Elementarne metode za rješavanje diofantskih jednadžbi s primjerima i problemima s matematičkih natjecanja

Gagić, Marina

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

MARINA GAGIĆ

ELEMENTARNE METODE ZA RJEŠAVANJE DIOFANTSKIH JEDNADŽBI S PRIMJERIMA I PROBLEMIMA S MATEMATIČKIH NATJECANJA

DIPLOMSKI RAD

Split, rujan 2024.

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

ODJEL ZA MATEMATIKU

ELEMENTARNE METODE ZA RJEŠAVANJE DIOFANTSKIH JEDNADŽBI S PRIMJERIMA I PROBLEMIMA S MATEMATIČKIH NATJECANJA

DIPLOMSKI RAD

Studentica:
Marina Gagić

Mentorica:
prof. dr. sc. Borka Jadrijević

Split, rujan 2024.

TEMELJNA DOKUMENTACIJSKA KARTICA

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU
ODJEL ZA MATEMATIKU

DIPLOMSKI RAD

ELEMENTARNE METODE ZA RJEŠAVANJE DIOFANTSKIH JEDNADŽBI S PRIMJERIMA I PROBLEMIMA S MATEMATIČKIH NATJECANJA

Marina Gagić

Sažetak:

Ovaj rad se bavi najvažnijim elementarnim metodama za rješavanje diofantskih jednadžbi kao što su metoda faktorizacije, parametarska metoda, metoda modularne aritmetike, metoda matematiče indukcije i metoda Fermatovog beskonačanog spusta. Svaka od navedenih metoda je ilustrirana primjerima te odabranim problemima s različitih matematičkih natjecanja uključujući Međunarodnu matematičku olimpijadu.

Ključne riječi:

Diofantske jednadžbe, elementarne metode, Fermat.

Podatci o radu:

48 stranica

Mentorica: *prof. dr. sc. Borka Jadrijević*

Članovi povjerenstva:

doc .dr. sc. Marija Bliznac Trebješanin

Pavao Radić, mag. math.

TEMELJNA DOKUMENTACIJSKA KARTICA

Povjerenstvo za diplomski rad je prihvatilo ovaj rad *24. rujna 2024. godine*

BASIC DOCUMENTATION CARD

FACULTY OF SCIENCE, UNIVERSITY OF SPLIT

DEPARTMENT OF MATHEMATICS

MASTER'S THESIS

ELEMENTARY METHODS FOR SOLVING DIOPHANTINE EQUATIONS WITH EXAMPLES AND PROBLEMS FROM MATHEMATICAL COMPETITIONS

Marina Gagić

Abstract:

This thesis deals with the most important elementary methods for solving Diophantine equations, such as the factoring method , the parametric method, the modular arithmetic method, the method of mathematical induction, and Fermat's method of infinite descent. Each of these methods is illustrated by examples and selected problems from various mathematical competitions, including the International Mathematical Olympiad.

Key words:

Diophantine equations, elementary methods, Fermat.

Specifications:

48 pages

Mentor: *professor Borka Jadrijević*

Committee:

assistant professor Marija Bliznac Trebješanin

Pavao Radić, MMath

This thesis was approved by a Thesis commettee on *September 24, 2024*

Uvod

Diofantske jednadžbe su algebarske jednadžbe s dvije ili više nepoznanica s cjelobrojnim koeficijentima kojima se traže racionalna ili najčešće cjelobrojna rješenja. Ime su dobile po starogrčkom matematičaru Diofantu Aleksandrijskom koji ih je proučavao i prvi simbolički zapisivao.

Ne postoji jedinstveni algoritam za rješavanje diofantskih jednadžbi, stoga za njihovo rješavanje, ovisno o danoj jednadžbi, koristimo različite matematičke alate i metode. Neke diofantske jedanadžbe još nisu riješene, za rješavanje nekih je trebalo razviti nove alate ili čak nove teorije da bi ih se riješilo, dok su s druge strane mnoge diofantske jednadžbe rješive elementarnim metodama, tj. bez korištenja složenih matematičkih alata. Budući da ne postoji "univerzalni recept" za rješavanje diofantskih jednadžbi, one se često pojavljuju i kao izazovni problemi na matematičkim natjecanjima.

U ovom diplomskom radu se bavimo elementarnim metodama za rješavanje diofantskih jednadžbi. Rad je podijeljen u dva poglavlja. U prvom poglavlju ćemo predstaviti diofantske jednadžbe općenito te navesti neke poznatije diofantske jednadžbe koje su utjecale na povijest matematike. U drugom poglavlju ćemo se baviti s elementarnim metodama rješavanja diofantskih jednadžbi, kao što su metoda faktorizacije, metoda modularne aritmetike, metoda matematičke indukcije i metoda Fermatovog beskonačanog spusta. Svako potpoglavlje koncipirano je tako da prvo prezentira općeniti postu-

pak rješavanja diofantskih jednadžbi danom metodom, a zatim, kroz odabrane primjere i probleme s različitih matematičkih natjecanja, se ilustrira praktična primjena tog postupka.

Sadržaj

Poglavlje 1

Diofantske jednadžbe

Diofantske jednadžbe su jednadžbe kojima tražimo rješenja u skupu cijelih brojeva (ili nekom njegovom poopćenju). Obično su to polinomijalne jednadžbe, točnije jednadžbe oblika

$$f(x_1, x_2, ..., x_n) = 0, \tag{1.1}$$

gdje je f polinom s n, $n \geq 2$ varijabli s cjelobrojnim koeficijentima. Uređenu n-torku cijelih brojeva $(x_1^0, x_2^0, ..., x_n^0)$ koja zadovoljava jednadžbu (1.1) nazivamo rješenje te jednadžbe. Ako se nepoznanice nalaze i u eksponentima, onda govorimo o eksponencijalnim ili kombinirano polinomijalno - eksponencijalnim diofantskim jednadžbama.
Kada proučavamo diofantske jednadžbe postavljamo sljedeća pitanja:

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

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

3. *Ako je rješiva, kako odrediti sva ili barem neka rješenja?*

Za neke tipove diofantskih jednadžbi stupnja većeg od dva s dvije ili više nepoznanica, odgovori na gornja pitanja postaju prilično kompliciranI. Čak

i kod problema koji se čini jednostavan, poput određivanja je li broj rješenja konačan ili beskonačan, suočavamo se s velikim poteškoćama.

Teorijska važnost diofantskih jednadžbi je velika zbog njihove uske povezanosti s mnogim problemima teorije brojeva, ali i drugih matematičkih disciplina. Naime, mnogi matematički problemi se svode na rješavanje neke diofantske jednadžbe, dok se s druge strane pokazalo da se neke diofantske jednadžbe nisu mogle riješiti dok se nisu razvile neke nove matematičke teorije ili alati.

Diofantske jednadžbe su dobile ime po Diofantu Aleksandrijskom koji ih je prvi zapisao simbolički. Njegovo najznačajnije djelo, *Arithmetica*, sastoji se od trinaest knjiga od kojih je preživjelo samo šest i imale su velik utjecaj na druge matematičare. Knjige se bave rješavanjem algebarskih jednadžbi, posebno onih koje imaju cjelobrojna rješenja. *Arithmetica* se značajno razlikuje po stilu i sadržaju od ostalih antičkih knjiga prvenstveno zbog uporabe simbola za veličine, matematičke operacije i odnose, što je drugačiji pristup od onog koji karakterizira to doba kada su se algebarski problemi zapisivali riječima. Djelo je postavilo temelje za razvoj teorije brojeva, ključne grane moderne matematike. Nadahnulo je neke od najpoznatijih matematičara, poput Eulera, Fermata, Pella i Lagrangea, da dođu do novih i značajnih otkrića.

Neke poznatije diofantske jednadžbe koje su utjecale na povijest teorije brojeva su:

- najjednostavnija **linearna diofantska jednadžba** koja je oblika

$$ax + by = c, \quad a, b, c \in \mathbb{Z}. \tag{1.2}$$

Za linearne diofantske jednadžbe vrijedi sljedeći teorem:

Teorem 1.1 *Neka su a, b i c cijeli brojevi i $d = (a, b)$. Ako $d \nmid c$, onda*

jednadžba (1.2) nema cjelobrojnih rješenja. Ako $d \mid c$, onda jednadžba (1.2) ima beskonačno mnogo cjelobrojnih rješenja. Ako je (x_1, y_1) jedno rješenje, onda su sva rješenja dana sa $x = x_1 + \frac{b}{d} \cdot t$, $y = y_1 - \frac{a}{d} \cdot t$, gdje je $t \in \mathbb{Z}$.

- **Pellova jednadžba**

$$x^2 - Dy^2 = 1, \quad D \in \mathbb{N} \text{ i } D \text{ nije potpun kvadrat.}$$

Matematičari su se stoljećima bavili ovom jednadžbom. Posebne slučajeve Pellove jednadžbe proučavali su starogrčki matematičari, ali i Fermat u 17. stoljeću. Iako su ime dobile po John Pellu, on nije značajnije pridonio razvoju njihove teorije.

- **Pitagorina jednadžba**

$$x^2 + y^2 = z^2 \tag{1.3}$$

je jedna od najjednostavnijih diofantskih jednadžbi drugog stupnja. Iako je ime dobila po Pitagori, bila je poznata još i starim Babiloncima 1000 godina prije nego se Pitagora rodio. Uređenu trojku prirodnih brojeva (x, y, z) koja zadovoljava jednadžbu (1.3) nazivamo Pitagorina trojka.

- **Fermatova jednadžba**

$$x^n + y^n = z^n, \quad n \in \mathbb{N}, n > 2. \tag{1.4}$$

Pierre de Fermat je u svom primjerku *Arithmetice* na marginama stranice zapisao svoj posljednji teorem, tj. tvrdnju da ne postoji prirodan broj $n > 2$ za kojeg jednadžba (1.4) ima rješenje u skupu prirodnih brojeva. Dodao je da ima sjajan dokaz ove tvrdnje, ali su margine preuske za njega. Tvrdnju je tek 1995. godine dokazao britanski matematičar Andrew Wiles.

Njemački matematičar David Hilbert je 1900. godine je u okviru predavanja na Međunarodnom matematičkom kongresu predstavio popis 23 problema u matematici. Svi su u to vrijeme bili neriješeni, a neki od njih su se pokazali izuzetno utjecajnim za razvoj matematike u 20. stoljeću. U 10. problemu postavio je pitanje:

Postoji li algoritam pomoću kojeg je nakon konačno mnogo koraka moguće odrediti ima li proizvoljna diofantska jednadžba rješenje u skupu cijelih brojeva?

Hilbertov 10. problem riješen je 1972. godine kada je Yuri Matiyasevich dokazao da takav algoritam ne postoji.

Poglavlje 2

Elementarne metode rješavanja diofantskih jednadžbi

Diofantske jednadžbe nemaju jedinstven način rješavanja, ali mnoge od njih se mogu riješiti elementarnim metodama, tj. metodama koje ne koriste složene matematičke alate.

2.1 Metoda faktorizacije

Pretpostavimo da diofantsku jednadžbu $f(x_1, x_2, ..., x_n) = 0$ možemo zapisati u obliku

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

gdje su $f_1, f_2, ..., f_k \in \mathbb{Z}[X_1, X_2, ..., X_n]$ i $a \in \mathbb{Z}$. Iz rastava broja a na proste faktore, dobivamo konačno mnogo faktorizacija od a na k cjelobrojnih faktora $a_1, a_2, ..., a_k$, tj. $a = a_1 \cdot a_2 \cdot ... \cdot a_k$. Svaka takva faktorizacija daje sustav jednadžbi

$$\begin{cases} f_1(x_1, x_2, ..., x_n) = a_1, \\ f_2(x_1, x_2, ..., x_n) = a_2, \\ \vdots \\ f_k(x_1, x_2, ..., x_n) = a_k. \end{cases}$$

Rješavanjem svih takvih sustava jednadžbi dobivamo skup rješenja početne jednadžbe. Ilustrirajmo ovu metodu na nekoliko primjera.

Primjer 2.1 *Odredimo sva cjelobrojna rješenja jednadžbe*

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

(Titu Andreescu)

Rješenje. Zapišimo jednadžbu u obliku:

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

ili kao

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

Posljednju jednadžbu možemo zapisati u obliku

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

što povlači

$$(x+1)(y-1) = \pm 2$$

Ako je $(x+1)(y-1) = 2$, dobivamo četiri sustava jednadžbi:

$x+1=2$	$x+1=-2$	$x+1=1$	$x+1=-1$
$y-1=1$	$y-1=-1$	$y-1=2$	$y-1=-2$

Rješavajući sustave dobivamo rješenja: $(x,y) = (1,2), (-3,0), (0,3), (-2,-1)$.

Ako je $(x+1)(y-1) = -2$, dobivamo sustave jednadžbi:

$$x+1=2 \qquad x+1=-2 \qquad x+1=1 \qquad x+1=-1$$
$$y-1=-1 \qquad y-1=1 \qquad y-1=-2 \qquad y-1=2$$

čija rješenja su: $(x,y)=(1,0),(-3,2),(0,-1),(-2,3)$.

Ovih osam uređenih parova su sva rješenja zadane diofantske jednadžbe.

Primjer 2.2 *Nađimo sve pravokutne trokute s cjelobrojnim duljinama stranica kojima su površina i opseg jednaki.*

Rješenje. Neka su x i y duljine kateta, a z duljina hipotenuze pravokutnog trokuta. Tada, prema Pitagorinom teoremu, vrijedi $z=\sqrt{x^2+y^2}$.

Izjednačavanjem površine i opsega dobivamo jednadžbu

$$\frac{xy}{2}=x+y+\sqrt{x^2+y^2},$$

što povlači $xy-2(x+y)=2\sqrt{x^2+y^2}$. Kvadriranjem dobivamo:

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

ili ekvivalentno

$$xy(xy-4x-4y+8)=0.$$

Budući da je $xy\neq 0$ (jer su x i y duljine kateta) slijedi

$$xy-4x-4y+8=0,$$

odnosno

$$(x-4)(y-4)=8.$$

Budući da postoje četiri cjelobrojne faktorizacije od 8 na dva faktora (do na poredak faktora) dobivamo osam sustava od dvije jednadžbe s dvije nepoznanice. Budući da tražimo rješenja (x,y) u prirodnim brojevima dobivamo $(x,y)=(6,8),(8,6),(5,12),(12,5)$. Ova rješenja daju samo dva pravokutna trokuta: trokut s katetama duljina 6 i 8, duljinom hipotenuze 10 i trokut s duljinama kateta 5 i 12 i hipotenuzom duljine 13.

2.1.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.3 *Nađite sva cjelobrojna rješenja jednadžbe*

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

(Poljska matematička olimpijada)

Rješenje. Uvođenjem supstitucije $x=u+1, y=v+1$, gornja jednadžba postaje

$$(u+1)^2v+(v+1)^2u=1,$$

što je ekvivalentno s

$$uv(u+v)+4uv+(u+v)=1.$$

Posljednju jednadžbu možemo zapisati kao

$$(u+v+4)(uv+1)=5.$$

Očito, jedan od faktora na lijevoj strani gornje jednadžbe mora biti jednak 5 ili -5, a drugi 1 ili -1. Tada zbroj $u+v$ i produkt uv trebaju zadovoljiti jedan od četiri sustava jednadžbi:

$$\begin{array}{cccc} u+v=1 & u+v=-9 & u+v=-3 & u+v=-5 \\ uv=0 & uv=-2 & uv=4 & uv=-6. \end{array}$$

Samo prvi i posljednji sustavi jednadžbi imaju cjelobrojna rješenja. Ona su: $(u,v)=(0,1),(1,0),(-6,1),(1,-6)$. Budući da je $(x,y)=(u+1,v+1)$ rješenja početne jednadžbe su dana s $(x,y)=(1,2),(-5,2),(2,1),(2,-5)$.

Zadatak 2.4 *Odredite sva cjelobrojna rješenja jednadžbe* $x^6+3x^3+1=y^4$.

(Rumunjska matematička olimpijada)

Rješenje. Zapišimo jednadžbu u obliku

$$(x^3+1)^2+(x^3+1)=y^4+1,$$

što je ekvivalentno s

$$(2x^3+3)^2-4y^4=5.$$

Rastavimo li lijevu stranu jednadžbe kao razliku kvadrata dobivamo sljedeće sustave:

$$\begin{aligned} 2x^3-2y^2+3&=1 & \qquad 2x^3-2y^2+3&=-1\\ 2x^3+2y^2+3&=5 & \qquad 2x^3+2y^2+3&=-5 \end{aligned}$$

$$\begin{aligned} 2x^3-2y^2+3&=5 & \qquad 2x^3-2y^2+3&=-5\\ 2x^3+2y^2+3&=1 & \qquad 2x^3+2y^2+3&=-1 \end{aligned}$$

Sva rješenja gornjih sustava su dana s $(x,y)=(0,1),(0,-1)$.

Zadatak 2.5 *Za svaki prirodan broj n, neka $s(n)$ označava broj uređenih parova prirodnih brojeva (x,y) za koje vrijedi*

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n}. \tag{2.1}$$

Pronađite sve prirodne brojeve n za koje je $s(n)=5$.

(Indijska matematička olimpijada)

Rješenje. Budući da su x i y prirodni brojevi, jednadžba (2.1) je ekvivalentna s diofantskom jednadžbom

$$n(x+y)=xy,$$

odnosno s

$$(x-n)(y-n)=n^2.$$

Budući da je $y \in \mathbb{N}$, iz (2.1) slijedi $\frac{1}{x} < \frac{1}{n}$, što povlači $x-n > 0$, tj. $x-n \in \mathbb{N}$. Analogno, zaključujemo da je $y - n \in \mathbb{N}$. Ako je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $\alpha_i \geq 1$ kanonski rastav od n, onda n^2 ima $(2\alpha_1+1)\cdots(2\alpha_k+1)$ pozitivnih djelitelja. Svakom od pozitivnih djelitelja d od n^2 odgovara sustav

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

koji očito ima jedinstveno rješenje u prirodnim brojevima. Stoga jednadžba (2.1) ima $s(n) = (2\alpha_1 + 1)\cdots(2\alpha_k + 1)$ rješenja.
Iz

$$(2\alpha_1 + 1)\cdots(2\alpha_k + 1) = 5$$

dobivamo $k = 1$ i $\alpha_1 = 2$. Dakle, ako je $s(n) = 5$, onda je $n = p^2$, gdje je p prost broj.

Zadatak 2.6 *Riješite sljedeću jednadžbu u skupu nenul cijelih brojeva:*

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

(16. SAD matematička olimpijada)

Rješenje. Zapišimo gornju jednadžbu u obliku

$$x^3 + x^2y^2 + yx + y^3 = x^3 - 3x^2y + 3xy^2 - y^3,$$

odnosno kao

$$x^2y^2 + xy + y^3 + 3x^2y - 3xy^2 + y^3 = 0,$$

što je ekvivalentno s

$$2y^2 + (x^2 - 3x)y + 3x^2 + x = 0.$$

Ako jednadžbu promatramo kao kvadratnu jednadžbu u y, onda jednadžba ima cjelobrojna rješenja ako je njena diskriminanta $x(x+1)^2(x-8)$ potpuni kvadrat. Slijedi da je $x(x-8) = z^2$, odnosno $(x-4)^2 - z^2 = 16$, za neki $z \in \mathbb{Z}$. To je ekvivalentno s

$$(x-z-4)(x+z-4) = 16.$$

Budući da postoji šest cjelobrojnih faktorizacija broja 16 na dva faktora, dobivamo dvanaest sustava jednadžbi. Rješavajući sustave i uzimajući u obzir uvjet zadataka, tj. da je $x \neq 0$, dobivamo $x \in \{-1, 8, 9\}$. Slijedi da su sva rješenja početne jednadžbe dana s $(x, y) = (-1, 1)$, $(8, -10)$, $(9, -6)$, $(9, -21)$.

Zadatak 2.7 *Pronađite sve cijele brojeve a, b, c, gdje je $1 < a < b < c$, tako da je broj $(a-1)(b-1)(c-1)$ djelitelj od $abc - 1$.*

(33. Međunarodna matematička olimpijada)

Rješenje. Definirajmo $a-1 = x$, $b-1 = y$, $c-1 = z$. Tada je $1 \leq x < y < z$ i $xyz | (xy + yz + zx + x + y + z)$.

Ideja rješenja je dokazati da ne može vrijediti $xyz \leq xy + yz + zx + x + y + z$ za beskonačno mnogo uređenih trojki (x, y, z) prirodnih brojeva. Neka je $f(x, y, z)$ kvocijent tražene djeljivosti. Budući da je

$$f(x, y, z) = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{xy} + \frac{1}{yz} + \frac{1}{zx}$$

vidimo da je funkcija f padajuća u svakoj od varijabli x, y, z. Zbog simetričnosti i budući da su x, y, z različiti prirodni brojevi za koje vrijedi $1 \leq x < y < z$, dobivamo

$$f(x, y, z) \leq f(1, 2, 3) = 2 + \frac{5}{6} < 3.$$

Stoga, ako je djeljivost ispunjena, onda je $f(x,y,z) \in \mathbb{N}$ i vrijedi $f(x,y,z) = 1$ ili $f(x,y,z) = 2$. Dakle, moramo riješiti u skupu prirodnih brojeva jednadžbe

$$xy + yz + zx + x + y + z = kxyz, \tag{2.2}$$

gdje je $k = 1$ ili $k = 2$.
Primijetimo da je $f(3,4,5) = \frac{59}{60} < 1$. Stoga je $x \in \{1,2\}$. Također, $f(2,3,4) = \frac{35}{24} < 2$. Dakle, za $x = 2$, nužno imamo $k = 1$. Zaključujemo da je potrebno promatrati samo tri jednadžbe oblika (2.2).
Prvi slučaj. $x = 1$ i $k = 1$. Dobivamo jednadžbu

$$1 + 2(y + z) + yz = yz \Longleftrightarrow 1 + 2(y + z) = 0$$

koja očito nema rješenja u prirodnim brojevima.
Drugi slučaj. $x = 1$ i $k = 2$. Dobivamo jednadžbu

$$1 + 2(y + z) = yz.$$

Zapišemo li je u obliku $(y-2)(z-2) = 5$, dobivamo sustav $y - 2 = 1$, $z - 2 = 5$ koji ima jedinstveno rješenje $(y,z) = (3,7)$.
Treći slučaj. $x = 2$ i $k = 1$. Dobivamo jednadžbu

$$2 + 3(y + z) = yz.$$

Zapišimo gornju jednadžbu u obliku $(y-3)(z-3) = 11$. Dobivamo $y-3 = 1$, $z - 3 = 11$, pa jednadžba ima jedinstveno rješenje $(y,z) = (4,14)$.
Iz drugog i trećeg slučaja slijede rješenja: $(a,b,c) = (2,4,8), (3,5,15)$.

Zadatak 2.8 *Neka je p prost i n prirodan broj. Dokažite da jednadžba $x(x+1) = p^{2n}y(y+1)$ nije rješiva u skupu prirodnih brojeva.*
Rješenje. Pretpostavimo da gornja jednadžba ima rješenja u prirodnim brojevima. Budući da su x i $x+1$ relativno prosti prirodni brojevi, tada

vrijedi da $p^{2n}|x$ ili $p^{2n}|(x+1)$. Stoga je u svakom slučaju $p^{2n} \leq x+1$. Lijevu stranu zadane jednadžbe možemo zapisati u obliku $x^2+x = x^2+x+\frac{1}{4}-\frac{1}{4} = \left(x+\frac{1}{2}\right)^2 - \frac{1}{4}$. Slično, desnu stranu možemo zapisati kao $p^{2n}\left(\left(y+\frac{1}{2}\right)^2 - \frac{1}{4}\right)$, pa zadanu jednadžbu možemo zapisati u obliku

$$\left(x+\frac{1}{2}\right)^2 - \frac{1}{4} = p^{2n}\left(\left(y+\frac{1}{2}\right)^2 - \frac{1}{4}\right),$$

što je ekvivalentno s

$$(2x+1)^2 - 1 = p^{2n}(2y+1)^2 - p^{2n}.$$

Tada je

$$p^{2n} - 1 = p^{2n}(2y+1)^2 - (2x+1)^2 \iff$$

$$p^{2n} - 1 = (p^n(2y+1) + (2x+1))(p^n(2y+1) - (2x+1)).$$

Budući da su $p^{2n}-1, x$ i y prirodni brojevi, onda su oba faktora na desnoj strani gornje jednadžbe također prirodni brojevi pa je $p^{2n}-1 > (2x+1)\cdot 1$, što je u kontradikciji s $p^{2n} \leq x+1$. Stoga, zadana jednadžba nije rješiva u prirodnim brojevima.

Napomena Tvrdnja Zadatka 2.8 ne vrijedi ako je eksponent od p neparan. Na primjer, jednadžba

$$x(x+1) = 2^3 y(y+1)$$

ima rješenja $(x,y) = (15,5), (32,11)$.

2.2 Rješavanje diofantskih jednadžbi korištenjem nejednakosti

Ova metoda se temelji na određivanju intervala u kojima leže varijable pomoću odgovarajućih nejednakosti. Općenito, na ovaj način dolazimo do konačno mnogo vrijednosti koje mogu poprimiti sve varijable ili barem neke od njih.

Primjer 2.9 *Nađimo sve uređene parove (x, y) cijelih brojeva tako da je*

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

Rješenje. Primijetimo da su svi uređeni parovi oblika $(k, -k)$, $k \in \mathbb{Z}$ rješenja ove jednadžbe. Stoga, ako je $x \neq -y$, tj. $x + y \neq 0$, jednadžba se svodi na rješavanje jednadžbe

$$x^2 - xy + y^2 = x + y,$$

što je ekvivalentno s

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

Slijedi da je $(x - 1)^2 \leq 1$ i $(y - 1)^2 \leq 1$, pa x, y leže u intervalu $[0, 2]$. Stoga su rješenja $(x, y) = (0, 1)$, $(1, 0)$, $(1, 2)$, $(2, 1)$, $(2, 2)$.

Primjer 2.10 *Nađimo sve uređene četvorke (x, y, z, w) prirodnih brojeva za koje vrijedi*

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

(Titu Andreescu)

Rješenje. Imamo

$$(x + y + z \pm 1)^2 = x^2 + y^2 + z^2 + 2xy + 2x(z \pm 1) + 2y(z \pm 1) \pm 2z + 1.$$

Iz ovoga slijedi

$$(x+y+z-1)^2 < w^2 < (x+y+z+1)^2.$$

Stoga w^2 može biti jednako samo $(x+y+z)^2$ pa dobivamo $x^2+y^2+z^2+2xy+2x(z-1)+2y(z+1) = (x+y+z)^2$. Ovo povlači da je $x=y$ pa su rješenja dana s $(x,y,z,w) = (m,m,n,2m+n), m,n \in \mathbb{N}$.

Primjer 2.11 *Dokažimo da sve jednadžbe oblika*

$$x^6 + ax^4 + bx^2 + c = y^3,$$

gdje je $a \in \{3,4,5\}$, $b \in \{4,5,...,12\}$, $c \in \{1,2,...,8\}$, *nemaju rješenja u skupu prirodnih brojeva.*

Rješenje. Navedeni uvjeti povlače da je

$$x^6 + 3x^4 + 3x^2 + 1 < y^3 < x^6 + 6x^4 + 12x^2 + 8,$$

tj.

$$\left(x^2+1\right)^3 < y^3 < \left(x^2+2\right)^3,$$

što pokazuje da nijedna od promatranih jednadžbi nije rješiva.

2.2.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.12 *U skupu prirodnih brojeva riješite jednadžbu*

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}.$$

(Rumunjska matematička olimpijada)

Rješenje. Bez smanjenja općenitosti možemo pretpostaviti da je $x \leq y \leq z$. Iz toga slijedi da je $\frac{3}{x} \geq \frac{3}{5}$, što povlači $x \leq 5$. Očito je $x \geq 2$, pa je

$x \in \{2,3,4,5\}$.

Ako je $x = 2$, tada je $\frac{1}{y} + \frac{1}{z} = \frac{1}{10}$ pa je $\frac{1}{y} < \frac{1}{10} \leq \frac{2}{y}$, što povlači $y \in \{11,12,...,20\}$. Slijedi da je $z = 10 + \frac{100}{y-10}$ i $(y-10)\,|100$. Provjerom svih mogućnosti dobivamo rješenja $(x,y,z) = (2,11,110)$, $(2,12,60)$, $(2,14,35)$, $(2,20,20)$.

Ako je $x = 3$, tada je $\frac{1}{y} + \frac{1}{z} = \frac{4}{15}$ pa je $y \in \{3,4,5,6,7\}$. Provjerom svih mogućnosti dobivamo rješenja $(x,y,z) = (3,4,60)$, $(3,5,15)$, $(3,6,10)$.

Ako je $x = 4$, tada dobivamo $\frac{1}{y} + \frac{1}{z} = \frac{7}{20}$ pa je $y \in \{4,5\}$, a rješenje je $(x,y,z) = (4,4,10)$.

Ako je $x = 5$, tada imamo $\frac{1}{y} + \frac{1}{z} = \frac{2}{5}$ pa je $y = z = 5$, što daje rješenje $(x,y,z) = (5,5,5)$.

Zadatak 2.13 *Nađite sve uređene trojke (x,y,z) prirodnih brojeva tako da vrijedi*

$$\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right) = 2.$$

(Britanska matematička olimpijada)

Rješenje. Bez smanjenja općenitosti možemo pretpostaviti da je $x \geq y \geq z$. Primijetimo da mora vrijediti $2 \leq \left(1+\frac{1}{z}\right)^3$, iz čega slijedi da je $z \leq 3$.

Ako je $z = 1$, tada je $\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right) = 1$, što je nemoguće.

Ako je $z = 2$, tada je $\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right) = \frac{4}{3}$. Stoga je $\frac{4}{3} \leq \left(1+\frac{1}{y}\right)^2$, iz čega slijedi da je $y < 7$. Budući da je $1+\frac{1}{x} > 1$, dobivamo $\left(1+\frac{1}{y}\right) < \left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right) < \frac{4}{3}$ što povlači $y > 3$. Stoga je $y \in \{4,5,6\}$ pa dobivamo rješenja $(x,y,z) = (7,6,2)$, $(9,5,2)$, $(15,4,2)$.

Ako je $z = 3$, tada je $\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right) = \frac{3}{2}$. Slijedi da je $y < 5$ i $y \geq z = 3$. Ove vrijednosti daju rješenja $(x,y,z) = (8,3,3)$, $(5,4,3)$.

Konačno, sva rješenja su (do na permutaciju) dana s $(x,y,z) = (7,6,2)$, $(9,5,2)$, $(15,4,2)$, $(8,3,3)$ i $(5,4,3)$.

Zadatak 2.14 *Odredite sve uređene parove (x, y) cijelih brojeva koji zadovljavaju jednadžbu*

$$(x+1)^4 - (x-1)^4 = y^3.$$

(Australska matematička olimpijada)

Rješenje. Imamo $(x+1)^4 - (x-1)^4 = 8x^3 + 8x$. Neka je uređeni par (x, y) cijelih brojeva rješenje zadane jednadžbe i pretpostavimo da je $x \geq 1$. Tada je

$$(2x)^3 < (x+1)^4 - (x-1)^4 < (2x+1)^3.$$

Stoga je $2x < y < 2x+1$, što je kontradikcija. Dakle, ako je (x, y) rješenje u cijelim brojevima, onda x nije pozitivan. Uočimo da ako je (x, y) rješenje, onda je i $(-x, -y)$ također rješenje, pa ni $-x$ nije pozitivan. Stoga je $(x, y) = (0, 0)$ jedino rješenje.

Zadatak 2.15 *Nađite sve prirodne brojeve x, y, z, t takve da je*

$$\begin{cases} x^n + y = z^n, \\ x + y^n = t^n, \end{cases}$$

za neki cijeli broj $n \geq 2$.

Rješenje. Iz prve jednadžbe dobivamo $x^n = z^n - y < z^n$. Stoga je $x < z$ ili $x + 1 \leq z$. Iz iste jednadžbe dobivamo $y = z^n - x^n \geq (x+1)^n - x^n = \binom{n}{1}x^{n-1} + \binom{n}{2}x^{n-2} + \cdots > x$, tj. $y > x$. Slično, iz druge jednadžbe dobivamo $y < x$, što je kontradikcija. Dakle, ne postoje prirodni brojevi x, y, z i t s gornjim svojstvom.

Zadatak 2.16 *Nađite sve uređene parove (x, y) prirodnih brojeva takve da je $x^y = y^x$.*

Rješenje. Očito su svi uređeni parovi oblika (n, n), $n \geq 1$ rješenja ove jednadžbe. Istražimo postoje li i druga rješenja.
Bez smanjenja općenitosti možemo pretpostaviti da je $x < y$ i neka je $y = x+t$ za neki prirodan broj t. Tada jednadžba poprima oblik

$$x^{x+t} = (x+t)^x \qquad \text{ili} \qquad x^t = \left(1 + \tfrac{t}{x}\right)^x < e^t < 3^t.$$

Stoga je $x < 3$. Budući da je x prirodan broj, onda je $x = 1$ ili $x = 2$.
Ako je $x = 1$, onda je $y = 1$.
Ako je $x = 2$, onda je $2^y = y^2$, pa je $y = 2$ ili $y = 4$. Naime, za $y \geq 5$ matematičkom indukcijom možemo pokazati da je $2^y > y^2$. Stoga $2^y = y^2$, $y \in \mathbb{N}$ povlači $y = 2$ ili $y = 4$. Dakle, sva rješenja jednadžbe su dana sa $(x, y) =(2, 4), (4, 2)$ i (n, n), $n \in \mathbb{N}$.

Zadatak 2.17 *Neka su a i b prirodni brojevi takvi da $ab + 1$ dijeli $a^2 + b^2$. Dokažite da je tada $\frac{a^2+b^2}{ab+1}$ kvadrat cijelog broja.*

(29. Međunarodna matematička olimpijada)

Rješenje. Neka je (a, b) uređeni par cijelih brojeva koji zadovoljava pretpostavku. Tada je (a, b) rješenje diofantske jednadžbe

$$a^2 - kab + b^2 = k, k \in \mathbb{Z}. \tag{2.3}$$

Ako je $a = 0$ ili $b = 0$, onda je k potpuni kvadrat. Pretpostavimo da je $a \neq 0$ i $b \neq 0$. Tada a i b imaju isti predznak. Zaista, ako je $ab < 0$, tada je

$$a^2 - kab + b^2 > k.$$

Možemo pretpostaviti da je $a > 0$ i $b > 0$. To povlači da je i $k > 0$. Ako je $a = b$, dobivamo $(2 - k)a^2 = k > 0$ pa zaključujemo da je $2 - k > 0$, što povlači $k = 1$.

Konačno, pretpostavimo da je $a > b > 0$ i neka je (a, b) rješenje od (2.3) s minimalnim b. Lako se vidi da je $(b, kb - a)$ također rješenje od (2.3). Ako je $kb = a$, onda je $k = b^2$ pa je k potpuni kvadrat. Ako je $kb \neq a$, onda je $kb - a > 0$ jer mora imati isti predznak kao i b. Tvrdimo da je $kb - a < b$. Vrijedi:

$$kb - a < b \Longleftrightarrow k < \frac{a+b}{b} \Longleftrightarrow \frac{a^2+b^2}{1+ab} < \frac{a}{b} + 1.$$

Posljednja nejednakost je zadovoljena jer je

$$\frac{a^2+b^2}{ab+1} < \frac{a^2+ab}{ab+1} < \frac{a^2+ab}{ab} = \frac{a}{b} + 1.$$

Stoga je $(b, kb-a)$ rješenje u prirodnim brojevima za koje vrijedi $kb-a < b$, što je u kontradikciji s minimalnošću od (a, b). Dakle, tvrdnja vrijedi.

2.3 Parametarska metoda

U mnogim slučajevima cjelobrojna rješenja diofantske jednadžbe

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

mogu se zapisati u parametarskom obliku:

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

gdje su $g_1, g_2, ..., g_n$ funkcije (polinomi) s cjelobrojnim koeficijentima s l varijabli $k_1, ..., k_l \in \mathbb{Z}$.

Skup rješenja nekih diofantskih jednadžbi može imati više parametarskih prikaza. Za većinu diofantskih jednadžbi, kojima nije moguće pronaći sva rješenja, parametarskom metodom dokazujemo postojanje beskonačno mnogo rješenja.

Primjer 2.18 *Odredimo sve uređene trojke (x, y, z) prirodnih brojeva tako da je*

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

Rješenje. Budući da su x, y, z prirodni brojevi, zadana jednadžba je ekvivalentna jednadžbi

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

Neka da je $d = gcd(x, y)$. Tada vrijedi $x = dm, y = dn$, gdje je $m, n \in \mathbb{N}$ i $gcd(m, n) = 1$. Stoga je $gcd(mn, m+n) = 1$ i $z = \frac{dmn}{m+n}$, što povlači $(m+n) \mid d$, tj. $d = k(m+n), k \in \mathbb{N}$.

Stoga su rješenja zadane jednadžbe dana s

$$x = km\,(m+n)\,, \quad y = kn\,(m+n)\,, \quad z = kmn, \quad k, m, n \in \mathbb{N}.$$

Napomena Ako su a, b, c relativno prosti prirodni brojevi takvi da je

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c},$$

onda je $a + b$ kvadrat. Zaista, tada je $k = 1$, $a = m(m+n)$, $b = n(m+n)$ pa je $a + b = (m+n)^2$.

Primjer 2.19 *Dokažimo da jednadžba*

$$2^x + 1 = xy$$

ima beskonačno mnogo rješenja u skupu prirodnih brojeva.

Rješenje. Dovoljno je dokazati da 3^k dijeli $2^{3^k} + 1$ za svaki $k \geq 0$. Ako je $k = 0$ ili 1 tvrdnja je očita. Za $k \geq 2$ imamo

$$2^{3^k} + 1 = \left(2^{3^{k-1}}\right)^3 + 1 = \left(2^{3^{k-1}} + 1\right)\left(2^{2 \cdot 3^{k-1}} - 2^{3^{k-1}} + 1\right).$$

Prvi faktor možemo zapisati kao $(3-1)^{3^{k-1}}+1$. Tada imamo

$$(3-1)^{3^{k-1}}+1 = 3^{3^{k-1}} - \binom{3^{k-1}}{1}\cdot 3^{3^{k-1}} + ... + \binom{3^{k-1}}{t}\cdot 3^{3^{k-1}-t} + ...$$

$$... + \binom{3^{k-1}}{3^{k-1}-1}\cdot 3\cdot(-1)^{3^{k-1}-1} + (-1)^{3^{k-1}} + 1.$$

Budući da vrijedi:

1) $3^{k-1}\Big|\binom{3^{k-1}}{t}$ za sve t, $1 \le t \le 3^{k-1}-1$,

2) $(-1)^{3^{k-1}}+1 = 0$, $k \ge 1$,

3) $3\Big|3^{3^{k-1}-t}$ za $1 \le t \le 3^{k-1}-1$, $k \ge 2$,

4) $3^k\Big|3^{3^{k-1}}$ za svaki $k \ge 2$ jer je $k \le 3^{k-1}$ za svaki $k \ge 1$,

slijedi da $3^k\Big|\left(2^{3^{k-1}}+1\right)$, što povlači da je $2^{3^k}+1$ djeljivo s 3^k. Stoga su $(x,y) = \left(3^k, \frac{2^{3^k}+1}{3^k}\right), k \ge 0$ rješenja jednadžbe. Uočimo da je drugi faktor od $2^{3^k}+1$ jednak $\left(2^{3^{k-1}}+1\right)^2 - 3\cdot 2^{3^{k-1}}$ pa je očito djeljiv s 3. Stoga je $2^{3^k}+1$ djeljivo i s 3^{k+1}.

2.3.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.20 *Dokažite da postoji beskonačno mnogo uređenih trojki $(x,y,z) \neq (0,0,0)$ cijelih brojeva takvih da je*

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

(Turnir gradova)

Rješenje. Neka je $z=-y$. Tada je

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

Uvođenjem supstitucije $y = mx, m \in \mathbb{Z}$ jednadžba poprima oblik $x^3 = x^2 + m^2x^2$, što je za $x \neq 0$ ekvivalentno s $x = 1 + 2m^2$. Dobivamo beskonačnu familiju rješenja (x, y, z), danu s $x = 2m^2 + 1$, $y = m(2m^2 + 1)$, $z = -m(2m^2 + 1)$, $m \in \mathbb{Z}$.

Zadatak 2.21 *Pokažite da jednadžba*

$$x^2 + y^2 = z^5 + z$$

ima beskonačno mnogo relativno prostih cjelobrojnih rješenja.

(Britanska matematička olimpijada)

Rješenje. Koristit ćemo Lagrangeov identitet

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

i dva dobro poznata rezultata:

1. Postoji beskonačno mnogo prostih brojeva oblika $4k + 1$.

2. Svaki prosti broj oblika $4k+1$ može se zapisati kao suma dva kvadrata.

Uzmimo bilo koji prosti broj p oblika $4k + 1$. Prema 2., taj broj može se prikazati kao suma dva kvadrata. Isto očito vrijedi i za $p^4 + 1 = (p^2)^2 + 1^2$, a Langrangeov identitet pokazuje da se $p^5 + p = p(p^4 + 1)$ također može prikazati kao suma dva kvadrata. Neka je $p^5 + p = u^2 + v^2$. Tada je $(x, y, z) = (u, v, p)$ rješenje zadane jednadžbe. Budući da je p prost, onda su x, y i z relativno prosti brojevi. Sada je dovoljno uočiti da (prema 1.) prostih brojeve oblika $4k + 1$ ima beskonačno mnogo. Dakle, zadana jednadžba ima beskonačno mnogo relativno prostih rješenja.

Zadatak 2.22 *Riješite u skupu cijelih brojeva jednadžbu*

$$x^2 + xy = y^2 + xz.$$

Rješenje. Početna jednadžba je ekvivalentna jednadžbi

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

Slijedi da je

$$x = mp^2, x + y - z = mq^2, y = \pm mpq.$$

Rješenja jednadžbe su $(x, y, z) = (mp^2, \pm mpq, m(p^2 \pm pq - q^2))$, $m, p, q \in \mathbb{Z}$.

Zadatak 2.23 *Dokažite da postoji beskonačno mnogo uređenih četvorki* (x, y, z, w) *prirodnih brojeva takvih da je*

$$x^4 + y^4 + z^4 = 2002^w.$$

(Titu Andreescu)

Rješenje. Primijetimo da je $2002 = 3^4+5^4+6^4$ pa je $2002^w = (3^4+5^4+6^4)^w$. Pretpostavimo da je $x_k = 3 \cdot 2002^k$, $y_k = 5 \cdot 2002^k$ i $z_k = 6 \cdot 2002^k, k \in \mathbb{N}$. Tada je

$$x_k^4 + y_k^4 + z_k^4 = 3^4 \cdot 2002^{4k} + 5^4 \cdot 2002^{4k} + 6^4 \cdot 2002^{4k} = 2002 \cdot 2002^{4k} = 2002^{4k+1}.$$

Ako definiramo $w_k = 4k + 1$, onda je

$$(x_k, y_k, z_k, w_k) = (3 \cdot 2002^k, 5 \cdot 2002^k, 6 \cdot 2002^k, 4k + 1), k \in \mathbb{N},$$

beskonačna familija rješenja dane jednadžbe u prirodnim brojevima.

2.4 Metoda modularne aritmetike

Osnovna svojstva kongruencija, odnosno jednostavna modularna aritmetika često se koristi za dokazivanje da određene diofantske jednadžbe nisu rješive ili za određivanje skupa u kojem se nalaze moguća rješenja.

2.4. Metoda modularne aritmetike

Teoriju kongruencije uveo je Carl Friedrich Gauss 1801. godine. Također je uveo i oznaku za kongruenciju koju i danas koristimo.

Definicija 2.1 *Neka su a, b i n cijeli brojevi i $n \neq 0$. Ako n dijeli razliku $a-b$, onda kažemo da je* ***a kongruentan b modulo n*** *i pišemo $a \equiv b \pmod{n}$. U protivnom, kažemo da a nije kongruentan b modulo n i pišemo $a \not\equiv b \pmod{n}$.*

Budući da je $a - b$ djeljivo s n ako i samo ako je djeljivo s $-n$, bez smanjenja općenitosti možemo promatrati samo pozitivne module n, tj. podrazumijevat ćemo da je modul prirodan broj.

Kongruencije imaju mnoga svojstva zajednička s jednakostima.

Neka su a, b, c cijeli brojevi i n prirodan broj. Tada vrijedi:

1. $a \equiv a \pmod{n}$ (refleksivnost).
2. Ako je $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$, onda je $a \equiv c \pmod{n}$ (tranzitivnost).
3. Ako je $a \equiv b \pmod{n}$, onda je $b \equiv a \pmod{n}$ (simetričnost).

Stoga je relacija *"biti kongruentan modulo n"* relacija ekvivalencije na skupu cijeli brojeva $\mathbb{Z}$.

Također vrijede još neka jednostavna svojstva kongruencija:

4. Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda je $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$, $ac \equiv bd \pmod{n}$.
5. Ako je $a \equiv b \pmod{n}$ i $d|n$, onda je $a \equiv b \pmod{d}$.
6. Ako je $a \equiv b \pmod{n}$, onda je $ac \equiv bc \pmod{nc}$ za svaki $c \neq 0$.

Svojstvo 4. pokazuje da se kongruencije (s istim modulom) mogu zbrajati, oduzimati i množiti na isti način kao što to možemo s jednakostima. Situacija s dijeljenjem je nešto kompleksnija i dana je u Teoremu 2.1. Iz svojstava 4.

direktno slijedi:

Propozicija 2.1 *Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{n}$, onda je $f(a) \equiv f(b) \pmod{n}$.*

Sljedeći teorem govori da se obje strane kongruencije ne smiju kratiti sa zajedničkim faktorom jer se nakon kraćenja u pravilu modul promijeni, ali ipak u jednom vrlo važnom slučaju modul ostaje nepromijenjen te je u tom slučaju dijeljenje (kraćenje) dopušteno.

Teorem 2.1 *Neka su $a, b, c \in \mathbb{Z}$. Tada je $ca \equiv cd \pmod{n}$ ako i samo ako*

$$a \equiv b \pmod{\frac{n}{\gcd(c,n)}}.$$

Specijalno, ako je $ca \equiv cb \pmod{n}$ i $\gcd(c,n) = 1$, onda je $a \equiv b \pmod{n}$.

Jedan od osnovnih i često korištenih rezultata u teoriji brojeva je i sljedeći teorem.

Teorem 2.2 (**Mali Fermatov teorem**) *Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.*

Primjer 2.24 *Dokažimo da jednadžba*

$$(x+1)^2 + (x+2)^2 + ... + (x+2001)^2 = y^2$$

nije rješiva u cijelim brojevima.

Rješenje. Supstitucijom $x = z - 1001$, dobivamo jednadžbu

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

odnosno

$$2001z^2 + 2\left(1^2 + 2^2 + ... + 1000^2\right) = y^2.$$

Korištenjem formule za sumu kvadrata prvih n prirodnih brojeva, dobivamo

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

što je ekvivalentno s

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

Lijeva strana gornje jednadžbe je kongruentna 2 modulo 3, pa ne može biti kvadrat nekog cijelog broja budući da su svi kvadrati kongruentni 0 ili 1 modulo 3. Zaključujemo, početna jednadžba nema rješenja.

Primjer 2.25 *Nađimo sve uređene parove (x, y) prirodnih brojeva tako da je*

$$x^2 - y! = 2001.$$

(Titu Andreescu)

Rješenje. Za y veći od 5, $y!$ je djeljivo s 9, pa je $x^2 = y! + 2001 \equiv 3 \pmod 9$. Budući da su svi kvadrati kongruentni $0, 1, 4$ ili 7 modulo 9, jednadžba nema rješenja za $y \geq 6$. Stoga su brojevi $1, 2, 3, 4$ i 5 jedini kandidati za y. Samo za $y = 4$ dobivamo da je $y! + 2001$ pravi kvadrat, što daje $x = 45$. Dakle, rješenje početne jednadžbe je $(x, y) = (45, 4)$.

2.4.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.26 *Dokažite da jednadžba $x^5 - y^2 = 4$ nema cjelobrojnih rješenja.*

(Balkanska matematička olimpijada)

Rješenje. Promatramo jednadžbu modulo 11. Primijetimo da ako $11|x$, onda je $x^{10} \equiv 0 \pmod{11}$. Ako vrijedi suprotno, tj. ako $11 \nmid x$, onda po Malom Fermatovom teoremu vrijedi $x^{10} \equiv 1 \pmod{11}$. Stoga je $(x^5)^2 = x^{10} \equiv 0$ ili 1 (mod 11) za svaki cijeli broj x, iz čega slijedi $x^5 \equiv -1, 0$, ili 1 (mod 11), odnosno $x^5 - 4 \equiv 6, 7$ ili 8 (mod 11). Međutim, svi kvadrati su kongruentni $0, 1, 3, 4, 5$ ili 9 modulo 11 pa jednadžba nema cjelobrojna rješenja.

Zadatak 2.27 *Odredite sve proste brojeve p za koje sustav jednadžbi*

$$\begin{cases} p+1 = 2x^2 \\ p^2+1 = 2y^2, \end{cases}$$

ima rješenja u cijelim brojevima x i y.

(Njemačka matematička olimpijada)

Rješenje. Jedini takav prost broj je 7. Naime, bez smanjenja općenitosti možemo pretpostaviti da su $x, y \geq 0$. Budući da je $p+1 = 2x^2$, onda je $p+1$ paran pa je $p \neq 2$. Također, iz gornjeg sustava dobivamo da je $2x^2 \equiv 1 \equiv 2y^2 \pmod{p}$. Budući da je p neparan broj, iz toga slijedi da je $x^2 \equiv y^2 \pmod{p}$, što povlači $x \equiv \pm y \pmod{p}$. Kako je očito $0 < x < y < p$, tada je $x + y = p$. Sada je

$$p^2 + 1 = 2\left(p - x\right)^2 = 2p^2 - 4px + p + 1,$$

što povlači: $p = 0$ ili $p = 4x - 1$. Dakle, budući da 0 nije prost broj, mora biti $p = 4x - 1$, što povlači $2x^2 = 4x$, tj. $x = 0$ ili $x = 2$.
Za $x = 0$ dobivamo $p = -1$, što nije prost broj.
Ako je $x = 2$, onda je $p = 7$ i $y = 5$. Dakle, $p = 7$ je jedini prost broj za koji sustav ima rješenje u cijelim brojevima.

Zadatak 2.28 *Dokažite da postoje jedinstveni prirodni brojevi a i n takvi da je*

$$a^{n+1} - (a+1)^n = 2001.$$

(Putnam matematičko natjecanje)

Rješenje. Pretpostavimo da je $a^{n+1} - (a+1)^n = 2001$. Primijetimo da je $a^{n+1} + ((a+1)^n - 1)$ višekratnik od a, stoga a dijeli $2002 = 2 \cdot 7 \cdot 11 \cdot 13$.

Budući da je 2001 djeljiv s 3, tada je $a \equiv 1 \pmod 3$, inače je točno jedan od brojeva a^{n+1} i $(a+1)^n$ višekratnik broja 3 pa njihova razlika nije djeljiva s 3. Sada je $a^{n+1} \equiv 1 \pmod 3$ pa je $(a+1)^n \equiv 1 \pmod 3$, što znači da je n paran.

Ako je a paran, tada je

$$a^{n+1} - (a+1)^n \equiv -(a+1)^n \pmod 4.$$

Budući da je n paran, imamo

$$-(a+1)^n \equiv -1 \pmod 4,$$

što je nemoguće budući da je $2001 \equiv 1 \pmod 4$. Stoga je a neparan i mora dijeliti $1001 = 7 \cdot 11 \cdot 13$. Budući da je a neparan i n paran, slijedi da je $a^{n+1} \equiv a^n \cdot a \equiv 1 \cdot a \equiv a \pmod 4$ i $(a+1)^n \equiv 0 \pmod 4$ pa je

$$a^{n+1} - (a+1)^n \equiv a \pmod 4$$

pa je $a \equiv 1 \pmod 4$. Djelitelji od $7 \cdot 11 \cdot 13$ koji su kongruentni 1 modulo 3 nisu djeljivi s 11 (budući da su 7 i 13 kongruentni 1 modulo 3). Stoga $a|(7 \cdot 13)$. Sada je $a \equiv 1 \pmod 4$ moguće samo ako $a|13$.

Budući da je $1 - 2^n \neq 2001$ za sve n, onda je $a \neq 1$. Stoga je jedino moguće da je $a = 13$. Lako se provjeri da je $a = 13$, $n = 2$ rješenje.

Preostaje provjeriti da jednadžba nema rješenja za ostale n. Ako je $n > 2$, tada je

$$13^{n+1} \equiv 2001 \equiv 1 \pmod 8.$$

Međutim, budući da je n paran, onda je $13^{n+1} \equiv 5 \pmod 8$, što je kontradikcija. Stoga je $a = 13$, $n = 2$ jedino rješenje.

Zadatak 2.29 *Odredite, ako postoje, sva nenegativna cjelobrojna rješenja*

$(x_1, x_2, ..., x_{14})$, *do na permutaciju, diofantske jednadžbe*

$$x_1^4 + x_2^4 + ... + x_{14}^4 = 15999. \tag{2.4}$$

(Američka matematička olimpijada)

Rješenje. Pokazat ćemo da kongruencija

$$x_1^4 + x_2^4 + ... + x_{14}^4 \equiv 15999 \pmod{16}$$

nema rješenje, što povlači da ni jednadžba (2.4) nema rješenje.
Ako je cijeli broj n paran, tada je $n = 2k$ za neki $k \in \mathbb{Z}$ pa je $n^4 = 16k^4 \equiv 0 \pmod{16}$.
Ako je n neparan, tada je

$$n^4 - 1 = (n-1)(n+1)(n^2+1) \equiv 0 \pmod{16},$$

budući da su $n-1$, $n+1$ i n^2+1 parni brojevi i jedan od brojeva $n-1$, $n+1$ je djeljiv s 4. To znači da je $n^4 \equiv 0 \pmod{16}$ za paran n i $n^4 \equiv 1 \pmod{16}$ za neparan n. Stoga, ako je točno r brojeva od $x_1, x_2, ..., x_{14}$ neparno, tada je

$$x_1^4 + x_2^4 + ... + x_{14}^4 \equiv r \pmod{16}.$$

Kako je $15999 = 16000 - 1 \equiv 15 \pmod{16}$ i budući da je $0 \leq r \leq 14$, kongruencija

$$x_1^4 + x_2^4 + ... + x_{14}^4 \equiv 15 \pmod{16}$$

nema rješenje. Stoga ni jednadžba (2.4) nema rješenje.

2.5 Metoda matematičke indukcije

Matematička indukcija jedna je od temeljnih metoda koja se koristi za dokazivanje tvrdnji koje ovise o prirodnim brojevima ili nenegativnim cijelim

brojevima. Metoda se temelji na tzv. principu matematičke indukcije.

Princip matematičke indukcije: *Neka je $P(n)$ neka tvrdnja koja ovisi o prirodnom broju n. Ako su ispunjena sljedeća dva uvjeta:*

1. *(Baza indukcije): $P(1)$ je istinita.*
2. *(Korak indukcije): Za svaki prirodan broj k vrijedi: Ako je $P(k)$ istinita, onda je $P(k+1)$ istinita.*

Tada je $P(n)$ istinita za svaki prirodan broj n.

Postoji nekoliko verzija principa matematičke indukcije u kojima se uz nešto izmijenjenu bazu i/ili korak indukcije, dobiva identičan ili sličan zaključak kao u osnovnoj verziji.

Matematička indukcija (slaba forma): *Neka je $n_0 \geq 0$ cijeli broj. Pretpostavimo:*

1. *$P(n_0)$ je istinita tvrdnja;*
2. *Za svaki nenegativan cijeli broj $k \geq n_0$ vrijedi: ako je $P(k)$ istinita, onda je $P(k+1)$ istinita.*

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

Matematička indukcija (s korakom s): *Neka je $n_0 \geq 0$ cijeli broj i neka je s fiksan prirodan broj. Pretpostavimo:*

1. *$P(n_0), P(n_0+1), ..., P(n_0+s-1)$ su istinite tvrdnje;*
2. *Za svaki $k \geq n_0$ vrijedi: ako je $P(k)$ istinita tvrdnja, onda je i $P(k+s)$ istinita.*

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

Matematička indukcija (jaka forma): *Neka je $n_0 \geq 0$ cijeli broj. Pretpostavimo:*

1. *$P(n_0)$ je istinita tvrdnja;*
2. *Za svaki nenegativan cijeli broj $k \geq n_0$ vrijedi: ako je $P(m)$ istinita tvrdnja za svaki m za koji vrijedi $n_0 \leq m \leq k$, onda je i $P(k+1)$ istinita.*

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

Sljedećim primjerima demonstrirat ćemo primjenu matematičke indukcije kod rješavanja diofantskih jednadžbi.

Primjer 2.30 *Dokažimo da je za sve prirodne brojeve n, jednadžba*

$$x^2 + xy + y^2 = 7^n$$

rješiva u skupu cijelih brojeva.

(Dorin Andrica)

Rješenje. Pokazat ćemo matematičkom indukcijom da postoje (cijeli) brojevi x_n i y_n takvi da je $x_n^2 + x_n y_n + y_n^2 = 7^n$ za svaki prirodan broj n. Ako je $n = 1$, onda jednadžba $x^2 + xy + y^2 = 7$, ima rješenje $(x, y) = (2, 1)$ pa je $x_1 = 2$ i $y_1 = 1$.
Pretpostavimo da postoje cijeli brojevi x_n, y_n koji zadovoljavaju jednadžbu $x^2 + xy + y^2 = 7^n$, tj. pretpostavimo da vrijedi

$$x_n^2 + x_n y_n + y_n^2 = 7^n.$$

Definirajmo $x_{n+1} = 2x_n - y_n, y_{n+1} = x_n + 3y_n$. Tada je

$$x_{n+1}^2 + x_{n+1} y_{n+1} + y_{n+1}^2$$

$$= (2x_n - y_n)^2 + (2x_n - y_n)(x_n + 3y_n) + (x_n + 3y_n)^2$$
$$= 4x_n^2 - 4x_n y_n + y_n^2 + 2x_n^2 + 6x_n y_n - x_n y_n - 3y_n^3 + x_n^2 + 6x_n y_n + 9y_n^2$$
$$= 7\left(x_n^2 + x_n y_n + y_n^2\right) = 7 \cdot 7^n = 7^{n+1}.$$

Dakle, za sve prirodne brojeve n, zadana jednadžba je rješiva u skupu cijelih brojeva.

Primjer 2.31 *Dokažimo da je za sve prirodne brojeve n, jednadžba*

$$x^2 + y^2 + z^2 = 59^n$$

rješiva u skupu prirodnih brojeva.

(Dorin Andrica)

Rješenje. Pokažimo da postoje prirodni brojevi x_n, y_n, z_n takvi da je $x_n^2 + y_n^2 + z_n^2 = 59^n$. Koristimo matematičku indukciju s korakom $s = 2$ i $n_0 = 1$. Rješenja jednadžbi

$$x_1^2 + y_1^2 + z_1^2 = 59 \qquad i \qquad x_2^2 + y_2^2 + z_2^2 = 59^2$$

su $(x_1, y_1, z_1) = (1, 3, 7)$ i $(x_2, y_2, z_2) = (14, 39, 42)$, pa tvrdnja vrijedi za $n = 1$ i $n = 2$.

Pretpostavimo da postoje prirodni brojevi x_k, y_k, z_k takvi da je $x_k^2 + y_k^2 + z_k^2 = 59^k$ za neki $k \geq 1$.

Definirajmo

$$x_{k+2} = 59x_k, \qquad y_{k+2} = 59y_k, \qquad z_{k+2} = 59z_k.$$

Tada je

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^2\left(x_k^2 + y_k^2 + z_k^2\right) = 59^2 \cdot 59^k = 59^{k+2}.$$

Stoga je zadana jednadžba rješiva u skupu prirodnih brojeva za svaki $n \in \mathbb{N}$.

2.5.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.32 *Dokažite da za sve cijele brojeve $n \geq 3$, postoje neparni prirodni brojevi x i y, tako da je*

$$7x^2 + y^2 = 2^n.$$

(Bugarska matematička olimpijada)

Rješenje. Dokazat ćemo da postoje neparni prirodni brojevi x_n, y_n takvi da $7x_n^2 + y_n^2 = 2^n, n \geq 3$.
Za $n = 3$, imamo jednadžbu oblika

$$7x_3^2 + y_3^2 = 8.$$

čije rješenje je $(x_3, y_3) = (1, 1)$.
Pretpostavimo da za neki cijeli broj $n \geq 3$ postoje neparni cijeli brojevi x_n, y_n koji zadovoljavaju jednadžbu $7x_n^2 + y_n^2 = 2^n$. Pokazat ćemo da postoji par neparnih prirodnih brojeva (x_{n+1}, y_{n+1}) takvih da je $7x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$. Imamo,

$$7\left(\frac{x_n \pm y_n}{2}\right)^2 + \left(\frac{7x_n \mp y_n}{2}\right)^2 = 2\left(7x_n^2 + y_n^2\right) = 2^{n+1},$$

jer je

$$7\left(\frac{x_n + y_n}{2}\right)^2 + \left(\frac{7x_n - y_n}{2}\right)^2 = \frac{56x_n^2 + 8y_n^2}{4} = 14x_n^2 + 2y_n^2.$$

Slično računamo i za drugi slučaj i dobivamo isti rezultat.
Točno jedan od brojeva $\frac{x_n+y_n}{2}$ i $\frac{|x_n-y_n|}{2}$ je neparan jer je njihova suma jednaka $max\left\{x_n, y_n\right\}$, što je neparan broj. Ako je, npr. $\frac{x_n+y_n}{2}$ neparan, tada je

$$\frac{7x_n - y_n}{2} = 3x_n + \frac{x_n - y_n}{2}$$

također neparan jer je suma parnog i neparnog broja. Stoga u ovom slučaju možemo odabrati

$$x_{n+1} = \frac{x_n + y_n}{2} \qquad i \qquad y_{n+1} = \frac{7x_n - y_n}{2}.$$

Ako je $\frac{x_n - y_n}{2}$ neparan, tada je

$$\frac{7x_n + y_n}{2} = 3x_n + \frac{x_n + y_n}{2},$$

neparan pa odaberemo

$$x_{n+1} = \frac{|x_n - y_n|}{2} \qquad i \qquad y_{n+1} = \frac{7x_n + y_n}{2}.$$

Dakle, za svaki cijeli broj $n \geq 3$, jednadžba $7x^2 + y^2 = 2^n$ ima rješenja u skupu neparnih prirodnih brojeva.

Zadatak 2.33 *Dokažite da je jednadžba*

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = \frac{n+1}{x_{n+1}^2} \tag{2.5}$$

rješiva u skupu prirodnih brojeva ako i samo ako je $n \geq 3$.

(Mathematical Reflections)

Rješenje. Za $n = 1$, imamo jednadžbu oblika

$$\frac{1}{x_1^2} = \frac{2}{x_2^2},$$

odnosno $\sqrt{2}x_1 = x_2$, koja nema rješenje budući da je $\sqrt{2}$ iracionalan broj. Za $n = 2$, imamo jednadžbu oblika

$$(x_2x_3)^2 + (x_1x_3)^2 = 3(x_1x_2)^2.$$

Za $1 \leq i \leq 3$, neka je $x_i = 3^{n_i}y_i$, gdje y_i nije djeljiv s 3. Bez smanjenja općenitosti možemo pretpostaviti da je $n_1 \geq n_2$. Tada je

$$3^{2(n_2+n_3)}((y_2y_3)^2 + 3^{2(n_1-n_2)}(y_1y_3)^2) = 3^{2(n_1+n_2)+1}(y_1y_2)^2. \tag{2.6}$$

Budući da je 1 jedini mogući kvadratni ostatak modulo 3, tada je

$$(y_1y_2)^2 \equiv 1 \pmod 3,$$

$$(y_2y_3)^2 + 3^{2(n_1-n_2)}(y_1y_3)^2 \equiv 1 \text{ ili } 2 \pmod 3$$

pa eksponenti od 3 na obje strane jednakosti moraju biti jednaki, što je nemoguće jer je jedan paran, a drugi neparan. Stoga početna jednadžba nema rješenja za $n = 2$.

Konačno, pokažimo da je jednadžba (2.5) rješiva ako je $n \geq 3$.

Neka je $n = 3$. Dijeljenjem $4^2 + 3^2 = 5^2$, s $3^2 4^2 5^2$ dobivamo

$$\frac{1}{15^2} + \frac{1}{20^2} = \frac{1}{12^2}.$$

Množenjem s $\frac{1}{12^2}$, dobivamo

$$\frac{1}{12^2 \cdot 15^2} + \frac{1}{12^2 \cdot 20^2} = \frac{1}{12^4}.$$

Jednakost možemo zapisati u obliku

$$\frac{1}{12^2 \cdot 15^2} + \left(\frac{1}{15^2} + \frac{1}{20^2}\right)\frac{1}{20^2} = \frac{4}{4 \cdot 12^4},$$

odnosno kao

$$\frac{1}{(12 \cdot 15)^2} + \frac{1}{(15 \cdot 20)^2} + \frac{1}{(20 \cdot 20)^2} = \frac{4}{(2 \cdot 12^2)^2}.$$

Stoga je

$$(x_1, x_2, x_3, x_4) = (12 \cdot 15, 15 \cdot 20, 20 \cdot 20, 2 \cdot 12^2)$$

rješenje jednadžbe (2.5) za $n = 3$.

Pretpostavimo da je $(x_1^{(0)}, ..., x_{n+1}^{(0)})$ rješenje od

$$\frac{1}{x_1^2} + \cdots + \frac{1}{x_n^2} = \frac{n+1}{x_{n+1}^2}$$

za neki $n \geq 3$. Tada je

$$\frac{1}{(x_1^{(0)})^2} + \cdots + \frac{1}{(x_n^{(0)})^2} + \frac{1}{(x_{n+1}^{(0)})^2} = \frac{n+1}{(x_{n+1}^{(0)})^2} + \frac{1}{(x_{n+1}^{(0)})^2} = \frac{n+2}{(x_{n+1}^{(0)})^2}$$

pa je $(x_1^{(0)}, ..., x_{n+1}^{(0)}, x_{n+1}^{(0)})$ rješenje od $\frac{1}{x_1^2} + \cdots + \frac{1}{x_{n+1}^2} = \frac{n+2}{x_{n+2}^2}$.

2.6 Fermatova metoda beskonačnog spusta

Fermatova otkrića i metode imali su velik utjecaj na razvoj matematike. Bio je jedan od prvih matematičara koji je koristio metodu dokazivanja zvanu "beskonačni spust".
Neka je P svojstvo koje se odnosi na nenegativne cijele brojeve i neka je $(P(n))_{n\geq 1}$, niz tvrdnji:

$$P(n)\text{: "}n \text{ zadovoljava svojstvo } P\text{."}$$

Sljedeća metoda je korisna za dokazivanje da je tvrdnja $P(n)$ neistinita za dovoljno velik n.
Neka je k nenegativan cijeli broj. Pretpostavimo:

1. *Tvrdnja $P(k)$ nije istinita*;

2. *Za svaki $m > k$ vrijedi: ako je $P(m)$ istinita tvrdnja, onda postoji j, $m > j \geq k$ za koji je tvrdnja $P(j)$ istinita.*

Tada $P(n)$ nije istinita tvrdnja za svaki $n \geq k$.

Ovo je upravo kontrapozicija jake indukcije primijenjena na negaciju tvrdnje $P(n)$. Ova metoda se naziva *metoda konačnog spusta.*

Fermatova metoda beskonačnog spusta je formulirana na sljedeći način:
Neka je k nenegativan cijeli broj. Pretpostavimo da vrijedi:

- *ako je tvrdnja $P(m)$ istinita za neki prirodan broj $m > k$, onda postoji manji prirodan broj j, $m > j > k$ takav da je $P(j)$ istinita tvrdnja.*

Tada tvrdnja $P(n)$ nije istinita za sve $n > k$.
Ovo znači da ako iz pretpostavke da postoji prirodan broj n za koji je tvrdnja $P(n)$ istinita, slijedi da je tvrdnja istinita i za neki strogo manji prirodan broj, onda možemo konstruirati strogo padajući niz prirodnih brojeva

$n > n_1 > n_2 > ...$ koji su svi veći od k, što je nemoguće jer takav niz ne postoji. Stoga ne postoji prirodan broj n, $n > k$ sa svojstvom $P(n)$.

Razlikujemo dva posebna slučaja Fermatove metode koja su korisna u proučavanju diofantskih jednadžbi:

T1. Ne postoji niz nenegativnih cijelih brojeva $(n_i)_{i\geq 1}$ takav da je $n_1 > n_2 > n_3 > \cdots$.

T2. Ako za niz nenegativnih cijelih brojeva $(n_i)_{i\geq 1}$ vrijedi $n_1 \geq n_2 \geq n_3 \geq \cdots$, onda postoji i_0 tako da je $n_{i_0} = n_{i_o+1} = \cdots$.

Primjer 2.34 *Riješimo u nenegativnim cijelim brojevima jednadžbu*

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

Rješenje. Možemo primijetiti da je $(x, y, z) = (0, 0, 0)$ trivijalno rješenje zadane jednadžbe i dokažimo da je jedino. Pretpostavimo da postoji netrivijalno rješenje (x_1, y_1, z_1). Budući da su $\sqrt[3]{2}$ i $\sqrt[3]{4}$ iracionalni brojevi, zaključujemo da $x_1 > 0, y_1 > 0$ i $z_1 > 0$.
Iz $x_1^3+2y_1^3 = 4z_1^3$ slijedi da $2|x_1$, pa je $x_1 = 2x_2, x_2 \in \mathbb{N}$. Tada je $4x_2^3+y_1^3 = 2z_1^3$ pa slijedi $y_1 = 2y_2, y_2 \in \mathbb{N}$. Na sličan način dobijemo $z_1 = 2z_2, z_2 \in \mathbb{N}$. Na taj način smo dobili novo rješenje (x_2, y_2, z_2), gdje je $x_1 > x_2, y_1 > y_2, z_1 > z_2$. Nastavimo ovaj postupak i dobijemo niz rješenja u prirodnim brojevima $(x_n, y_n, z_n)_{n\geq 1}$, tako da je $x_1 > x_2 > x_3 > \cdots$. No, ovo je u kontradikciji s T1. Prema tome, jedino rješenje je $(x, y, z) = (0, 0, 0)$.

Primjer 2.35 *(a) Dokažimo da ako postoji uređena trojka (x, y, z) prirodnih brojeva tako da je*

$$x^2 + y^2 + 1 = xyz,$$

tada je z=3.

(b) Pronađimo sve takve trojke.

Rješenje. (a) Neka je (x, y, z) rješenje u prirodnim brojevima i $z \neq 3$. Tada je $x \neq y$ jer je inače $x^2(z-2) = 1$, što je nemoguće budući da je $z - 2 \neq 1$. Imamo

$$0 = x^2 + y^2 + 1 - xyz = (x - yz)^2 + y^2 + 1 + xyz - y^2z^2$$

$$= (yz - x)^2 + y^2 + 1 - (yz - x)yz,$$

stoga je $(yz - x, y, z)$ također rješenje u prirodnim brojevima, budući da $x(yz - x) = xyz - x^2 = y^2 + 1 > 0$ povlači $yz - x > 0$. Primijetimo da ako je $x > y$, onda je $x^2 > y^2+1 = x(yz-x)$. Stoga je $x > yz-x$, što pokazuje da je novo rješenje "manje" od početnog, u smislu da je $x+y+z > (yz-x)+y+z$. Stoga, uz uvjet da je $x \neq y$, ovaj postupak se može nastaviti u beskonačnost, što je nemoguće budući da u procesu konstruiramo beskonačan padajući niz prirodnih brojeva, što je u kontradikciji s T1. Iz toga slijedi da ne postoje rješenja ako je $z \neq 3$.

(b) Očito je $(x, y) = (1, 1)$ rješenje jednadžbe

$$x^2 + y^2 + 1 = 3xy.$$

Neka je $(x, y) = (a, b)$, $a > b$ neko drugo rješenje. Tada je $b^2 + (3b - a)^2 + 1 = 3b(3b - a)$ pa je $(x, y) = (b, 3b - a)$ također rješenje. Iz

$$(a - b)(a - 2b) = a^2 - 3ab + 2b^2 = b^2 - 1 > 0$$

slijedi da je $a > 2b$ pa je $3b - a < b$. Stoga novo rješenje ima manji y. Nastavljajući postupak dolazimo do rješenja s $y = 1$ pa je $x^2 + 2 = 3x$ što povlači $x = 1$ ili $x = 2$. Slijedi da se sva rješenja mogu dobiti iz $(a_1, b_1) = (1, 1)$ pomoću rekurzivnih relacija

$$(a_{n+1}, b_{n+1}) = (b_n, 3b_n - a_n).$$

Nizovi $(a_n)_{n\geq 1}$ i $(b_n)_{n\geq 1}$ zadovoljavaju istu rekurziju $x_{n+1} = 3x_n - x_{n-1}$, $x_1 = 1$, $x_2 = 2$, što karakterizira Fibonaccijeve brojeve neparnog indeksa. Stoga je $(a_n, b_n) = (F_{2n+1}, F_{2n-1})$, $n \geq 1$.
Slijedi da su sva rješenja u prirodnim brojevima dana sa $(x, y) = (1, 1)$, (F_{2n+1}, F_{2n-1}), (F_{2n-1}, F_{2n+1}), $n \geq 1$.

2.6.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.36 *Riješite u nenegativnim cijelim brojevima jednadžbu*

$$2^x - 1 = xy.$$

(Putnam matematičko natjecanje)

Rješenje. Uočimo da su rješenja $(x, y) = (0, k), k \in \mathbb{N}_0$ i $(x, y) = (1, 1)$. Primjenom Fermatove metode beskonačnog spusta na proste faktore broja x, dokažimo da ne postoje druga rješenja.
Ako je (x, y) rješenje u prirodnim brojevima, onda je očito x neparan. Stoga, neka je (x, y) rješenje, gdje je $x > 1$, neka je $p_1 > 2$ prost djelitelj od x i neka je q najmanji prirodan broj za kojeg vrijedi $p_1|(2^q - 1)$. Prema malom Fermatovom teoremu imamo $p_1|(2^{p_1-1} - 1)$, stoga vrijedi $q \leq p_1 - 1 < p_1$. Uočimo da $p_1|(2^q - 1)$ povlači $q \geq 2$.
Dokažimo da $q|x$. Pretpostavimo suprotno, $q \nmid x$. Tada postoje cijeli brojevi k i r, takvi da je $x = kq + r$, gdje je $0 < r < q$. Tada je

$$2^x - 1 = 2^{kq}2^r - 1 = (2^q)^k \cdot 2^r - 1 = (2^q - 1 + 1)^k \cdot 2^r - 1 \equiv 2^r - 1 \pmod{p_1}.$$

Slijedi da $p_1|(2^r - 1)$, što je u kontradikciji s minimalnošću od q. Stoga $q|x$ i $1 < q < p_1$.
Neka je sada p_2 prosti djelitelj od q. Očito, p_2 je djelitelj od x i $2 < p_2 < p_1$.

Nastavimo postupak i dobijemo beskonačan niz padajući prostih djelitelja broja x: $p_1 > p_2 > \cdots$, što je u kontradikciji s T1.

Zadatak 2.37 *Neka je a prirodan broj. Dokažite da je (x, y) rješenje jednadžbe*

$$\left|x^2 + axy - y^2\right| = 1$$

u prirodnim brojevima ako i samo ako postoji prirodan broj k takav da je $(x, y) = (x_k, x_{k+1})$, gdje je niz $(x_n)_{n\geq 1}$ definiran s $x_1 = 1$, $x_2 = a$ i $x_{n+2} = ax_{n+1} + x_n$ za svaki $n \geq 1$.

(Rumunjska matematička olimpijada)

Rješenje. Neka je $f(x, y) = x^2 + axy - y^2$. Imamo $f(x_1, x_2) = f(1, a) = 1$. Primjenom matematičke indukcije, lako se vidi da je za svaki $n \geq 1$, (x_n, x_{n+1}) rješenje jednadžbe.

Neka je $(x, y) \in \mathbb{N} \times \mathbb{N}$ rješenje jednadžbe. Iz $x^2 + axy - y^2 = \pm 1$ slijedi da je $y(y - ax) = x^2 \pm 1 \geq 0$, s tim da je $x^2 \pm 1 = 0$ ako i samo ako je $x = 1$ i $y = a$. U tom slučaju je $(x, y) = (x_1, x_2)$

Sada pretpostavimo da je $y > ax$. Uređeni par $(x^{(1)}, y^{(1)}) = (y - ax, x)$ je također rješenje, budući da $f(x, y) = \pm 1$ povlači $f(y - ax, x) = \mp 1$. Također, $x + y \geq x^{(1)} + y^{(1)}$ i $y^{(1)} \geq ax^{(1)}$. Naime, budući da iz $(y - ax)^2 + ax\,(y - ax) - x^2 = \mp 1$ slijedi $x\,(x - a(y - ax)) = (y - ax)^2 \pm 1$, onda je $x \geq a(y - ax)$, odnosno $y^{(1)} \geq ax^{(1)}$. Na taj način dobivamo niz rješenja $(x^{(n)}, y^{(n)})_{n\geq 1}$ takav da je $y^{(n)} - ax^{(n)} \geq 0$ i

$$x + y \geq x^{(1)} + y^{(1)} \geq x^{(2)} + y^{(2)} \geq \cdots .$$

Primjenom T2., slijedi da postoji prirodan broj k takav da je $x^{(n)} + y^{(n)} = x^{(k)} + y^{(k)}$ za sve $n \geq k$. U ovom slučaju za rješenje $(x^{(k)}, y^{(k)})$ imamo $y^{(k)} = ax^{(k)}$ i $(x, y) = (x_k, x_{k+1})$.

2.7 Razne diofantske jednadžbe

Mnoge elementarne diofantske jednadžbe ne mogu se riješiti metodama opisanim u prethodnim poglavljima. U nastavku ćemo prikazati nekoliko primjera takvih jednadžbi.

Primjer 2.38 *Riješimo u prirodnim brojevima sustav jednadžbi*

$$\begin{cases} x^2 + 3y = u^2, \\ y^2 + 3x = v^2. \end{cases}$$

(Titu Andreescu)

Rješenje. Nejednakosti

$$x^2 + 3y \geq (x+2)^2, \qquad y^2 + 3x \geq (y+2)^2$$

ne mogu obje istovremeno biti istinite jer njihovim zbrajanjem dobivamo $x + y \leq -8$, što je nemoguće jer su x i y prirodni brojevi. Dakle, barem jedna od nejednakosti $x^2 + 3y < (x+2)^2$ i $y^2 + 3x < (y+2)^2$ je istinita.
Bez smanjenja općenitosti, pretpostavimo da je $x^2 + 3y < (x+2)^2$. Tada

$$x^2 < x^2 + 3y < (x+2)^2$$

povlači

$$x^2 + 3y = (x+1)^2,$$

odnosno

$$3y = 2x + 1.$$

Iz Teorema 1.1 dobivamo $x = 3k + 1$, $y = 2k + 1$ za neki nenegativan cijeli broj k i $y^2 + 3x = 4k^2 + 13k + 4$. Za $k > 5$ vrijedi

$$(2k+3)^2 < 4k^2 + 13k + 4 < (2k+4)^2,$$

pa y^2+3x ne može biti kvadrat. Stoga promatramo samo $k \in \{0,1,2,3,4,5\}$. Samo za $k = 0$ i $k = 5$ dobivamo da je $y^2 + 3x$ kvadrat. Za $k = 0$ dobivamo rješenje $(x, y, u, v) = (1, 1, 2, 2)$, a za $k = 5$ rješenje $(x, y, u, v) = (16, 11, 17, 13)$. Zbog simetričnosti imamo i rješenje $(x, y, u, v) = (11, 16, 13, 17)$.

Primjer 2.39 *Riješimo jednadžbu*

$$1 + x_1 + 2x_1x_2 + \cdots + (n-1)x_1x_2 \cdots x_{n-1} = x_1x_2 \cdots x_n$$

u međusobno različitim prirodnim brojevima $x_1, x_2, ..., x_n$.

(Titu Andreescu)

Rješenje. Jednadžbu možemo zapisati u obliku

$$x_1(x_2 \cdots x_n - (n-1)x_2 \cdots x_{n-1} - \cdots - 2x_2 - 1) = 1$$

pa dobivamo $x_1 = 1$ i

$$x_2(x_3 \cdots x_n - (n-1)x_3 \cdots x_{n-1} - \cdots - 3x_3 - 2) = 2.$$

Budući da je $x_2 \neq x_1$, slijedi da je $x_2 = 2$ i

$$x_3(x_4 \cdots x_n - (n-1)x_4 \cdots x_{n-1} - \cdots - 4x_4 - 3) = 3.$$

Budući da je $x_3 \neq x_2$ i $x_3 \neq x_1$, onda je $x_3 = 3$. Nastavljajući ovaj postupak, dobivamo: $x_1 = 1, x_2 = 2, ..., x_{n-1} = n-1$. Konačno, u zadnjem koraku imamo da je

$$(n-1)(x_n - (n-1)) = n-1$$

pa je $x_n = n$. Dakle, jednadžba ima jedinstveno rješenje $(x_1, x_2, ..., x_n) = (1, 2, ..., n)$ u međusobno različitim prirodnim brojevima.

2.7.1 Zadaci i problemi s matematičkih natjecanja

Zadatak 2.40 *Dokažite da jednadžba*

$$6\left(6a^2+3b^2+c^2\right)=5n^2$$

nema cjelobrojnih rješenja osim $a=b=c=n=0$.

(Azijsko-pacifička matematička olimpijada)

Rješenje. Pretpostavimo da postoji netrivijalno cjelobrojno rješenje (a,b,c,n). Možemo pretpostaviti da $gcd(a,b,c,n)=1$. Imamo

$$6a^2+3b^2+c^2=\frac{5n^2}{6},$$

pa očito $6|n$. Ako je $n=6m$, onda je

$$2a^2+b^2+\frac{c^2}{3}=10m^2,$$

i stoga $3|c$. Ako je $c=3d$, onda je

$$2a^2+b^2+3d^2=10m^2.$$

Za bilo koji cijeli broj x, imamo $x^2\equiv 0,1,4 \pmod 8$. Stoga je

$$2a^2\equiv 0,2 \pmod 8,$$
$$b^2\equiv 0,1,4 \pmod 8,$$
$$3d^2\equiv 0,3,4 \pmod 8.$$

S druge strane vrijedi

$$2a^2+b^2+3d^2=10m^2\equiv 0,2 \pmod 8$$

što povlači $b^2\equiv 3d^2\equiv 0,4 \pmod 8$. Stoga su b i d parni brojevi. Slijedi da je c također paran. Neka je $b=2r$ i $c=2s$. Tada zadanu jednadžbu možemo zapisati kao

$$36a^2+72r^2+24s^2=180m^2,$$

pa je $36a^2$ je očito djeljiv s 8. Stoga je a paran broj, kao i b, c i n, što je u kontradikciji s pretpostavkom da su brojevi a, b, c i n relativno prosti.

Zadatak 2.41 *Dokažite da za svaki prost broj p jednadžba*

$$2^p + 3^p = q^n$$

nema cjelobrojna rješenja (q, n), gdje su $q, n > 1$.

(Talijanska matematička olimpijada)

Rješenje. Ako je $p = 2$, onda je $q^n = 13$, što je nemoguće. Ako je p neparan, tada $5|(2^p + 3^p)$. Budući da je $n > 1$, tada vrijedi da $25|(2^p + 3^p)$. Stoga, kako je $p \geq 3$ i p neparan, imamo

$$2^p + (5-2)^p = 2^p + \left(5^p + \binom{p}{1}5^{p-1}(-2) + \cdots + \binom{p}{p-1}5(-2)^{p-1} + (-2)^p\right)$$

$$\equiv 2^p + \binom{p}{p-1}5(-2)^{p-1} + (-1)^p 2^p = 5p2^{p-1} \pmod{25},$$

pa je $5p2^{p-1} \equiv 0 \pmod{25}$, što povlači $5|p$. Dakle, $p = 5$, ali jednadžba $q^n = 2^5 + 3^5 = 5^2 \cdot 11$ nema rješenja.

Zadatak 2.42 *Nađite sva rješenja (x, y, z, t) u prirodnim brojevima jednadžbe*

$$(x + y)(y + z)(z + x) = txyz$$

takva da je $gcd(x, y) = gcd(y, z) = gcd(z, x) = 1$.

(Rumunjska matematička olimpijada)

Rješenje. Očito vrijedi da je $gcd(x, x + y) = gcd(x, x + z) = 1$ pa x dijeli $y + z$. Analogno zaključujemo da y dijeli $z + x$ i z dijeli $x + y$.

Neka su a, b i c cijeli brojevi takvi da je

$$\begin{cases} x + y = cz, \\ y + z = ax, \\ z + x = by. \end{cases}$$

Budući da su x, y, z prirodni brojevi, očito su i a, b, c također prirodni brojevi.

Ako gornje jednadžbe promatramo kao homogeni sustav od tri linearne jednadžbe s tri nepoznanice x, y, z , onda on ima netrivijalno rješenje ako i samo ako je $\triangle = abc - 2 - a - b - c = 0$, gdje je $\triangle$ determinanta matrice

$$\begin{pmatrix} 1 & 1 & -c \\ 1 & -b & 1 \\ -a & 1 & 1 \end{pmatrix}.$$

Diofantska jednadžba $abc-2 = a+b+c$ se može riješiti u prirodnim brojevima promatrajući tri slučaja.

Prvi slučaj. $a = b = c$.

Tada je $a(a^2-3) = 2$ iz čega slijedi $a = b = c = 2$, što povlači da je $x = y = z$. Budući da je $gcd(x, y) = gcd(y, z) = gcd(z, x) = 1$, dobivamo $x = y = z = 1$ i $t = 8$. Stoga je rješenje početne jednadžbe $(x, y, z, t) = (1, 1, 1, 8)$.

Drugi slučaj. $a = b$, $a \neq c$.

Tada imamo

$$a^2c - 2 = 2a + c \iff c(a^2 - 1) = 2(a + 1) \iff c(a - 1) = 2.$$

Ako je $c = 2$, onda je $a = 2 = c$, što je kontradikcija. Ako je $c = 1$, tada je $a = b = 3$, što povlači $x = y = 1$ i $z = 2$ pa je rješenje početne jednadžbe $(x, y, z, t) = (1, 1, 2, 9)$.

Treći slučaj. $a > b > c$.

Tada je $abc - 2 = a + b + c < 3a$. Stoga je $a(bc - 3) < 2$. Slijedi da je $bc - 3 < 2 \Longrightarrow bc < 5$. Tada imamo sljedeće slučajeve:

(a) $b = 2, c = 1 \Longrightarrow a = 5$. Dobivamo rješenje $(x, y, z, t) = (1, 2, 3, 10)$.

(b) $b = 3, c = 1 \Longrightarrow a = 3$ pa imamo drugi slučaj.

(c) $b = 4, c = 1 \Longrightarrow 3a = 7$, što je nemoguće.

Dakle, sva rješenja jednadžbe $(x+y)(y+z)(z+x) = txyz$ u prirodnim brojevima koja zadovoljavaju tražene uvjete su $(x, y, z, t) = (1, 1, 1, 8), (1, 1, 2, 9)$, $(1, 2, 3, 10)$ te ona dobivena permutacijama x, y i z.

Literatura

[1] I. Alković, M. Bliznac Trebješanin, *Metoda beskonačnog spusta i Fermatov posljednji teorem*, Acta Mathematica Spalatensia 3, 55.-62., 2020.

[2] T. Andreescu, D. Andrica, *Number Theory: Structures, Examples and Problems*. Birkhäuser, Boston, 2009.

[3] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations*. Birkhäuser, Boston 2010.

[4] A. Dujella, *Teorija brojeva*. Školska knjiga, Zagreb 2019.

[5] A. Kopecki, *Diofant i diofantske jednadžbe*, diplomski rad, Sveučilište J.J. Strossmayera u Osijeku, 2011.
`https://www.mathos.unios.hr/~mdjumic/uploads/diplomski/KOP08.pdf` (travanj 2024.)

[6] G. Korpal, *Diophantine equations*, izvješće o projektu, NISER, Bhubaneswar, 2015.
`https://gaurish4math.wordpress.com/wp-content/uploads/2015/12/diophantine-equations-gaurish-rev4.pdf` (veljača 2024.)

[7] J. Mandić, *Diofantske jednadžbe*, skripta, PMF-Matematički odsjek, Split.

Literatura

[8] D. Sučić, *Diofantske jednadžbe višeg stupnja*, diplomski rad, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, 2019. https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A8339/datastream/PDF/view (ožujak 2024.)