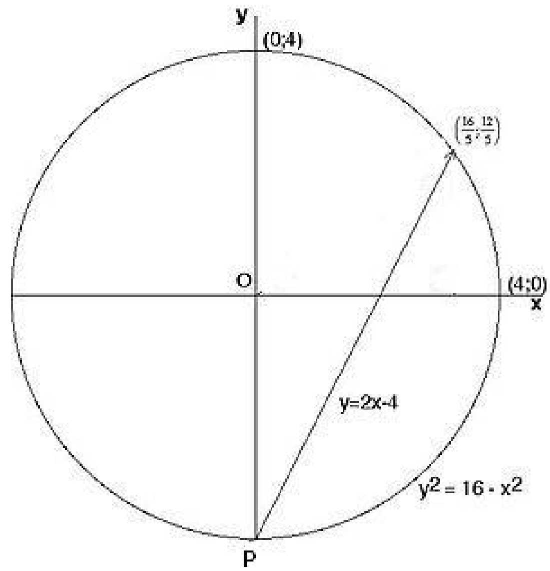
4.3. Moderna geometrijska interpretacija

Na početku 20. stoljeća otkrivena je geometrijska interpretacija Diofantovih supstitucija.
Promotrimo točku $(x, y) \in \mathbb{R}^2$ koja zadovoljava zadanu jednadžbu $x^2 + y^2 = a^2$. Geometrijski, ovo je u stvari jednadžba kružnice, a točka (x, y) leži na toj kružnici.
Promotrimo jednu očitu racionalnu točku, npr. $P(0, -a)$ i pravac koji prolazi kroz tu točku.
Sa zadanim koeficijentom pravca $m \in \mathbb{Q}$, jednadžba pravca je $y+a = m(x-0)$, tj. $y = mx-a$.
Ovaj pravac siječe kružnicu u još jednoj točki čije koordinate dobivamo rješavanjem sustava jednadžbi

$$x^2 + y^2 = a^2$$

$$y = mx - a.$$

Rješenja su $x = 0$ i $x = \frac{2am}{m^2+1}$. Prvo rješenje odgovara točki P, dok iz drugog rješenja dobijemo koordinate druge točke sjecišta $\left(\frac{2am}{m^2+1}, \frac{a(m^2-1)}{m^2+1}\right)$.
Budući da je a racionalan broj, za bilo koji racionalan broj m, pomoću ovih formula dobije se racionalna točka koja zadovoljava traženu jednakost.
Na sljedećoj slici prikazana je situacija Diofantova rješenja $(a = 4, m = 2)$ kada tražena točka ima koordinate $\left(\frac{16}{5}, \frac{12}{5}\right)$.



Slika 4.1 *Geometrijska interpretacija Diofantova rješenja*

5. Problem 16 knjiga V

Promotrimo jedan problem kojeg je Diofant u svojoj Arithmetici naveo kao problem 16 u petoj knjizi.
Problem glasi: Pronaći tri broja takva da kub njihove sume umanjen za neki od ta tri broja daje kub.
Problem se u biti bavi rješavanjem neodređene kubne jednadžbe i dobar je pokazatelj Diofantova utjecaja na druge matematičare jer su mnogi proučavali neobično Diofantovo rješavanje, te pokušavali dokazali porizam kojeg je Diofant koristio pri rješavanju.
Spomenimo još da su problemi 15 i 17 u istoj knjizi slični ovom problemu.
Problem 15 glasi: Pronaći tri broja takva da kub njihove sume uvećan za neki od njih daje kub, a problem 17: Pronaći tri broja takva da neki od njih umanjen za kub njihove sume daje kub.

5.1. Diofantovo rješenje

Diofant je pretpostavio da je suma tražena tri broja jednaka x, a da su brojevi oblika $\frac{7}{8}x^3$, $\frac{26}{27}x^3$, $\frac{63}{64}x^3$. Tada je

$$\frac{4877}{1728}x^3 = x. \tag{1}$$

Diofant je uzeo ovaj oblik brojeva jer je

$$x^3 - \frac{7}{8}x^3 = \frac{1}{8}x^3 = \left(\frac{x}{2}\right)^3.$$

Analogno se dobije s druga dva broja.
Iz (1) slijedi $x^2 = \frac{1728}{4877}$, te je zaključio da će problem biti riješen ako je razlomak $\frac{4877}{1728}$ jednak omjeru dva kvadrata. Spomenimo još, da je tada razlomak $\frac{4877}{1728}$ jednak kvadratu nekog broja.

Diofant je problem traženja brojeva sveo na problem traženja kubova s desne strane jednakosti.
Kako bi bilo lakše pratiti Diofantovo rješenje, definirajmo probleme na sljedeći način:

$$x^3 - x_1 = a^3$$

$$x^3 - x_2 = b^3$$

$$x^3 - x_3 = c^3.$$

Zbrajanjem ove tri jednakosti dobije se

$$3x^3 - (x_1 + x_2 + x_3) = 3x^3 - x = a^3 + b^3 + c^3,$$

iz čega slijedi

$$x = 3x^3 - (a^3 + b^3 + c^3).$$

Dalje iz (1) imamo

$$\frac{4877}{1728}x^3 = 3x^3 - (a^3 + b^3 + c^3).$$

Sada za $x = 1$ vrijedi

$$\frac{4877}{1728} = 3 - (a^3 + b^3 + c^3).$$

Ako ova jednakost vrijedi za određeni x, onda mora vrijediti i za svaki x.
Iz prethodne jednakosti može se zaključiti da kubovi a^3, b^3, c^3 moraju biti manji od 1.
Također, iz rasprave o razlomku $\frac{4877}{1728}$ slijedi da tada $3-(a^3+b^3+c^3)$ mora biti kvadrat nekog broja. Iz ovog je vidljivo da kvadrat mora biti manji od 3.
Diofant je ovdje počeo promatrati slučaj kada je i suma kubova manja od 1. Tada slijedi da je kvadrat veći od 2 te je Diofant za njegovu vrijednost uzeo broj $2\frac{1}{4} = \frac{9}{4}$. Sada vrijedi

$$3 - (a^3 + b^3 + c^3) = \frac{9}{4}.$$

Bachet i Fermat pokušali su objasniti Diofantov izbor jer je to jedini broj između 2 i 3 koji odgovara, ali nisu uspjeli.
Iz prethodne jednakosti dobije se da je suma kubova jednaka

$$a^3 + b^3 + c^3 = 3 - \frac{9}{4} = \frac{3}{4}.$$

Cilj je zapisati razlomak $\frac{3}{4}$ kao sumu neka tri kuba.
Proširivanjem s 54 dobije se $\frac{3}{4} = \frac{162}{216}$. Ovako prošireni razlomak je odgovarao Diofantu jer je nazivnik $216 = 6^3$ što je potrebno jer su a^3, b^3, c^3 kubovi, a brojnik je potrebno rastaviti na sumu tri kuba. Diofant je znao da vrijedi $162 = 125 + 64 - 27 = 5^3 + 4^3 - 3^3$ i pomoću tvrdnje 3 iz Porizma: "razlika dva kuba može se zapisati kao suma dva kuba", zaključio je da se mogu pronaći tražena tri kuba.
Međutim, Diofant nije zapisao konačna rješenja, već je samo komentirao kako doći do njih.

Viete je pronašao formule da se razlika dva kuba $a^3 - b^3$ zapiše kao suma dva kuba $x^3 + y^3$ (ovo su novi a, b, x):

$$x = b\frac{2a^3 - b^3}{a^3 + b^3}$$

$$y = a\frac{a^3 - 2b^3}{a^3 + b^3}.$$

Ove formule su objašnjene u sljedećem potpoglavlju.
Upotrebom formula dobije se

$$x = \frac{40}{91}, y = \frac{303}{91}$$

te imamo
$$a^3+b^3+c^3=\frac{162}{216}=\left(\frac{5}{6}\right)^3+\left(\frac{303}{91\cdot 6}\right)^3+\left(\frac{40}{91\cdot 6}\right)^3,$$
tj. sređivanjem se dobiju tražena tri kuba
$$a^3+b^3+c^3=\left(\frac{5}{6}\right)^3+\left(\frac{101}{182}\right)^3+\left(\frac{20}{273}\right)^3.$$

Diofant je sada otkrio koliko iznosi suma tražena tri broja $x=x_1+x_2+x_3$ tako što se iz rasprave o razlomku $\frac{4877}{1728}$ i kvadratu $\frac{9}{4}$ može zaključiti da se taj razlomak može predstaviti tim kvadratom te iz (1) slijedi
$$x=\frac{9}{4}x^3$$
iz čega se dobije $x=\frac{2}{3}$. Diofant je sada zaključio da su ovime pronađeni traženi brojevi.

Mi ćemo nastaviti dalje, da otkrijemo kako točno oni izgledaju.
Prisjetimo se da vrijedi
$$\frac{9}{4}=3-(a^3+b^3+c^3)$$
što se može zapisati u obliku
$$\frac{9}{4}=(1-a^3)+(1-b^3)+(1-c^3).$$
Kako vrijedi jednakost $x=\frac{9}{4}x^3$, množenjem s x^3 dobivamo
$$\frac{9}{4}x^3=x=(1-a^3)x^3+(1-b^3)x^3+(1-c^3)x^3.$$
Budući da x predstavlja sumu tražena tri broja, zaključujemo da su $(1-a^3)x^3,(1-b^3)x^3$, $(1-c^3)x^3$ traženi brojevi.
Točnije, traženi brojevi jednaki su
$$x_1=\left(1-\left(\frac{5}{6}\right)^3\right)\cdot\left(\frac{2}{3}\right)^3=\frac{91}{216}\cdot\frac{8}{27}\approx 0.1248$$
$$x_2=\left(1-\left(\frac{101}{182}\right)^3\right)\cdot\left(\frac{2}{3}\right)^3=\frac{4998267}{6028568}\cdot\frac{8}{27}\approx 0.2457$$
$$x_3=\left(1-\left(\frac{20}{273}\right)^3\right)\cdot\left(\frac{2}{3}\right)^3=\frac{20338417}{20346417}\cdot\frac{8}{27}\approx 0.2962.$$

5.2. Vieteovo rješenje porizma

Viete je u svojoj knjizi Zetetics proučavao porizam 3 u obliku

$$a^3 - b^3 = x^3 + y^3 \text{ , za } a > b > 0 \text{ i } x, y > 0, \tag{2}$$

gdje su a^3, b^3 zadani, a x^3, y^3 traženi kubovi.

Ovaj problem riješio je pomoću Diofantove metode tangente uvođenjem supstitucije $x = t - b, y = a - kt$ pomoću koje se dobije

$$t^3(1-k^3) + 3t^2(ak^2 - b) + 3t(b^2 - a^2k) = 0.$$

Tada stavlja $b^2 - a^2k = 0$ što je ekvivalentno uvjetu da je $y = a - k(x+b)$ tangenta na krivulju (2) u točki $(-b, a)$ i pomoću $k = \frac{b^2}{a^2}$ iz prethodne jednakosti dobije

$$t = \frac{3a^3b}{a^3 + b^3}.$$

Sada se lako dobiju traženi brojevi

$$x = b\frac{2a^3 - b^3}{a^3 + b^3}$$

$$y = a\frac{a^3 - 2b^3}{a^3 + b^3}.$$

Osim ovog, promatrao je dva analogna problema: "suma dva kuba može se zapisati kao razlika dva kuba" i "razlika dva kuba jednaka je razlici druga dva kuba", tj.

$$a^3 + b^3 = x^3 - y^3 \text{ , za } x > y > 0 \text{ i } a, b > 0$$

$$a^3 - b^3 = x^3 - y^3 \text{ , za } x > y > 0 \text{ i } a > b > 0.$$

Ove probleme je također riješio pomoću Diofantove metode tangenti i dobio slične formule za x, y.

Ukratko, može se reći da je Viete proučavao jednadžbu oblika

$$x^3 + y^3 + z^3 = v^3$$

te da njegove formule uključuju i negativna rješenja.

Euler je zaključio da se pomoću Vieteovih formula ne dobiju sva moguća rješenja, te je općenitije promatrao ovaj problem - u 3 slučaja:

- kada je poznat jedan kub
- kada nije poznat nijedan kub
- pronaći sve skupove brojeva takvi da tri kuba u sumi daju kub.

Objašnjavanje ovih slučajeva izlazi iz okvira naše teme, za detaljnije informacije vidjeti [7], str 329.

Iz Vieteovih formula vidljivo je da su rješenja pozitivna samo ako je $a^3 > 2b^3$ što je u suprotnosti s Diofantovom tvrdnjom.

5.3. Fermatovo rješenje porizma

Fermat je riješio ovaj nesporazum ponavljanjem Diofantove metode tangente (vidjeti [4], str 52).
Zaključio je da, ako uvjet $a^3 > 2b^3$ nije zadovoljen, prvo se mogu primjeniti Vieteove formule iz 3. problema, pa razliku dva kuba zapišemo pomoću razlike druga dva kuba. Postupak se ponavlja dok uvjet ne bude zadovoljen, i tada se koriste Vieteove formule iz 1. problema, i zadana razlika dva kuba se može zapisati kao suma druga dva kuba.
Osim navedenih problema, Fermat je proučavao i jednadžbu

$$x^3 + y^3 = a^3 + b^3,$$

tj. problem "suma dva kuba može se zapisati kao suma dva kuba" i došao do sličnih zaključaka.

6. Diofantske jednadžbe

Diofant je prvi sustavno proučavao jednadžbe s više nepoznanica, i tražio je pozitivna racionalna rješenja, nikad cjelobrojna.
Njemu u čast takve jednadžbe dobile su njegovo ime.

Moderna definicija diofantske jednadžbe je

Definicija 6.1. *Diofantska jednadžba je jednadžba oblika*

$$f(x_1, x_2, ..., x_n) = 0,$$

gdje je f polinom u n varijabli, $n \geq 2$, s cjelobrojnim koeficijentima.
Uređena n – torka cijelih brojeva $(x_1^0, x_2^0, ..., x_n^0)$ koja zadovoljava danu jednadžbu naziva se rješenje jednadžbe.
Jednadžba koja ima jedno ili više rješenja naziva se rješiva jednadžba.

U vezi s diofantskim jednadžbama postavljaju se sljedeća tri problema:

1. Je li jednadžba rješiva, tj postoji li rješenje jednadžbe?

2. Ako je jednadžba rješiva, ima li konačno ili beskonačno mnogo rješenja?

3. U slučaju rješivosti odrediti sva rješenja jednadžbe.

Proučavanje diofantskih jednadžbi ovog tipa nastavilo se kod kineskih matematičara u 3. stoljeću, Arapa u 8 – 12 stoljeću, te kasnije sve do Fermata, Eulera, Lagrangea, Gaussa i mnogih drugih.
Danas se diofantske jednadžbe rješavaju pomoću geometrijskih i algebarskih metoda te se taj dio matematike naziva *diofantska analiza.*

Promotrimo sada najpoznatije diofantske jednadžbe, linearne i Pellove.

6.1. Linearne diofantske jednadžbe

Definicija 6.2. *Linearna jednadžba oblika*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{3}$$

gdje su $a_1, a_2, ..., a_n, b$ cijeli brojevi, $n \geq 1$, naziva se linearna diofantska jednadžba.

Za linearne diofantske jednadžbe vrijedi sljedeći teorem

Teorem 6.1. *Jednadžba (3) je rješiva ako i samo ako vrijedi $(a_1, a_2, ..., a_n)|b$.*

Dokaz. Za dokaz vidjeti [1], str 59. □

Postoji više metoda rješavanja linearnih diofantskih jednadžbi. Navest ćemo *Eulerovu metodu* koja se koristi za rješavanje linearne diofantske jednadžbe $ax + by = c$.

Rješavanje ove jednadžbe ekvivalentno je rješavanju kongruencije $ax \equiv c \pmod{b}$. Ovo znači da $b|(ax - c)$, tj. $ax - c = by$. Budući da je y proizvoljan broj, vrijedi i $ax - c = -by$ iz čega slijedi $ax + by = c$ i došli smo do početne jednadžbe.
Eulerova metoda temelji se na svođenju jednadžbe na kongruenciju modulo najmanji koeficijent. Dobivena kongruencija se pojednostavi i svede na jednadžbu. Postupak se ponavlja sve dok se ne dobije kongruencija u kojoj je na lijevoj strani neka varijabla s koeficijentom 1. Sada je poznat njezin oblik i vraća se unazad kako bi se dobile ostale varijable.
Promotrimo jedan primjer iz kojeg će nam ova metoda biti jasnija.

Primjer 6.1. *Odrediti sva cjelobrojna rješenja jednadžbe*

$$5x - 2y = 7.$$

Rješenje:
Provjerimo prvo je li jednadžba uopće rješiva: vrijedi $(5, 2) = 1|7$ *pa po teoremu zaključujemo da je.*
Promotrimo ovu jednadžbu modulo najmanji koeficijent, tj. modulo 2. Sada imamo

$$5x \equiv 7 \ (mod\ 2),$$

tj.

$$x \equiv 1 \ (mod\ 2), \tag{4}$$

budući da je $5 \equiv 1$ *(mod 2) i* $7 \equiv 1$ *(mod 2).*
Iz kongruencije (4) slijedi da je $x = 1 + 2t, t \in \mathbb{Z}$, *a uvrštavanjem ovog izraza u početnu jednadžbu dobije se* $y = 5t - 1, t \in \mathbb{Z}$.

Nelinearne diofantske jednadžbe su jednadžbe u kojima se nepoznanice, osim u prvoj potenciji, pojavljuju i u potencijama višeg reda (npr. x^2, xy, x^3). Dokazano je da nema opće metode kojom bi se za svaku nelinearnu diofantsku jednadžbu moglo utvrditi ima li cjelobrojna rješenja.

6.2. Pellove jednadžbe

Definicija 6.3. *Diofantska jednadžba oblika*

$$x^2 - dy^2 = 1,$$

gdje je d prirodan broj koji nije potpun kvadrat naziva se Pellova jednadžba.

Ime joj je dao Leonhard Euler u svojoj knjizi Algebra. Po svemu sudeći, ove zasluge pogrešno su pripisane Pellu jer, iako je rješavao ovakve jednadžbe, nije bitno pridonio njihovoj teoriji. Neke jednadžbe ovog tipa nalaze se u tekstovima starogrčkih matematičara kao što su Arhimed i Diofant koji je proučavao drukčiji oblik Pellove jednadžbe oblika $a^2x^2 + c = y^2$. Međutim, prvi koji su sustavno proučavali Pellove jednadžbe su srednjovjekovni indijski matematičari od kojih je najbitniji Brahmagupta. Od europskih matematičara, metode za rješavanje Pellovih jednadžbi dali su Brouncker, Fermat, Euler i Lagrange.

Pierre de Fermat je prvi europski matematičar koji je jednadžbi pridao veći značaj.
1657. godine dao je tvrdnju bez dokaza, da ako je d pozitivan i nije kvadrat, onda Pellova jednadžba ima beskonačno mnogo rješenja (vidjeti [1], str 105).

Negativna Pellova jednadžba zadana je kao

$$x^2 - dy^2 = -1,$$

gdje je $d > 1$ i nije kvadrat.
Grytczuk, Luca and Wójtowicz su pokazali da jednadžba ima rješenja u pozitivnim cijelim brojevima ako i samo ako postoji Pitagorina trojka (A, B, C) i pozitivni cijeli brojevi a, b takvi da vrijedi

$$D = a^2 + b^2 \text{ i } |aA - bB| = 1.$$

7. Metode rješavanja diofantskih jednadžbi

Postoji mnogo metoda za rješavanje diofantskih jednadžbi:

- metoda dekompozicije
- rješavanje diofantskih jednadžbi pomoću nejednakosti
- metoda uvođenja parametara
- metoda modularne aritmetike
- Fermatova metoda beskonačnog spusta
- metoda matematičke indukcije.

Promotrimo ih detaljnije. Primjeri i njihova rješenja su preuzeti iz [1].

7.1. Metoda dekompozicije

Metoda dekompozicije temelji se na traženju nultočaka polinoma s cjelobrojnim koeficijentima $f(x_1, x_2, ..., x_n) = 0$. Procedura se sastoji od toga da se polinom zapiše u obliku produkta

$$f_1(x_1, x_2, ..., x_n)f_2(x_1, x_2, ..., x_n) \cdots f_k(x_1, x_2, ..., x_n) = a,$$

gdje su $f_1, f_2, ..., f_n$ također polinomi s cjelobrojnim koeficijentima, te $a \in \mathbb{Z}$.

Promotrimo primjere.

Primjer 7.1. *Pronađite sva cjelobrojna rješenja jednadžbe*

$$(x^2 + 1)(y^2 + 1) + 2(x - y)(1 - xy) = 4(1 + xy).$$

Rješenje:

$$x^2y^2 - 2xy + 1 + x^2 + y^2 - 2xy + 2(x - y)(1 - xy) = 4$$
$$(xy - 1)^2 + (x - y)^2 - 2(x - y)(xy - 1) = 4$$
$$[xy - 1 - (x - y)]^2 = 4$$
$$(x + 1)(y - 1) = \pm 2$$

Dakle, imamo dva slučaja:
Ako je $(x + 1)(y - 1) = 2$ dobiju se sljedeći sustavi jednadžbi

$$\begin{cases} x + 1 = 2 \\ y - 1 = 1 \end{cases} \quad \begin{cases} x + 1 = -2 \\ y - 1 = -1 \end{cases} \quad \begin{cases} x + 1 = 1 \\ y - 1 = 2 \end{cases} \quad \begin{cases} x + 1 = -1 \\ y - 1 = -2 \end{cases}$$

čija su rješenja $(1,2),(-3,0),(0,3),(-2,-1)$.

Ako je $(x+1)(y-1)=-2$ *dobiju se sljedeći sustavi jednadžbi*

$$\begin{cases} x+1=2 \\ y-1=-1 \end{cases} \quad \begin{cases} x+1=-2 \\ y-1=1 \end{cases} \quad \begin{cases} x+1=1 \\ y-1=-2 \end{cases} \quad \begin{cases} x+1=-1 \\ y-1=2 \end{cases}$$

čija su rješenja $(1,0),(-3,2),(0,-1),(-2,3)$.

Primjer 7.2. *Neka su* p,q *prosti brojevi. Riješiti u skupu pozitivnih cijelih brojeva jednadžbu*

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{pq}.$$

Rješenje: *Ova jednadžba je ekvivalentna algebarskoj diofantskoj jednadžbi*

$$(x-pq)(y-pq)=p^2q^2.$$

Uzimajući u obzir sve pozitivne djeljitelje broja p^2q^2 *dobiju se sljedeći sustavi jednadžbi:*

$$\begin{cases} x-pq=1 \\ y-pq=p^2q^2 \end{cases} \quad \begin{cases} x-pq=p \\ y-pq=pq^2 \end{cases} \quad \begin{cases} x-pq=q \\ y-pq=p^2q \end{cases}$$

$$\begin{cases} x-pq=p^2 \\ y-pq=q^2 \end{cases} \quad \begin{cases} x-pq=pq \\ y-pq=pq \end{cases} \quad \begin{cases} x-pq=pq^2 \\ y-pq=p \end{cases}$$

$$\begin{cases} x-pq=p^2q \\ y-pq=q \end{cases} \quad \begin{cases} x-pq=q^2 \\ y-pq=p^2 \end{cases} \quad \begin{cases} x-pq=p^2q^2 \\ y-pq=1 \end{cases}$$

čija su rješenja redom

$$(1+pq,pq(1+pq))\ ,\ (p(1+q),pq(1+q))\ ,\ (q(1+p),pq(1+p)),$$

$$(p(p+q),q(p+q))\ ,\ (2pq,2pq)\ ,\ (pq(1+q),p(1+q)),$$

$$(pq(1+p),q(1+p))\ ,\ (q(p+q),p(p+q))\ ,\ (pq(1+pq),1+pq).$$

7.2. Metoda nejednakosti

Bit metode nejednakosti sastoji se u sužavanju područja mogućih vrijednosti nepoznanica u jednadžbi pomoću prikladnih nejednakosti, te razmatranju slučajeva u tako dobivenom suženom skupu.

Primjer 7.3. *Pronađite sve parove cijelih brojeva* (x,y) *takve da vrijedi*

$$x^3+y^3=(x+y)^2.$$

Rješenje:
Imamo dva slučaja:

1. *ako je* $x + y = 0$, *tada su rješenja oblika* $(k, -k), k \in \mathbb{Z}$

2. *ako je* $x + y \neq 0$, *jednadžba postaje* $(x - y)^2 + (x - 1)^2 + (y - 1)^2 = 2$. *Tada vrijedi* $(x - 1)^2 \leq 1, (y - 1)^2 \leq 1$ *iz čega slijedi da se varijable* x, y *nalaze u intervalu* $[0, 2]$, *pa su rješenja početne jednadžbe* $(0, 1), (1, 0), (1, 2), (2, 1), (2, 2)$.

Primjer 7.4. *Riješite u skupu prirodnih brojeva jednadžbu:*

$$17(xyz + xy + xz + z + 1) - 54(yz + y + z) = 0.$$

Rješenje:
Uočimo da je $xyz + xy + xz = x(yz + y + z)$ *što nam omogućuje pojednostavljenje jednadžbe.*

$$17(xyz + xy + xz) + 17(z + 1) - 54(yz + y + z) = 0$$

$$17x(yz + y + z) + 17(z + 1) - 54(yz + y + z) = 0$$

$$17(z + 1) = (54 - 17x)(yz + y + z).$$

Lijeva strana uvijek je pozitivna. Da bi desna strana bila pozitivna, nužno je $x < 4$. *Razlikujemo tri slučaja* $x = 1, 2, 3$.
Za x=1
jednadžba poprima oblik $17(z + 1) = 37(yz + y + z)$ *odnosno:*

$$17(z + 1) = 37(yz + y) + 37z \ (17 - 37y)(z + 1) = 37z.$$

Budući je lijeva strana uvijek negativna, a desna pozitivna, ta jednadžba nema rješenja u skupu prirodnih brojeva.
Za x=2
jednadžba poprima oblik $17(z + 1) = 20(yz + y + z)$ *odnosno:*

$$(17 - 20y)(z + 1) = 20z.$$

Budući je lijeva strana uvijek negativna, a desna pozitivna, ta jednadžba nema rješenja u skupu prirodnih brojeva.
Za x=3
jednadžba poprima oblik $17(z + 1) = 3(yz + y + z)$ *odnosno:*

$$(17 - 3y)(z + 1) = 3z.$$

Vidimo da mora biti $y < 6$. *Uspoređujući faktore s lijeve i desne strane vidimo da mora biti i* $17 - 3y < 3$, *odnosno* $3y > 14$, *tj.* $y > 4$.
Dakle, $y = 5$. *Iz jednadžbe slijedi da je* $z = 2$. *Polazna nelinearna diofantska jednadžba ima jedinstveno rješenje*

$$x = 3, y = 5, z = 2.$$

7.3. Metoda uvođenja parametara

U mnogo situacija, cjelobrojna rješenja diofantske jednadžbe $f(x_1, x_2, ..., x_n) = 0$ mogu se prikazati u parametarskom obliku

$$x_1 = g_1(k_1, ..., k_l)$$
$$x_2 = g_2(k_1, ..., k_l)$$
$$\vdots$$
$$x_n = g_n(k_1, ..., k_l),$$

gdje su $g_1, g_2, ..., g_n$ funkcije od l varijabli s cjelobrojnim vrijednostima i $k_1, ..., k_l \in \mathbb{Z}$. Neke diofantske jednadžbe imaju više parametarskih oblika.
Za većinu diofantskih jednadžbi nije moguće pronaći sva rješenja. U mnogim takvim slučajevima parametarska metoda osigurava dokazivanje postojanja beskonačno mnogo rješenja.

Primjer 7.5. *Dokažite da postoji beskonačno mnogo cijelih brojeva (x, y, z) koji zadovoljavaju jednadžbu*

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2.$$

Rješenje:
Uvodeći $z = -y$ jednadžba postaje

$$x^3 = x^2 + 2y^2.$$

Sada postavljajući $y = mx, m \in \mathbb{Z}$ dobivamo

$$x = 1 + 2m^2.$$

Dakle, rješenje početne jednadžbe je beskonačna familija rješenja $x = 2m^2 + 1, y = m(2m^2 + 1), z = -m(2m^2 + 1), m \in \mathbb{Z}$.

Definicija 7.1. Najveća zajednička mjera (najveći zajednički djelitelj) *dvaju brojeva je najveći broj s kojim su djeljiva oba zadana broja. Ako je najveća zajednička mjera (NZM) neka dva broja jednaka 1, kažemo da su brojevi* relativno prosti.

Primjer 7.6. *Pronađite sve trojke pozitivnih cijelih brojeva (x, y, z) takvih da vrijedi*

$$\frac{1}{x}\frac{1}{y} = \frac{1}{z}.$$

Rješenje:
Jednadžba je ekvivalentna sljedećoj jednadžbi

$$z = \frac{xy}{x+y}.$$

Neka je $d = NZM(x, y)$. Tada je $x = dm, y = dn$, tako da je $NZM(m, n) = 1$. Slijedi da je $NZM(mn, m + n) = 1$. Stoga je $z = \frac{dmn}{m+n}$ iz čega slijedi $(m + n)|d$, tj. $d = k(m + n), k \in \mathbb{Z}_+$. Dakle, rješenja jednadžbe su $x = km(m + n), y = kn(m + n), z = kmn$, gdje su $k, m, n \in \mathbb{Z}_+$.

7.4. Metoda modularne aritmetike

Modularna aritmetika je naziv za dio matematike koji proučava računske operacije s kongruencijama.

Definicija 7.2. *Neka su a i b cijeli brojevi i m prirodan broj. Za brojeve a i b kažemo da su kongruentni modulo m ako vrijedi $m|(a-b)$. Oznaka: $a \equiv b$ (mod m).*

Ova metoda pomoću kongruencija pokazuje da neka diofantska jednadžba nema rješenje.

Definicija 7.3. *Neka je $NZM(a,m) = 1$. Ako kongruencija $x^2 \equiv a$ (mod m) ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m.*

Definicija 7.4. *Neka je p neparan prost broj.* Legendreov simbol $\left(\frac{a}{p}\right)$ *definira se kao*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } a \text{ kvadratni ostatak modulo } p \\ -1, & \text{ako je } a \text{ kvadratni neostatak modulo } p \\ 0, & \text{ako } p|a. \end{cases}$$

Teorem 7.1. ***Eulerov kriterij:***

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (\text{mod } m).$$

Dokaz. Za dokaz vidjeti [5], str 29. □

Primjer 7.7. *Pokažite da jednadžba*

$$(x+1)^2 + (x+2)^2 + \cdots + (x+2001)^2 = y^2$$

nema rješenja.
Rješenje:
Uvođenjem supstitucije $x = z - 2001$ jednadžba postaje

$$(z-1000)^2 + \cdots + (z-1)^2 + z^2 + (z+1)^2 + \cdots + (z+1000)^2 = y^2.$$

Sređivanjem izraza dobije se

$$2001z^2 + 2(1^2 + 2^2 + \cdots + 1000^2) = y^2,$$

a primjenom formule za sumu prvih n kvadrata $1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$ dobivamo

$$2001z^2 + 2\frac{1000 \cdot 1001 \cdot 2001}{6} = y^2,$$

tj.

$$2001z^2 + 1000 \cdot 1001 \cdot 667 = y^2.$$

Uočimo da je lijeva strana kongruetna 2 modulo 3. Promotrimo vrijedi li isto i za desnu stranu, tj. je li 2 kvadratni ostatak modulo 3. Po Eulerovom kriteriju vrijedi

$$\left(\frac{2}{3}\right) \equiv 2^{\frac{3-1}{2}} \ (mod\ 3)$$

$$\left(\frac{2}{3}\right) \equiv 2 \ (mod\ 3),$$

tj.

$$\left(\frac{2}{3}\right) \equiv -1 \ (mod\ 3)$$

što po definiciji Legendreova simbola znači da 2 nije kvadratni ostatak modulo 3 i došli smo do kontradikcije.
Dakle, ova jednadžba nema rješenja.

Teorem 7.2. ***Mali Fermatov teorem***
Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \ (mod\ p)$. Za svaki cijeli broj vrijedi $a^p \equiv a \ (mod\ p)$.

Dokaz. Za dokaz vidjeti [5], str 18. □

Primjer 7.8. *Pokažite da jednadžba*

$$x^5 - y^2 = 4$$

nema cjelobrojnih rješenja.
Rješenje:
Promotrimo ovu jednadžbu modulo 11.
Uočimo da vrijedi:

- *ako $11|x$, tada $11|x^{10}$, iz čega slijedi $x^{10} \equiv 0 \ (mod\ 11)$*
- *ako $11 \nmid x$, tada po Malom Fermatovom teoremu vrijedi $x^{10} \equiv 1 \ (mod\ 11)$.*

Dakle,

$$(x^5)^2 = x^{10} \equiv 0 \ ili\ 1 (mod\ 11) \ za\ svaki\ x.$$

Dalje, vrijedi

$$x^5 \equiv -1, 0 \ ili\ 1 (mod\ 11)$$

iz čega slijedi $y^2 = x^5 - 4 \equiv 6, 7$ *ili* 8 *(mod* 11*). Provjerimo jesu li 6, 7, 8 stvarno kvadratni ostaci modulo 11.*
Po Eulerovom kriteriju slijedi

$$\left(\frac{6}{11}\right) \equiv 6^5 \ (mod\ 11),$$

tj.

$$\left(\frac{6}{11}\right) \equiv -1 \ (mod\ 11),$$

pa iz definicije Legendreova simbola slijedi da 6 nije kvadratni ostatak modulo 11.
Na jednak način se dobije da ni 7 ni 8 nisu kvadratni ostaci modulo 11 i došli smo do kontradikcije.
Dakle, ova jednadžba nema cjelobrojnih rješenja.

7.5. Fermatova metoda beskonačnog spusta

Fermatova metoda beskonačnog spusta (FMBS) se koristi kako bi se pokazalo da neko svojstvo ne vrijedi za nenegativne cijele brojeve. Pod pretpostavkom da je svojstvo istinito za neki pozitivan cijeli broj, potrebno je pokazati da svojstvo vrijedi i za puno manji broj. To bi značilo da postoji beskonačan padajući niz pozitivnih cijelih brojeva koji zadovoljavaju ovo svojstvo, i tu je kontradikcija budući da postoji samo konačan broj prirodnih brojeva koji su manji od početnog broja. Slijedi da svojstvo ne vrijedi ni za jedan nenegativan cijeli broj.
Pomoću ove metode Fermat je dokazao svoj veliki teorem za $n = 4$ tako što je pokazao da jednadžba $x^4 + y^4 = z^2$ nema cjelobrojnih rješenja, dok je Euler, također koristeći ovu metodu, pokazao da ne vrijedi za $n = 3, 4$.
Danas je FMBS nezamjenjiv alat u proučavanju problema diofantske analize (vidjeti [4], str 56, 42).

Postoje dva specijalna slučaja FMBS metode koji se koriste kod diofantskih jednadžbi:
FMBS prva varijanta:
Ne postoji niz nenegativnih cijelih brojeva $n_1 > n_2 > ...$
FMBS druga varijanta:
Ako niz nenegativnih cijelih brojeva $(n_i)_{i\geq 1}$ zadovoljava nejednakost $n_1 > n_2 > ...$, tada postoji i_0 takav da vrijedi $n_{i_0} = n_{i_0+1} = ...$

Primjer 7.9. *Riješite jednadžbu*

$$x^3 + 2y^3 = 4z^3$$

u skupu nenegativnih cijelih brojeva.
Rješenje:
Uočimo da je $(0, 0, 0)$ *trivijalno rješenje ove jednadžbe, pokažimo da je jedino. Pretpostavimo*

suprotno, da postoji netrivijalno rješenje (x_1, y_1, z_1). *Budući da su* $\sqrt[3]{2}, \sqrt[3]{4}$ *iracionalni, slijedi* $x_1, y_1, z_1 > 0$ *(inače rješenje ne bi bilo cjelobrojno).*
Iz $x_1^3 + 2y_1^3 = 4z_1^3$ *slijedi da* $2|x_1$, *pa se* x_1 *može zapisati kao* $x_1 = 2x_2, x_2 \in \mathbb{Z}_+$. *Tada je* $8x_2^3 + 2y_1^3 = 4z_1^3$, *tj.* $4x_2^3 + y_1^3 = 2z_1^3$ *iz čega slijedi da je* $y_1 = 2y_2, y_2 \in \mathbb{Z}_+$. *Slično se dobije i* $z_1 = 2z_2, z_2 \in \mathbb{Z}_+$. *Dakle, dobije se novo rješenje* (x_2, y_2, z_2) *takvo da je* $x_1 > x_2, y_1 > y_2, z_1 > z_2$.
Nastavljajući ovu proceduru, konstruira se niz pozitivnih cjelobrojnih rješenja $(x_n, y_n, z_n)_{n\geq 1}$ *takav da* $x_1 > x_2 > x_3 ...$, *što je u kontradikciji s FMBS prvom varijantom.*

7.6. Metoda matematičke indukcije

Matematička indukcija (MI) jak je alat koji se koristi kako bi se pokazalo da neka tvrdnja vrijedi za sve nenegativne cijele brojeve.
Neka je $P(n)$ svojstvo koje vrijedi za nenegativan broj n. Pomoću metode matematičke indukcije pokazuje se da je $P(n)$ istinita tvrdnja za svaki $n \geq n_0$, gdje je n_0 zadan nenegativan cijeli broj.
Postoji više formulacija matematičke indukcije:
MI (slaba forma) sastoji se od tri koraka:

1. provjere da je $P(n_0)$ istinita tvrdnja
2. pretpostavke da je tvrdnja $P(k)$ istinita za $k \geq n_0$
3. dokazivanja istinitosti tvrdnje $P(k+1)$.

Tada je tvrdnja $P(n)$ istinita za svaki $n \geq n_0$.

MI (s korakom s) sastoji se od tri koraka:

1. provjere da su $P(n_0), P(n_0+1), ..., P(n_0+s-1)$ istinite tvrdnje
2. pretpostavke da je tvrdnja $P(k)$ istinita za $k \geq n_0$
3. dokazivanja istinitosti tvrdnje $P(k+s)$.

Tada je tvrdnja $P(n)$ istinita za svaki $n \geq n_0$.

Primjer 7.10. *Dokazati da je jednadžba*

$$x^2 + y^2 + z^2 = 59^n,\ n \in \mathbb{N}$$

rješiva u skupu prirodnih brojeva.
Rješenje:
Za rješavanje ovog problema koristit ćemo matematičku indukciju s korakom $s = 2$ *i* $n_0 = 1$.

1. *Uočimo da je rješenje za* $n = 1$ *jednako* $(x_1, y_1, z_1) = (1, 3, 7)$, *a za* $n = 2$ $(x_2, y_2, z_2) = (14, 39, 42)$ *jer je*
$$1^2 + 3^2 + 7^2 = 59$$
$$14^2 + 39^2 + 42^2 = 59^2.$$

2. *Pretpostavimo sada da postoji rješenje jednadžbe* (x_k, y_k, z_k), *tj. da vrijedi* $x_k^2 + y_k^2 + z_k^2 = 59^k$, $k \geq 1$.

3. *Pomoću prethodne pretpostavke potrebno je pokazati da postoji rješenje jednadžbe* $(x_{k+2}, y_{k+2}, z_{k+2})$, *tj. da vrijedi* $x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^{k+2}$.

Uočimo da se definiranjem $(x_{n+2}, y_{n+2}, z_{n+2})$, $n \geq 3$ *kao*

$$x_{n+2} = 59x_n,\ y_{n+2} = 59y_n,\ z_{n+2} = 59z_n$$

dobije željeno:

$$(59x_k)^2 + (59y_k)^2 + (59z_k)^2 = 59^2(x^2 + y^2 + z^2) = 59^2 59^k = 59^{k+2}.$$

Zaključujemo da je dana jednadžba rješiva u skupu prirodnih brojeva.

8. Hilbertov 10. problem

David Hilbert (1862. - 1943.) bio je njemački matematičar koji je dao doprinos u mnogim granama matematike: teoriji brojeva, funkcionalnoj analizi, integralnim jednadzbama...

Slika 8.1 *David Hilbert*

Najpoznatiji je po konceptu *Hilbertova prostora* i po govoru kojeg je održao 1900. godine na kongresu u Parizu. U govoru je izložio 23 problema u dotadašnjoj matematici, za koje je vjerovao da će u budućnosti biti predmet istraživanja. Njegovo izlaganje smatra se najutjecajnijim govorom o matematici. Njegovi problemi jako su različiti - neki predstavljaju cijela područja matematike koja još treba istražiti, a neki su konkretniji i brzo rješeni. Hilbert je probleme podijelio u četiri grupe. U prvoj grupi nalazi se šest osnovnih problema, drugih šest odnosi se na njegova istraživanja u teoriji brojeva, treća grupa od šest problema predstavlja mješavinu algebarskih i geometrijskih problema, dok posljednjih pet opisuju Hilbertove hobije.
Sam Hilbert, kao ni njegovi učenici, nije se previše bavio rješavanjem ovih problema, već se posvetio proučavanju Hilbertovog prostora. Međutim, problemi su bili jako brzo prihvaćeni od strane mladih matematičara, koji su svoja istraživanja usmjerili u pravcima koje je Hilbert i predvidio.

Spomenimo ukratko 10. Hilbertov problem koji proučava rješivost diofantske jednadžbe, točnije postavlja sljedeće pitanje: Postoji li algoritam koji bi u konačno mnogo koraka utvrdio ima li proizvoljna diofantska jednadžba rješenje?

Prošlo je mnogo godina dok se nije pokazalo da ne postoji takav algoritam. Do tog rezultata je došao Yuri Matiyasevich 1972. godine uz pomoć radova Martina Davisa, Hilary Putnam i Julie Robinson (vidjeti [6]).

Literatura

[1] Titu Andreescu, Dorin Andrica, An introduction to diophantine equations, GIL Publishing House, Romania, 2002.

[2] Krešimir Burazin, Nelinearne diofantske jednadžbe, Osječki matematički list 7, 2007.

[3] Franka Miriam Brückler, Povijest matematike 1, Sveučilište Josipa Jurja Strossmayera, Odjel za matematiku, Osijek, 2007.

[4] Isabella Grigoryevna Bashmakova, Diophantus and Diophantine equations, The Mathematical Association of America, 1997.

[5] Andrej Dujella, Uvod u teoriju brojeva, skripta, PMF-matematički odjel, Sveučilište u Zagrebu

[6] Jeremy Gray, The Hilbert problems 1900-2000, Sveučilište Bielefeld, Odjel za matematiku, Njemačka
(dostupno na *http://www.mathematik.uni-bielefeld.de/∼kersten/hilbert/gray.html*)

[7] Sir Thomas Little Heath, Diophantus of Alexandria: A study in the history of Greek algebra, Cambridge, 1910.

[8] Paul Hewitt, A brief history of elliptic curves
(dostupno na *http://livetoad.org/Courses/Documents/132d/Notes/history_of_elliptic_curves.pdf*)

[9] Franz Lemmermeyer, Some problems of Diophantus, Bilkent University, Fakulty of science, Ankara, Turkey
(dostupno na *http://www.fen.bilkent.edu.tr/∼franz/M300/diopro.pdf*)

[10] D. S. Malik, John N. Mordeson, M.K. Sen, Fundamentals of Mathematics, 2009.

[11] Yuri Matijasevich, Hilbert's tenth problem, Nauka Publishers, 1993.

[12] Gagan Tara Nanda, Richard Han, Diophantus and Number Theory, UC Berkeley, USA
(dostupno na *http://www.ocf.berkeley.edu/ gagnanda/mathstuff/Paper%201.pdf*)

[13] Jennifer Orlansky, Francois Viete: Father of Modern Algebraic Notation, The State University of New Jersey
(dostupno na *http://www.math.rutgers.edu/courses/436/Honors02/vieta.html*)

[14] André Weil, Number Theory: An Approach Through History from Hammurapi to Legendre, Birkhäuser Boston, 2007.

[15] Eberhard Zeidler, Oxford user's guide to mathematics, Oxford University Press, 1996.

[16] *http://www.matematika.ba/istorija-matematike/poznati-zadaci-velikih-matematiara*

[17] *http://lesbillgates.hubpages.com/hub/Mathematical-greats-Diophantus*

9. Sažetak

U radu je opisan Diofantov život te njegov doprinos matematici kao i utjecaj na druge matematičare: Eulera, Fermata, Vietea. Diofant je značajan matematičar jer je prvi koji je uveo simboliku u algebru te ga se često naziva ocem algebre.
Diofantske jednadžbe su algebarske jednadžbe s dvije ili više nepoznanica s cjelobrojnim koeficijentima za koje se traže cjelobrojna ili racionalna rješenja. U radu su navedene linearne diofantske i Pellove jednadžbe, te današnje metode rješavanja diofantskih jednadžbi.
Također, ukratko je opisan Hilbertov 10. problem.

Ključne riječi: Diofant, diofantske jednadžbe, Pellove jednadžbe

10. Summary

This paper consideres a Diophantine life and his contributions to mathematics and the influence on other mathematicians: Euler, Fermat, Viete. Diophantus is a significant mathematician because it was the first who introduced symbolism into algebra, and that's why he is often called the father of algebra.
Diophantine equations are algebraic equations with two or more unknowns with integer coefficients that are looking for integer or rational solutions. The paper listed a linear Diophantine and Pell's equation, and present methods for solving Diophantine equations.
Also, the Hilbert's 10th problem is briefly described.

Keywords: Diophantus, Diophantine equation, Pell's equation

11. Životopis

Anita Kopecki rođena je 03. ožujka 1987. godine u Đakovu. 1997. godine postaje članicom Slovačkog kulturno - umjetničkog društva "Braća Banas" u Josipovcu Punitovačkom koji se bavi očuvanjem kulturnog amaterizma i njegovanjem običaja slovačke nacionalne manjine u Republici Hrvatskoj. Osnovnu školu završila je 2001. godine u Josipovcu Punitovačkom, te iste godine upisala 3. gimnaziju u Osijeku. Svake godine sudjeluje na natjecanjima iz raznih predmeta, a najbolji rezultati su državna natjecanja iz kemije i matematike.

2005. godine upisuje Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku pri Sveučilištu J. J. Strossmayera u Osijeku, te počinje primati državnu stipendiju. U zimskom semestru akademske 2008./09. godine sudjelovala je u realizaciji projekta pod nazivom *Matematika s 1/2 muke* kojemu je cilj bio uklanjanje teškoća u praćenju nastave matematike na svim sastavnicama sveučilišta.

Tijekom studija primila je nekoliko nagrada i priznanja. U siječnju 2009. godine primila je nagradu i priznanje za postignut izuzetan uspjeh (4,82) na 3. godini studija. Osim toga, u prosincu 2009. godine dobila je nagradu od *Lions Club Osijek*, a odlukom Senata Sveučilišta Josipa Jurja Strossmayera u svibnju 2010. godine primila je Rektorovu nagradu za seminarski rad pod nazivom *Primjena Fermat - Torricceli - Weberove točke u satnoj prognozi prirodnog plina* pod mentorstvom prof. dr. sc. Rudolfa Scitovski.