Titu Andreescu
Dorin Andrica
Ion Cucurezeanu

# An Introduction to Diophantine Equations

## A Problem-Based Approach

Birkhäuser

Titu Andreescu
Dorin Andrica
Ion Cucurezeanu

# An Introduction to Diophantine Equations

## A Problem-Based Approach

Birkhäuser

Titu Andreescu
School of Natural Sciences
and Mathematics
University of Texas at Dallas
800 W. Campbell Road
Richardson, TX 75080, USA
titu.andreescu@utdallas.edu

Ion Cucurezeanu
Faculty of Mathematics
and Computer Science
Ovidius University of Constanta
B-dul Mamaia, 124
900527 Constanta, Romania

Dorin Andrica
Faculty of Mathematics
and Computer Science
Babeş-Bolyai University
Str. Kogalniceanu 1
3400 Cluj-Napoca, Romania
dandrica@math.ubbcluj.ro
and
King Saud University
Department of Mathematics
College of Science
Riyadh 11451, Saudi Arabia
dandrica@ksu.edu.sa

ISBN 978-0-8176-4548-9 e-ISBN 978-0-8176–4549-6
DOI 10.1007/978-0-8176-4549-6
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010934856

Mathematics Subject Classification (2010): 11D04, 11D09, 11D25, 11D41, 11D45, 11D61, 11D68, 11-06, 97U40



Printed on acid-free paper

Birkhäuser is part of Springer Science+Business Media

www.birkhauser-science.com

# Preface

*Diophantus*, the "father of algebra," is best known for his book *Arithmetica*, a work on the solution of algebraic equations and the theory of numbers. However, essentially nothing is known of his life, and there has been much debate regarding precisely the years in which he lived.

Diophantus did his work in the great city of Alexandria. At this time, Alexandria was the center of mathematical learning. The period from 250 BCE to 350 CE in Alexandria is known as the Silver Age, also the Later Alexandrian Age. This was a time when mathematicians were discovering many ideas that led to our current conception of mathematics. The era is considered silver because it came after the Golden Age, a time of great development in the field of mathematics. This Golden Age encompasses the lifetime of Euclid.

The quality of mathematics from this period was an inspiration for the axiomatic methods of today's mathematics.

While it is known that Diophantus lived in the Silver Age, it is hard to pinpoint the exact years in which he lived. While many references to the work of Diophantus have been made, Diophantus himself made few references to other mathematicians' work, thus making the process of determining the time that he lived more difficult.

Diophantus did quote the definition of a polygonal number from the work of Hypsicles, who was active before 150 BCE, so we can conclude that Diophantus lived after that date. From the other end, Theon, a mathematician also from Alexandria, quoted the work of Diophantus in 350 CE. Most historians believe that Diophantus did most of his work around 250 CE. The greatest amount of information about Diophantus's life comes from the possibly fictitious collection of riddles written by Metrodorus around 500 CE. One of these is as follows:

> *His boyhood lasted* 1/6 *of his life; he married after* 1/7 *more; his beard grew after* 1/12 *more, and his son was born five years later; the son lived to half his father's age, and the father died four years after the son.*

Diophantus was the first to employ symbols in Greek algebra. He used a symbol (arithmos) for an unknown quantity, as well as symbols for algebraic operations and for powers. *Arithmetica* is also significant for its results in the theory of numbers, such as the fact that no integer of the form $8n+7$ can be written as the sum of three squares.

*Arithmetica* is a collection of 150 problems that give approximate solutions to equations up to degree three. *Arithmetica* also contains equations that deal with indeterminate equations. These equations deal with the theory of numbers.

The original *Arithmetica* is believed to have comprised 13 books, but the surviving Greek manuscripts contain only six.

The others are considered lost works. It is possible that these books were lost in a fire that occurred not long after Diophantus finished *Arithmetica*.

In what follows, we call a *Diophantine equation* an equation of the form

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

where $f$ is an $n$-variable function with $n \geq 2$. If $f$ is a polynomial with integral coefficients, then (1) is an *algebraic Diophantine equation*.

An $n$-uple $(x_1^0, x_2^0, \ldots, x_n^0) \in \mathbb{Z}^n$ satisfying (1) is called a *solution* to equation (1). An equation having one or more solutions is called *solvable*.

Concerning a Diophantine equation three basic problems arise:

**Problem 1.** Is the equation solvable?

**Problem 2.** If it is solvable, is the number of its solutions finite or infinite?

**Problem 3.** If it is solvable, determine all of its solutions.

Diophantus's work on equations of type (1) was continued by Chinese mathematicians (third century), Arabs (eight through twelfth centuries) and taken to a deeper level by Fermat, Euler,

Lagrange, Gauss, and many others. This topic remains of great importance in contemporary mathematics.

This book is organized in two parts. The first contains three chapters. Chapter 1 introduces the reader to the main elementary methods in solving Diophantine equations, such as decomposition, modular arithmetic, mathematical induction, and Fermat's infinite descent. Chapter 2 presents classical Diophantine equations, including linear, Pythagorean, higher-degree, and exponential equations, such as Catalan's. Chapter 3 focuses on Pell-type equations, serving again as an introduction to this special class of quadratic Diophantine equations. Chapter 4 contains some advanced methods involving Gaussian integers, quadratic rings, divisors of certain forms, and quadratic reciprocity. Throughout Part I, each of the sections contains representative examples that illustrate the theory.

Part II contains complete solutions to all exercises in Part I. For several problems, multiple solutions are presented, along with useful comments and remarks. Many of the selected exercises and problems are original or have been given original solutions by the authors.

The book is intended for undergraduates, high school students and teachers, mathematical contest (including Olympiad and Putnam) participants, as well as any person interested in mathematics.

We would like to thank Richard Stong for his careful reading of the manuscript. His pertinent suggestions have been very useful in improving the text.

June 2010

Titu Andreescu
Dorin Andrica
Ion Cucuruzeanu

# Contents

**Preface** **v**

**I Diophantine Equations** **1**

**I.1 Elementary Methods for Solving Diophantine Equations** **3**

1.1 The Factoring Method . . . . . 3

1.2 Solving Diophantine Equations Using Inequalities . 13

1.3 The Parametric Method . . . . . 20

1.4 The Modular Arithmetic Method . . . . . 29

1.5 The Method of Mathematical Induction . . . . . 36

1.6 Fermat's Method of Infinite Descent (FMID) . . . . 47

1.7 Miscellaneous Diophantine Equations . . . . . 58

**I.2 Some Classical Diophantine Equations 67**

2.1 Linear Diophantine Equations . . . . . 67

2.2 Pythagorean Triples and Related Problems . . . . . 76

2.3 Other Remarkable Equations . . . . . 88

**I.3 Pell-Type Equations 117**

3.1 Pell's Equation: History and Motivation . . . . . 118

3.2 Solving Pell's Equation . . . . . 121

3.3 The Equation $ax^2 - by^2 = 1$ . . . . . 135

3.4 The Negative Pell's Equation . . . . . 140

**I.4 Some Advanced Methods for Solving Diophantine Equations 147**

4.1 The Ring $\mathbb{Z}[i]$ of Gaussian Integers . . . . . 151

4.2 The Ring of Integers of $\mathbb{Q}[\sqrt{d}]$ . . . . . 162

4.3 Quadratic Reciprocity and Diophantine Equations . 178

4.4 Divisors of Certain Forms . . . . . 181

4.4.1 Divisors of $a^2 + b^2$ . . . . . 182

4.4.2 Divisors of $a^2 + 2b^2$ . . . . . 186

4.4.3 Divisors of $a^2 - 2b^2$ . . . . . 188

**II Solutions to Exercises and Problems 191**

**II.1 Solutions to Elementary Methods for Solving Diophantine Equations 193**

1.1 The Factoring Method . . . . . 193

1.2 Solving Diophantine Equations Using Inequalities . 202

1.3 The Parametric Method . . . . . 213

1.4 The Modular Arithmetic Method . . . . . 219
1.5 The Method of Mathematical Induction . . . . . 229
1.6 Fermat's Method of Infinite Descent (FMID) . . . . 239
1.7 Miscellaneous Diophantine Equations . . . . . 253

**II.2 Solutions to Some Classical Diophantine Equations 265**

2.1 Linear Diophantine Equations . . . . . 265
2.2 Pythagorean Triples and Related Problems . . . . . 273
2.3 Other Remarkable Equations . . . . . 278

**II.3 Solutions to Pell-Type Equations 289**

3.1 Solving Pell's Equation by Elementary Methods . . 289
3.2 The Equation $ax^2 - by^2 = 1$ . . . . . 298
3.3 The Negative Pell's Equation . . . . . 301

**II.4 Solutions to Some Advanced Methods in Solving Diophantine Equations 309**

4.1 The Ring $\mathbb{Z}[i]$ of Gaussian Integers . . . . . 309
4.2 The Ring of Integers of $\mathbb{Q}[\sqrt{d}]$ . . . . . 314
4.3 Quadratic Reciprocity and Diophantine Equations . 322
4.4 Divisors of Certain Forms . . . . . 324

**References 327**

**Glossary 331**

**Index 341**

# Part I

# Diophantine Equations

# I.1

# Elementary Methods for Solving Diophantine Equations

## 1.1 The Factoring Method

Given the equation $f(x_1, x_2, \ldots, x_n) = 0$, we write it in the equivalent form

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

where $f_1, f_2, \ldots, f_k \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$ and $a \in \mathbb{Z}$. Given the prime factorization of $a$, we obtain finitely many decompositions into $k$ integer factors $a_1, a_2, \ldots, a_k$. Each such factorization yields a system of equations

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

Solving all such systems gives the complete set of solutions to (1).

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*,
DOI 10.1007/978-0-8176-4549-6_1, © Springer Science+Business Media, LLC 2010

We illustrate this method by presenting a few examples.

**Example 1.** *Find all integral solutions to the equation*

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

(Titu Andreescu)

*Solution.* Write the equation in the form

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

or

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

This is equivalent to

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

or

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

If $(x+1)(y-1)=2$, we obtain the systems of equations

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

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

yielding the solutions $(1,2),(-3,0),(0,3),(-2,-1)$.

If $(x+1)(y-1)=-2$, we obtain the systems

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

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

whose solutions are $(1,0),(-3,2),(0,-1),(-2,3)$.

All eight pairs that we have found satisfy the given equation.

**Example 2.** *Let $p$ and $q$ be two primes. Solve in positive integers the equation*

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

*Solution.* The equation is equivalent to the algebraic Diophantine equation

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

Observe that $\frac{1}{x}<\frac{1}{pq}$ hence we have $x>pq$.

Considering all positive divisors of $p^2q^2$ we obtain the following systems:

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

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

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

yielding the solutions

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

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

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

**Remark.** The equation

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n},$$

where $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, has $(2\alpha_1+1)\cdots(2\alpha_k+1)$ solutions in positive integers.

Indeed, the equation is equivalent to

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

and $n^2=p_1^{2\alpha_1}\cdots p_k^{2\alpha_k}$ has $(2\alpha_1+1)\cdots(2\alpha_k+1)$ positive divisors.

**Example 3.** *Determine all nonnegative integral pairs $(x,y)$ for which*

$$(xy-7)^2=x^2+y^2.$$

(Indian Mathematical Olympiad)

*Solution.* The equation is equivalent to

$$(xy-6)^2+13=(x+y)^2,$$

or

$$(xy-6)^2-(x+y)^2=-13.$$

We obtain the equation

$$[xy-6-(x+y)][xy-6+(x+y)]=-13,$$

yielding the systems

$$\begin{cases} xy-6-(x+y)=-1,\\ xy-6+(x+y)=13, \end{cases} \qquad \begin{cases} xy-6-(x+y)=-13,\\ xy-6+(x+y)=1. \end{cases}$$

These systems are equivalent to

$$\begin{cases} x+y=7, \\ xy=12, \end{cases} \qquad \begin{cases} x+y=7, \\ xy=0. \end{cases}$$

The solutions to the equation are $(3,4),(4,3),(0,7),(7,0)$.

**Example 4.** *Solve the following equation in integers $x, y$:*

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

(Polish Mathematical Olympiad)

*Solution.* Setting $x=u+1$, $y=v+1$, the equation becomes

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

which is equivalent to

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

The last equation could be written as

$$uv(u+v+4)+(u+v+4)=5,$$

or

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

One of the factors must be equal to 5 or $-5$ and the other to 1 or $-1$. This means that the sum $u+v$ and the product $uv$ have to satisfy one of the four systems of equations:

$$\begin{cases} u+v=1, \\ uv=0, \end{cases} \qquad \begin{cases} u+v=-9, \\ uv=-2, \end{cases}$$

$$\begin{cases} u+v=-3, \\ uv=4, \end{cases} \qquad \begin{cases} u+v=-5, \\ uv=-6. \end{cases}$$

Only the first and the last of these systems have integral solutions. They are $(0,1),(1,0),(-6,1),(1,-6)$. Hence the final outcome $(x,y)=(u+1,v+1)$ must be one of the pairs $(1,2)$, $(-5,2)$, $(2,1)$, $(2,-5)$.

**Example 5.** *Find all integers $n$ for which the equation*

$$x^3+y^3+z^3-3xyz=n$$

*is solvable in positive integers.*

(Titu Andreescu)

*Solution.*

We rewrite the identity

$$x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-zx)$$

as

$$x^3+y^3+z^3-3xyz=(x+y+z)\cdot\frac{1}{2}\Big[(x-y)^2+(y-z)^2+(z-x)^2\Big] \quad (1)$$

and

$$x^3+y^3+z^3-3xyz=(x+y+z)^3-3(x+y+z)(xy+yz+zx). \quad (2)$$

From (1) we see that the equation is solvable for $n=3k+1$ and $n=3k+2$, $k\geq 1$, since triples of the form $(k+1,k,k)$ and $(k+1,k+1,k)$ are solutions to the given equation.

If $n$ is divisible by 3, then from (2) it follows that $x+y+z$ is divisible by 3, and so $n=x^3+y^3+z^3-3xyz$ is divisible by 9.

Conversely, the given equation is solvable in positive integers for all $n = 9k$, $k \geq 2$, since triples of the form $(k-1, k, k+1)$ satisfy the equation, as well as for $n = 0$ $(x = y = z)$.

In conclusion, $n = 3k+1$, $k \geq 1$, $n = 3k+2$, $k \geq 1$, and $n = 9k$, $k = 0, 2, 3, 4, \ldots$.

**Example 6.** *Find all triples of positive integers* $(x, y, z)$ *such that*

$$x^3 + y^3 + z^3 - 3xyz = p,$$

*where* $p$ *is a prime greater than* 3.

(Titu Andreescu, Dorin Andrica)

*Solution.* The equation is equivalent to

$$(x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx) = p.$$

Since $x+y+z > 1$, we must have $x+y+z = p$ and $x^2+y^2+z^2-xy-yz-zx = 1$. The last equation is equivalent to $(x-y)^2 + (y-z)^2 + (z-x)^2 = 2$. Without loss of generality, we may assume that $x \geq y \geq z$. If $x > y > z$, we have $x - y \geq 1$, $y - z \geq 1$ and $x - z \geq 2$, implying $(x-y)^2 + (y-z)^2 + (z-x)^2 \geq 6 > 2$.

Therefore we must have $x = y = z + 1$ or $x - 1 = y = z$. The prime $p$ has one of the forms $3k+1$ or $3k+2$. In the first case the solutions are $\left(\frac{p+2}{3}, \frac{p-1}{3}, \frac{p-1}{3}\right)$ and the corresponding permutations. In the second case the solutions are $\left(\frac{p+1}{3}, \frac{p+1}{3}, \frac{p-2}{3}\right)$ and the corresponding permutations.

**Example 7.** *Find all triples* $(x, y, z)$ *of integers such that*

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

*Solution.* From the identity

$$(x+y+z)^3 = x^3+y^3+z^3+3(x+y)(y+z)(z+x)$$

we obtain $8 = (x+y)(y+z)(z+x)$. It follows that $(3-x)(3-y)(3-z) = 8$. On the other hand, $(3-x)+(3-y)+(3-z)-3(x+y+z) = 6$, implying that either $3-x$, $3-y$, $3-z$ are all even, or exactly one of them is even. In the first case, we get $|3-x| = |3-y| = |3-z| = 2$, yielding $x, y, z \in \{1, 5\}$. Because $x+y+z = 3$, the only possibility is $x = y = z = 1$. In the second case, one of $|3-x|$, $|3-y|$, $|3-z|$ must be 8, say $|3-x| = 8$, yielding $x \in \{-5, 11\}$ and $|3-y| = |3-z| = 1$, from which $y, z \in \{2, z\}$. Taking into account that $x+y+z = 3$, the only possibility is $x = -5$ and $y = z = 4$. In conclusion, the desired triples are $(1,1,1)$, $(-5,4,4)$, $(4,-5,4)$, and $(4,4,-5)$.

**Example 8.** *Find all primes $p$ for which the equation $x^4+4 = py^4$ is solvable in integers.*

(Ion Cucurezeanu)

*Solution.* The equation is not solvable in integers for $p = 2$, for the left-hand side must be even, hence 4 (mod 16), while the right-hand side is either 0 (mod 16) or 2 (mod 16). The same modular arithmetic argument shows that for each odd prime $p$, $x$ and $y$ must be odd. The equation is equivalent to $(x^2+2)^2-(2x)^2 = py^4$, which can be written as $(x^2-2x+2)(x^2+2x+2) = py^4$. We have $\gcd(x^2-2x+2, x^2+2x+2) = 1$. Indeed, if $d \mid x^2-2x+2$ and $d \mid x^2+2x+2$, then $d$ must be odd, and we have $d \mid 4x$. It follows that $d \mid x$; hence we get $d = 1$. Because $\gcd(x^2-2x+2, x^2+2x+2) = 1$, taking into account that $x^2-2x+2 = a^4$ and $x^2+2x+2 = pb^4$ for some positive

integers $a$ and $b$ whose product is $y$, it follows that $(x-1)^2+1=a^4$ and $(x+1)^2+1=pb^4$. The first equation yields $a^2=1$ and $x=1$; hence the second gives $p=5$ and $b^2=1$. Therefore, the only prime for which the equation is solvable is $p=5$. In this case the solutions $(x,y)$ are $(1,1)$, $(-1,1)$, $(1,-1)$, and $(-1,-1)$.

## Exercises and Problems

**1.** Solve the following equation in integers $x, y$ :

$$x^2+6xy+8y^2+3x+6y=2.$$

**2.** For each positive integer $n$, let $s(n)$ denote the number of ordered pairs $(x,y)$ of positive integers for which

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

Find all positive integers $n$ for which $s(n)=5$.

(Indian Mathematical Olympiad)

**3.** Let $p$ and $q$ be distinct prime numbers. Find the number of pairs of positive integers $x, y$ that satisfy the equation

$$\frac{p}{x}+\frac{q}{y}=1.$$

(KöMaL)

**4.** Find the positive integer solutions to the equation

$$x^3-y^3=xy+61.$$

(Russian Mathematical Olympiad)

**5.** Solve the Diophantine equation

$$x - y^4 = 4,$$

where $x$ is a prime.

**6.** Find all pairs $(x, y)$ of integers such that

$$x^6 + 3x^3 + 1 = y^4.$$

(Romanian Mathematical Olympiad)

**7.** Solve the following equation in nonzero integers $x, y$ :

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

(16th USA Mathematical Olympiad)

**8.** Find all integers $a, b, c$ with $1 < a < b < c$ such that the number $(a-1)(b-1)(c-1)$ is a divisor of $abc - 1$.

(33rd IMO)

**9.** Find all right triangles with integer side lengths such that their areas and perimeters are equal.

**10.** Solve the following system in integers $x, y, z, u, v$:

$$\begin{cases} x + y + z + u + v = xyuv + (x + y)(u + v), \\ xy + z + uv = xy(u + v) + uv(x + y). \end{cases}$$

(Titu Andreescu)

**11.** Prove that the equation $x(x+1) = p^{2n}y(y+1)$ is not solvable in positive integers, where $p$ is a prime and $n$ is a positive integer.

**12.** Find all triples $(x, y, p)$, where $x$ and $y$ are positive integers and $p$ is a prime, satisfying the equation

$$x^5 + x^4 + 1 = p^y.$$

(Titu Andreescu)

**13.** Find all pairs $(x, y)$ of integers such that

$$xy + \frac{x^3 + y^3}{3} = 2007.$$

(Titu Andreescu)

## 1.2 Solving Diophantine Equations Using Inequalities

This method consists in restricting the intervals in which the variables lie using appropriate inequalities. Generally, this process leads to only finitely many possibilities for all variables or for some of them.

**Example 1.** *Find all pairs $(x, y)$ of integers such that*

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

*Solution.* Note that all pairs of the form $(k, -k)$, $k \in \mathbb{Z}$, are solutions. If $x + y \neq 0$, the equation becomes

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

which is equivalent to

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

It follows that $(x-1)^2 \leq 1$ and $(y-1)^2 \leq 1$, restricting the interval in which the variables $x, y$ lie to $[0, 2]$. We obtain the solutions $(0,1), (1,0), (1,2), (2,1), (2,2)$.

**Example 2.** *Solve the following equation in positive integers* $x, y, z$ :

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

(Romanian Mathematical Olympiad)

*Solution.* Taking symmetry into account, we may assume that $2 \leq x \leq y \leq z$. This implies the inequality $\frac{3}{x} \geq \frac{3}{5}$, and hence $x \in \{2, 3, 4, 5\}$.

If $x = 2$, then $\frac{1}{y} + \frac{1}{z} = \frac{1}{10}$ with $y \in \{11, 12, \ldots, 20\}$. It follows that $z = 10 + \frac{100}{y-10}$ and $(y-10) \mid 100$. We obtain the solutions $(2, 11, 110)$, $(2, 12, 60)$, $(2, 14, 35)$, $(2, 15, 30)$, $(2, 20, 20)$.

If $x = 3$, we have $\frac{1}{y} + \frac{1}{z} = \frac{4}{15}$ with $y \in \{3, 4, 5, 6, 7\}$. We obtain the solutions $(3, 4, 60)$, $(3, 5, 15)$, $(3, 6, 10)$.

If $x = 4$, then $\frac{1}{y} + \frac{1}{z} = \frac{7}{20}$ with $y \in \{4, 5\}$, and the solution is $(4, 4, 10)$.

If $x = 5$, then $\frac{1}{y} + \frac{1}{z} = \frac{2}{5}$ and $y = z = 5$, yielding the solution $(5, 5, 5)$.

**Example 3.** *Find all quadruples* $(x, y, z, w)$ *of positive integers for which*

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

(Titu Andreescu)

*Solution.* We have

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

It follows that

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

Hence $x^2+y^2+z^2+2xy+2x(z-1)+2y(z+1)$ can be equal only to $(x+y+z)^2$. This implies $x=y$ therefore the solutions are $(m,m,n,2m+n)$, $m,n \in \mathbb{Z}_+$.

**Example 4.** *Find all solutions in integers of the equation*

$$x^3+(x+1)^3+(x+2)^3+\cdots+(x+7)^3 = y^3.$$

(Hungarian Mathematical Olympiad)

*Solution.* The solutions are $(-2,6),(-3,4),(-4,-4),(-5,-6)$. Let

$$P(x) = x^3+(x+1)^3+(x+2)^3+\cdots+(x+7)^3 = 8x^3+84x^2+420x+784.$$

If $x \geq 0$, then

$$\begin{aligned}(2x+7)^3 &= 8x^3+84x^2+294x+343\\ &< P(x) < 8x^3+120x^2+600x+1000 = (2x+10)^3,\end{aligned}$$

so $2x+7 < y < 2x+10$; therefore $y$ is $2x+8$ or $2x+9$. But neither of the equations

$$\begin{aligned}P(x)-(2x+8)^3 &= -12x^2+36x+272 = 0,\\ P(x)-(2x+9)^3 &= -24x^2-66x+55 = 0,\end{aligned}$$

has any integer roots, so there are no solutions with $x \geq 0$. Next, note that $P$ satisfies $P(-x-7) = -P(x)$, so $(x,y)$ is a solution if and only if $(-x-7,-y)$ is a solution. Therefore there are no solutions with $x \leq -7$. So for $(x,y)$ to be a solution, we must have

$-6 \le x \le -1$. For $-3 \le x \le -1$, we have $P(-1) = 440$, not a cube, $P(-2) = 216 = 6^3$, and $P(-3) = 64 = 4^3$, so $(-2, 6)$ and $(-3, 4)$ are the only solutions with $-3 \le x \le -1$. Therefore $(-4, -4)$ and $(-5, -6)$ are the only solutions with $-6 \le x \le -4$. Hence the only solutions are $(-2, 6), (-3, 4), (-4, -4)$, and $(-5, -6)$.

**Example 5.** *Find all triples $(x, y, z)$ of positive integers such that*

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

(United Kingdom Mathematical Olympiad)

*Solution.* Without loss of generality we may assume $x \ge y \ge z$. Note that we must have $2 \le (1 + 1/z)^3$, which implies that $z \le 3$.

If $z = 1$, then $\left(1 + \frac{1}{x}\right)\left(1 + \frac{1}{y}\right) = 1$, which is clearly impossible.

The case $z = 2$ leads to $\left(1 + \frac{1}{x}\right)\left(1 + \frac{1}{y}\right) = \frac{4}{3}$. Therefore $\frac{4}{3} \le \left(1 + \frac{1}{y}\right)^2$, which forces $y < 7$. Since $1 + \dfrac{1}{x} > 1$, we obtain $y > 3$. Plugging in the appropriate values yields the solutions $(7, 6, 2), (9, 5, 2), (15, 4, 2)$.

If $z = 3$, then $\left(1 + \frac{1}{x}\right)\left(1 + \frac{1}{y}\right) = \frac{3}{2}$. Similar analysis leads to $y < 5$ and $y \ge z = 3$. These values yield the solutions $(8, 3, 3)$ and $(5, 4, 3)$.

In conclusion, the solutions are all permutations of $(7, 6, 2)$, $(9, 5, 2)$, $(15, 4, 2)$, $(8, 3, 3)$ and $(5, 4, 3)$.

**Example 6.** *Find all positive integers $n, k_1, \ldots, k_n$ such that*

$$k_1 + \cdots + k_n = 5n - 4$$

*and*

$$\frac{1}{k_1} + \cdots + \frac{1}{k_n} = 1.$$

(Putnam Mathematical Competition)

*Solution.* By the arithmetic–harmonic mean(AM–HM) inequality or the Cauchy–Schwarz inequality,

$$(k_1 + \cdots + k_n)\left(\frac{1}{k_1} + \cdots + \frac{1}{k_n}\right) \geq n^2.$$

We must thus have $5n - 4 \geq n^2$, so $n \leq 4$. Without loss of generality, we may suppose that $k_1 \leq \cdots \leq k_n$.

If $n = 1$, we must have $k_1 = 1$, which works. Note that hereinafter we cannot have $k_1 = 1$.

If $n = 2$, then $(k_1, k_2) \in \{(2, 4), (3, 3)\}$, neither of which works.

If $n = 3$, then $k_1 + k_2 + k_3 = 11$, so $2 \leq k_1 \leq 3$. Hence $(k_1, k_2, k_3) \in \{(2, 2, 7), (2, 3, 6), (2, 4, 5), (3, 3, 5), (3, 4, 4)\}$, and only $(2, 3, 6)$ works.

If $n = 4$, we must have equality in the AM–HM inequality, which happens only when $k_1 = k_2 = k_3 = k_4 = 4$. Hence the solutions are $n = 1$ and $k_1 = 1$, $n = 3$ and $(k_1, k_2, k_3)$ is a permutation of $(2, 3, 6)$, and $n = 4$ and $(k_1, k_2, k_3, k_4) = (4, 4, 4, 4)$.

## Exercises and Problems

**1.** Solve in positive integers the equation

$$3(xy + yz + zx) = 4xyz.$$

**2.** Find all triples $(x, y, z)$ of positive integers such that

$$xy + yz + zx - xyz = 2.$$

**3.** Determine all triples $(x, y, z)$ of positive integers such that

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

(Romanian Mathematical Olympiad)

**4.** Determine all pairs $(x, y)$ of integers that satisfy the equation

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

(Australian Mathematical Olympiad)

**5.** Prove that all the equations

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

where $a \in \{3, 4, 5\}$, $b \in \{4, 5, \ldots, 12\}$, $c \in \{1, 2, \ldots, 8\}$, are not solvable in positive integers.

(Dorin Andrica)

**6.** Solve in positive integers the equation

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

**7.** Find all integer solutions to the equation

$$(x^2 - y^2)^2 = 1 + 16y.$$

(Russian Mathematical Olympiad)

**8.** Find all integers $a, b, c, x, y, z$ such that

$$a + b + c = xyz,$$
$$x + y + z = abc,$$

and $a \geq b \geq c \geq 1$, $x \geq y \geq z \geq 1$.

(Polish Mathematical Olympiad)

**9.** Let $x, y, z, u$, and $v$ be positive integers such that

$$xyzuv = x + y + z + u + v.$$

Find the maximum possible value of $\max\{x, y, z, u, v\}$.

**10.** Solve in distinct positive integers the equation

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

(Titu Andreescu)

**11.** Find all positive integers $x, y, z, t$ such that

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

for some integer $n \geq 2$.

**12.** Find all pairs $(x, y)$ of positive integers such that $x^y = y^x$.

**13.** Solve in positive integers the equation $x^y + y = y^x + x$.

**14.** Let $a$ and $b$ be positive integers such that $ab+1$ divides $a^2+b^2$. Prove that $\frac{a^2+b^2}{ab+1}$ is the square of an integer.

(29th IMO)

**15.** Find all integers $n$ for which the equation

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

is solvable in positive integers.

(American Mathematical Monthly, reformulation)

## 1.3 The Parametric Method

In many situations the integral solutions to a Diophantine equation

$$f(x_1, x_2, \ldots, x_n) = 0$$

can be represented in a parametric form as follows:

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

where $g_1, g_2, \ldots, g_n$ are integer-valued $l$-variable functions and $k_1, \ldots, k_l \in \mathbb{Z}$.

The set of solutions to some Diophantine equations might have multiple parametric representations.

For most Diophantine equations it is not possible to find all solutions explicitly. In many such cases the parametric method provides a proof of the existence of infinitely many solutions.

**Example 1.** *Prove that there are infinitely many triples $(x, y, z)$ of integers such that*

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

(Tournament of Towns)

*Solution.* Setting $z = -y$, the equation becomes $x^3 = x^2 + 2y^2$. Taking $y = mx$, $m \in \mathbb{Z}$, yields $x = 1 + 2m^2$. We obtain the infinite family of solutions

$$x = 2m^2 + 1, \quad y = m(2m^2 + 1), \quad z = -m(2m^2 + 1), \quad m \in \mathbb{Z}.$$

**Example 2.** *(a) Let $m$ and $n$ be distinct positive integers. Prove that there exist infinitely many triples $(x, y, z)$ of positive integers*

*such that*

$$x^2 + y^2 = (m^2 + n^2)^z,$$

*with*

*(i) $z$ odd; (ii) $z$ even.*

*(b) Prove that the equation*

$$x^2 + y^2 = 13^z$$

*has infinitely many solutions in positive integers $x, y, z$.*

*Solution.* (a) For (i), consider the family

$$x_k = m(m^2 + n^2)^k, \quad y_k = n(m^2 + n^2)^k, \quad z_k = 2k + 1, \quad k \in \mathbb{Z}_+.$$

For (ii), consider the family

$$x_k = |m^2 - n^2|(m^2 + n^2)^{k-1}, \quad y_k = 2mn(m^2 + n^2)^{k-1},$$

$$z_k = 2k, \ k \in \mathbb{Z}_+.$$

(b) Since $2^2 + 3^2 = 13$, we can take $m = 2$, $n = 3$ and obtain the families of solutions

$$x'_k = 2 \cdot 13^k, \quad y'_k = 3 \cdot 13^k, \quad z'_k = 2k + 1, \quad k \in \mathbb{Z}_+;$$

$$x''_k = 5 \cdot 13^{k-1}, \quad y''_k = 12 \cdot 13^{k-1}, \quad z''_k = 2k, \quad k \in \mathbb{Z}_+.$$

**Remarks.** (1) Taking into account Lagrange's identity

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

we can generate an infinite family of solutions by defining recursively the sequences $(x_k)_{k\geq 1}$, $(y_k)_{k\geq 1}$ as follows:

$$\begin{cases} x_{k+1} = mx_k - ny_k, \\ y_{k+1} = nx_k + my_k, \end{cases}$$

where $x_1 = m$, $y_1 = n$.

It is not difficult to check that $(|x_k|, y_k, k)$, $k \in \mathbb{Z}_+$, are solutions to the given equation.

(2) Another way to generate an infinite family of solutions is with complex numbers. Let $k$ be a positive integer. We have $(m + in)^k = A_k + iB_k$, where $A_k, B_k \in \mathbb{Z}$. Taking moduli, we obtain

$$(m^2 + n^2)^k = A_k^2 + B_k^2,$$

and thus $(|A_k|, |B_k|, k)$ is a solution to the given equation.

**Example 3.** *Find all triples* $(x, y, z)$ *of positive integers such that*

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

*Solution.* The equation is equivalent to

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

Let $d = \gcd(x, y)$. Then $x = dm$, $y = dn$, with $\gcd(m, n) = 1$. It follows that $\gcd(mn, m + n) = 1$. Therefore

$$z = \frac{dmn}{m + n},$$

which implies $(m + n) \mid d$, i.e., $d = k(m + n)$, $k \in \mathbb{Z}_+$.

The solutions to the equation are given by

$$x = km(m + n), \quad y = kn(m + n), \quad z = kmn,$$

where $k, m, n \in \mathbb{Z}_+$.

**Remark.** (1) If $a, b, c$ are positive integers with no common factor such that

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

then $a+b$ is a square. Indeed, $k=1$, $a=m(m+n)$, $b=n(m+n)$, and hence $a+b=(m+n)^2$.

(2) If $a,b,c$ are positive integers satisfying

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

then $a^2+b^2+c^2$ is a square. Indeed,

$$\begin{aligned} a^2+b^2+c^2 &= k^2\Big[m^2(m+n)^2+n^2(m+n)^2+m^2n^2\Big] \\ &= k^2\Big[(m+n)^4-2mn(m+n)^2+m^2n^2\Big] \\ &= k^2\Big[(m+n)^2-mn\Big]^2. \end{aligned}$$

**Example 4.** *Prove that for each integer $n\geq 3$ the equation*

$$x^n+y^n=z^{n-1}$$

*has infinitely many solutions in positive integers.*

*Solution.* An infinite family of solutions is given by

$$x_k=k(k^n+1)^{n-2},\quad y_k=(k^n+1)^{n-2},\quad z_k=(k^n+1)^{n-1},\quad k\in\mathbb{Z}_+.$$

**Example 5.** *Let $a,b$ be positive integers. Prove that the equation*

$$x^2-2axy+(a^2-4b)y^2+4by=z^2$$

*has infinitely many positive integer solutions $(x_j,y_j,z_j)$, where $(x_j)$, $(y_j)$, $(z_j)$ are increasing sequences.*

(Dorin Andrica)

*Solution.* We will use the following auxiliary result:

**Lemma.** *If $A, B$ are relatively prime positive integers, then there exist positive integers $u, v$ such that*

$$Au - Bv = 1. \tag{1}$$

*Proof.* Consider the integers

$$1 \cdot A,\ 2 \cdot A, \ldots, (B-1) \cdot A \tag{2}$$

modulo $B$. All these remainders are distinct. Indeed, if

$$k_1 A = q_1 B + r \qquad \text{and} \qquad k_2 A = q_2 B + r$$

for some $k_1, k_2 \in \{1, 2, \ldots, B-1\}$, then

$$(k_1 - k_2)A = (q_1 - q_2)B \equiv 0 \pmod{B}.$$

Since $\gcd(A, B) = 1$, it follows that $|k_1 - k_2| \equiv 0 \pmod{B}$.

Taking into account that $k_1, k_2 \in \{1, 2, \ldots, B-1\}$, we have $|k_1 - k_2| < B$. Thus $k_1 - k_2 = 0$.

It is not difficult to see that $k \cdot A \not\equiv 0 \pmod{B}$ for all $k \in \{1, 2, \ldots, B-1\}$. Hence at least one of the integers (2) gives remainder 1 on division by $B$, i.e., there exist $u \in \{1, 2, \ldots, B-1\}$ and $v \in \mathbb{Z}_+$ such that $A \cdot u = B \cdot v + 1$. □

**Remark.** Let $(u_0, v_0)$ be the *minimal* solution in positive integers to equation (1), i.e., $u_0$ (and $v_0$) is minimal. Then all solutions in positive integers to equation (1) are given by

$$u_m = u_0 + Bm, \quad v_m = v_0 + Am, \quad m \in \mathbb{Z}_+. \tag{3}$$

Returning to the original problem, let us consider the sequence $(y_n)_{n\geq 1}$, given by

$$y_{n+1} = by_n^2 + ay_n + 1, \quad y_1 \in \mathbb{Z}_+. \tag{4}$$

Clearly $\gcd(y_n, y_{n+1}) = 1$, $n \in \mathbb{Z}_+$. From the above Lemma, there is a sequence of positive integers $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$ such that

$$y_{n+1}u_n - y_n v_n = 1, \quad n \in \mathbb{Z}_+.$$

From (4) we obtain

$$bu_n y_n^2 + (au_n - v_n)y_n + u_n - 1 = 0, \quad n \in \mathbb{Z}_+. \tag{5}$$

Regarding (5) as a quadratic equation in $y_n$ and taking into account that $y_n \in \mathbb{Z}_+$, it follows that the discriminant

$$D_n = (au_n - v_n)^2 - 4bu_n(u_n - 1)$$

is a perfect square. That is,

$$v_n^2 - 2au_n v_n + (a^2 - 4b)u_n^2 + 4bu_n = z_n^2, \quad n \in \mathbb{Z}_+.$$

It is clear that the sequences $(u_n)_{n\geq 1}$ and $(v_n)_{n\geq 1}$ contain strictly increasing subsequences $(u_{n_j})_{j\geq 1}$, $(v_{n_j})_{j\geq 1}$, respectively. An infinite family of solutions with the desired property is given by $(v_{n_j}, u_{n_j}, z_{n_j})$, $j \geq 1$.

**Remark.** The left-hand side of the given equation, which we may write as

$$(x - ay)^2 - 4by(y - 1),$$

is the discriminant of the quadratic equation

$$byt^2 + (ay - x)t + y - 1 = 0,$$

with a new unknown $t$. Therefore, this discriminant is a perfect square if the last equation has an integer root. (As we know, the square root of a nonnegative integer is either irrational or an integer.) Rewriting the equation in the form

$$y(bt^2 + at + 1) = 1 + xt,$$

we can see that the number $t = 1$ is a root if

$$y(b + a + 1) = 1 + x,$$

which is satisfied by infinitely many pairs of integers $(x, y)$. In this case, by routine computation, we get $z = by - y + 1$. Thus we have found an infinite family of solutions

$$x = (a + b + 1)m - 1, \quad y = m, \quad z = (b - 1)m + 1, \ m \in Z_+.$$

**Example 6.** *Prove that the equation*

$$2^x + 1 = xy$$

*has infinitely many solutions in positive integers.*

*Solution.* It suffices to prove that $3^k$ divides $2^{3^k} + 1$ for all $k \geq 0$. Indeed, for all $k \geq 1$,

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

The first factor can be written as $(3 - 1)^{3^{k-1}} + 1$, and since $(-1)^{3^{k-1}} + 1 = 0$, it is divisible by $3^{k-1}$. The second factor is equal to $\left(2^{3^{k-1}} + 1\right)^2 - 3 \cdot 2^{3^{k-1}}$, which is clearly divisible by 3. Hence $\left(3^k, \frac{2^{3^k}+1}{3^k}\right)$, $k \geq 0$, are all solutions to the given equation.

## Exercises and Problems

**1.** Prove that the equation

$$x^2 = y^3 + z^5$$

has infinitely many solutions in positive integers.

**2.** Show that the equation

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

has infinitely many solutions in relatively prime integers.

(United Kingdom Mathematical Olympiad)

**3.** Prove that for each integer $n \geq 2$ the equation

$$x^n + y^n = z^{n+1}$$

has infinitely many solutions in positive integers.

**4.** Let $n$ be an integer greater than 2. Prove that the equation

$$x^n + y^n + z^n + u^n = v^{n-1}$$

has infinitely many solutions $(x, y, z, u, v)$ in positive integers.

(Dorin Andrica)

**5.** Let $a, b, c, d$ be positive integers with $\gcd(a, b) = 1$. Prove that the following system of equations has infinitely many solutions in positive integers:

$$\begin{cases} ax - yz - c = 0, \\ bx - yt + d = 0. \end{cases}$$

(Titu Andreescu)

**6.** Find all triples $(x, y, z)$ of integers such that

$$xy(z+1) = (x+1)(y+1)z.$$

**7.** Solve in integers the equation

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

**8.** Prove that the equation

$$x^3 + y^3 + z^3 + w^3 = 2008$$

has infinitely many solutions in integers.

(Titu Andreescu)

**9.** Prove that there are infinitely many quadruples $(x, y, z, w)$ of positive integers such that

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

(Titu Andreescu)

**10.** Prove that each of the following equations has infinitely many solutions in integers $x, y, z, u$:

$$x^2 + y^2 + z^2 = 2u^2,$$
$$x^4 + y^4 + z^4 = 2u^2.$$

**11.** Prove that there are infinitely many quadruples $(x, y, u, v)$ of positive integers such that $xy + 1$, $xu + 1$, $xv + 1$, $yu + 1$, $yv + 1$, $uv + 1$ are all perfect squares.

## 1.4 The Modular Arithmetic Method

In many situations, simple modular arithmetic considerations are employed in proving that certain Diophantine equations are not solvable or in reducing the range of their possible solutions.

**Example 1.** *Prove that the equation*

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

*is not solvable.*

*Solution.* Let $x = z - 1001$. The equation becomes

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

or

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

It follows that

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

or equivalently,

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

The left-hand side is congruent to 2 (mod 3), so it cannot be a perfect square.

**Example 2.** *Find all pairs $(p, q)$ of prime numbers such that*

$$p^3 - q^5 = (p+q)^2.$$

(Russian Mathematical Olympiad)

*Solution.* The only solution is $(7, 3)$. First suppose that neither $p$ nor $q$ equals 3. Then $p \equiv 1$ or $2 \pmod 3$ and $q \equiv 1$ or $2 \pmod 3$. If $p \equiv q \pmod 3$, then the left-hand side is divisible by 3, while the right-hand side is not. If $p \not\equiv q \pmod 3$, the right-hand side is divisible by 3, while the left-hand side is not.

If $p = 3$, then $q^5 < 27$, which is impossible.

If $q = 3$, we obtain $p^3 - 243 = (p+3)^2$, whose only integer solution is $p = 7$.

**Example 3.** *Prove that the equation $x^5 - y^2 = 4$ has no solutions in integers.*

(Balkan Mathematical Olympiad)

*Solution.* We consider the equation modulo 11. Since $(x^5)^2 = x^{10} \equiv 0$ or $1 \pmod{11}$ for all $x$, we have $x^5 \equiv -1,\ 0$, or $1 \pmod{11}$. So $x^5 - 4$ is either $6, 7$, or 8 modulo 11. However, the quadratic residues modulo 11 are $0, 1, 3, 4, 5$, and 9, so the equation has no integral solutions.

**Example 4.** *Determine all primes $p$ for which the system of equations*

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

*has a solution in integers $x, y$.*

(German Mathematical Olympiad)

*Solution.* The only such prime is $p = 7$. Assume without loss of generality that $x, y \geq 0$. Note that $p + 1 = 2x^2$ is even, so $p \neq 2$. Also, $2x^2 \equiv 1 \equiv 2y^2 \pmod p$, which implies $x \equiv \pm y \pmod p$, since

$p$ is odd. Since $x < y < p$, we have $x + y = p$. Then

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

so $p = 4x - 1$, $2x^2 = 4x$, $x$ is 0 or 2, and $p$ is $-1$ or 7. Of course, $-1$ is not prime, but for $p = 7$, $(x, y) = (2, 5)$ is a solution.

**Example 5.** *Prove that if $n$ is a positive integer such that the equation*

$$x^3 - 3xy^2 + y^3 = n$$

*has a solution in integers $x, y$, then it has at least three such solutions. Prove that the equation has no integer solution when $n = 2891$.*

(23rd IMO)

*Solution.* Completing the cube, we obtain

$$\begin{aligned} x^3 - 3xy^2 + y^3 &= 2x^3 - 3x^2y - x^3 + 3x^2y - 3xy^2 + y^3 \\ &= 2x^3 - 3x^2y + (y - x)^3 \\ &= (y - x)^3 - 3(y - x)(-x)^2 + (-x)^3. \end{aligned}$$

This shows that if $(x, y)$ is a solution, then so is $(y - x, -x)$. The two solutions are distinct, since $y - x = x$ and $-x = y$ lead to $x = y = 0$. Similarly,

$$\begin{aligned} x^3 - 3xy^2 + y^3 &= x^3 - 3x^2y + 3xy^2 - y^3 + 2y^3 + 3x^2y - 6xy^2 \\ &= (x - y)^3 + 3xy(x - y) - 3xy^2 + 2y^3 \\ &= (-y)^3 - 3(-y)(x - y)^2 + (x - y)^3, \end{aligned}$$

so $(-y, x - y)$ is the third solution to the equation.

We use these two transformations to solve the second part of the problem. Let $(x, y)$ be a solution. Since 2891 is not divisible by 3,

$x^3 + y^3$ is not divisible by 3 as well. So either both $x$ and $y$ give the same residue modulo 3 (different from 0), or exactly one of $x$ and $y$ is divisible by 3. Either of the two situations implies that one of the numbers $-x, y, x - y$ is divisible by 3, and using the above transformations, we may assume that $y$ is a multiple of 3. It follows that $x^3$ must be congruent to 2891 (mod 9), which is impossible, since 2891 has residue 2, and the only cubic residues modulo 9 are 0, 1, and 8.

**Example 6.** *Solve the equation*

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

(31st IMO, reformulated)

*Solution.* The only solutions are $(1, 3)$ and $(3, 1)$. Indeed, let $x = 3^k d$, with $\gcd(d, 3) = 1$. Clearly, $d$ is odd and $3^{2^k} d^2$ divides $2^{3^k d} + 1$. But

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

for all $k \geq 1$, hence

$$2^{d \cdot 3^k} + 1 = \left(2^d + 1\right) \prod_{j=0}^{k-1} \left(2^{2d \cdot 3^j} - 2^{d \cdot 3^j} + 1\right). \tag{1}$$

Because $2^{2m} - 2^m + 1 \equiv 3 \pmod 9$ for each odd $m$, it follows that

$$\prod_{j=0}^{k-1} \left(2^{2d \cdot 3^j} - 2^{d \cdot 3^j} + 1\right)$$

is divisible by $3^k$ but not by $3^{k+1}$.

Taking into account that $3^{2k} d^2 \mid 2^{d3^k} + 1$, from (1) we get $3^k \mid 2^d + 1$.

The case $d = 1$ yields $k = 1$, generating the solution $(3, 1)$.

Because $d$ is odd and $\gcd(d, 3) = 1$, we have $d \geq 5$ and $d$ is congruent to 1 or 5 (mod 6).

If $d \equiv 1 \pmod 6$, then $2^d + 1 \equiv 3 \pmod 9$, and if $d \equiv 5 \pmod 6$, then $2^d + 1 \equiv 6 \pmod 9$. In both cases, 9 does not divide $2^d + 1$. It follows that $k = 0$ or $k = 1$. For $k = 0$ and $k = 1$, $d$ divides $2^x + 1$. Let $p$ be the least prime factor of $d$. From $p \mid 2^x + 1$ it follows that $2^x \equiv -1 \pmod p$. But from Fermat's little theorem, $2^{p-1} \equiv 1 \pmod p$. Let $u$ be the order of 2 modulo $p$, that is, the least positive integer $u$ such that $2^u \equiv 1 \pmod p$. From the minimality of $u$ it follows that $u \mid p - 1$. But from $2^x \equiv -1 \pmod p$ we have $2^{2x} \equiv 1 \pmod p$, and hence $u \mid 2x$. Because $\gcd(p - 1, d) = 1$, we get $\gcd(u, d) = 1$, and $u \mid 2 \cdot 3^k \cdot d$ with $k = 0$ or $k = 1$ yields $u \in \{1, 2, 3, 6\}$. Taking into account that $2^u \equiv 1 \pmod p$, it follows that $p$ divides one of the numbers 1, 3, 7, and 63. But $p$ is a prime greater than or equal to 5, and hence $p = 7$. However, 7 does not divide $2^x + 1$, since $2^x + 1 \equiv 2, 3, \text{ or } 5 \pmod 7$.

Hence there is no prime $p$ that divides $d$ and $2^x + 1$, and thus $d = 1$ and $x = 3$.

## Exercises and Problems

**1.** Prove that the equation

$$(x + 1)^2 + (x + 2)^2 + \cdots + (x + 99)^2 = y^z$$

is not solvable in integers $x, y, z$, with $z > 1$.

(Hungarian Mathematical Olympiad)

**2.** Find all pairs $(x, y)$ of positive integers for which

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

(Titu Andreescu)

**3.** Prove that the equation

$$x^3 + y^4 = 7$$

has no solution in integers.

**4.** Find all pairs $(x, y)$ of positive integers satisfying the equation

$$3^x - 2^y = 7.$$

**5.** Determine all nonnegative integral solutions $(x_1, x_2, \ldots, x_{14})$ if any, apart from permutations, to the Diophantine equation

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

(8th USA Mathematical Olympiad)

**6.** Find all pairs $(x, y)$ of integers such that

$$x^3 - 4xy + y^3 = -1.$$

(G.M. Bucharest)

**7.** Find all triples $(x, y, z)$ of nonnegative integers such that

$$5^x 7^y + 4 = 3^z.$$

(Bulgarian Mathematical Olympiad)

**8.** Prove that the equation

$$4xy - x - y = z^2$$

has no solution in positive integers.

(Euler)

**9.** Prove that the system of equations

$$\begin{cases} x^2 + 6y^2 = z^2, \\ 6x^2 + y^2 = t^2, \end{cases}$$

has no nontrivial integer solutions.

**10.** Find all pairs $(a, b)$ of positive integers that satisfy the equation

$$a^{b^2} = b^a.$$

(37th IMO)

**11.** Find all primes $q_1, q_2, \ldots, q_6$ such that

$$q_1^2 = q_2^2 + \cdots + q_6^2.$$

(Titu Andreescu)

**12.** Prove that there are unique positive integers $a$ and $n$ such that

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

(Putnam Mathematical Competition)

## 1.5 The Method of Mathematical Induction

Mathematical induction is a powerful and elegant method for proving statements depending on nonnegative integers.

Let $(P(n))_{n\geq 0}$ be a sequence of propositions. The method of mathematical induction assists us in proving that $P(n)$ is true for all $n \geq n_0$, where $n_0$ is a given nonnegative integer.

**Mathematical Induction** (weak form): *Suppose that:*

- $P(n_0)$ *is true;*
- *For all* $k \geq n_0$, $P(k)$ *is true implies* $P(k+1)$ *is true.*

*Then* $P(n)$ *is true for all* $n \geq n_0$.

**Mathematical Induction** (with step $s$): *Let* $s$ *be a fixed positive integer. Suppose that:*

- $P(n_0), P(n_0+1), \ldots, P(n_0+s-1)$ *are true;*
- *For all* $k \geq n_0$, $P(k)$ *is true implies* $P(k+s)$ *is true.*

*Then* $P(n)$ *is true for all* $n \geq n_0$.

**Mathematical Induction** (strong form): *Suppose that*

- $P(n_0)$ *is true;*
- *For all* $k \geq n_0$, $P(m)$ *is true for all* $m$ *with* $n_0 \leq m \leq k$ *implies* $P(k+1)$ *is true.*

*Then* $P(n)$ *is true for all* $n \geq n_0$.

This method of proof is widely used in various areas of mathematics, including number theory. The following examples are meant

to show how mathematical induction works in studying Diophantine equations.

**Example 1.** *Prove that for all integers $n \geq 3$, there exist odd positive integers $x, y$, such that $7x^2 + y^2 = 2^n$.*

(Bulgarian Mathematical Olympiad)

*Solution.* We will prove that there exist odd positive integers $x_n, y_n$ such that $7x_n^2 + y_n^2 = 2^n$, $n \geq 3$.

For $n = 3$, we have $x_3 = y_3 = 1$. Now suppose that for a given integer $n \geq 3$ we have odd integers $x_n, y_n$ satisfying $7x_n^2 + y_n^2 = 2^n$. We shall exhibit a pair $(x_{n+1}, y_{n+1})$ of odd positive integers such that $7x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$. In fact,

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

Precisely one of the numbers $\frac{x_n+y_n}{2}$ and $\frac{|x_n-y_n|}{2}$ is odd (since their sum is the larger of $x_n$ and $y_n$, which is odd). If, for example, $\frac{x_n+y_n}{2}$ is odd, then

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

is also odd (as a sum of an odd and an even number); hence in this case we may choose

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

If $\frac{x_n-y_n}{2}$ is odd, then

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

so we can choose

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

**Example 2.** *Prove that for all positive integers $n$, the equation*

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

*is solvable in positive integers.*

(Dorin Andrica)

*Solution.* We use mathematical induction with pace $s = 2$ and $n_0 = 1$. Note that for $(x_1, y_1, z_1) = (1, 3, 7)$ and $(x_2, y_2, z_2) = (14, 39, 42)$ we have

$$x_1^2 + y_1^2 + z_1^2 = 59 \qquad \text{and} \qquad x_2^2 + y_2^2 + z_2^2 = 59^2.$$

Define now $(x_n, y_n, z_n)$, $n \geq 3$, by

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

for all $n \geq 1$. Then

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^2(x_k^2 + y_k^2 + z_k^2);$$

hence $x_k^2 + y_k^2 + z_k^2 = 59^k$ implies $x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^{k+2}$.

**Remark.** We can write the solutions as

$$(x_{2n-1}, y_{2n-1}, z_{2n-1}) = (1 \cdot 59^{n-1}, 3 \cdot 59^{n-1}, 7 \cdot 59^{n-1})$$

and

$$(x_{2n}, y_{2n}, z_{2n}) = (14 \cdot 59^n, 39 \cdot 59^n, 42 \cdot 59^n), \quad n \geq 1.$$

**Example 3.** *Prove that for all $n \geq 3$ the equation*

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1 \tag{1}$$

*is solvable in distinct positive integers.*

*Solution.* For the base case $n = 3$ we have

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1.$$

Assuming that for some $k \geq 3$,

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = 1,$$

where $x_1, x_2, \ldots, x_k$ are distinct positive integers, we obtain

$$\frac{1}{2x_1} + \frac{1}{2x_2} + \cdots + \frac{1}{2x_k} = \frac{1}{2}.$$

It follows that

$$\frac{1}{2} + \frac{1}{2x_1} + \frac{1}{2x_2} + \cdots + \frac{1}{2x_k} = 1,$$

where $2, 2x_1, 2x_2, \ldots, 2x_k$ are distinct.

**Remarks.** (1) Note that

$$\sum_{k=1}^{n-1} \frac{k}{(k+1)!} = \sum_{k=1}^{n-1} \frac{(k+1)-1}{(k+1)!} = \sum_{k=1}^{n-1} \left( \frac{1}{k!} - \frac{1}{(k+1)!} \right) = 1 - \frac{1}{n!}.$$

Hence

$$\frac{1}{\frac{2!}{1}} + \frac{1}{\frac{3!}{2}} + \cdots + \frac{1}{\frac{n!}{n-1}} + \frac{1}{n!} = 1$$

i.e., $\left( \frac{2!}{1}, \frac{3!}{2}, \ldots, \frac{n!}{n-1}, n! \right)$ is a solution to equation (1) and all its components are distinct.

(2) Another solution to equation (1) whose components are distinct is given by

$$\Big(2, 2^2, \ldots, 2^{n-2}, 2^{n-2}+1, 2^{n-2}\Big(2^{n-2}+1\Big)\Big).$$

Indeed,

$$\begin{aligned}
&\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{n-2}}+\frac{1}{2^{n-2}+1}+\frac{1}{2^{n-2}(2^{n-2}+1)}\\
&\quad=1-\frac{1}{2^{n-2}}+\frac{2^{n-2}}{2^{n-2}(2^{n-2}+1)}+\frac{1}{2^{n-2}(2^{n-2}+1)}\\
&\quad=1-\frac{1}{2^{n-2}}+\frac{1}{2^{n-2}}=1.
\end{aligned}$$

(3) Another way to construct solutions to equation (1) is to consider the sequence

$$a_1=2,\quad a_{m+1}=a_1\cdots a_m+1,\quad m\geq 1.$$

Then for all $n\geq 3$,

$$\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_{n-1}}+\frac{1}{a_n-1}=1. \tag{2}$$

Indeed, from the recurrence relation it follows that

$$a_{k+1}-1=a_k(a_k-1),\quad k\geq 1,$$

or

$$\frac{1}{a_{k+1}-1}=\frac{1}{a_k-1}-\frac{1}{a_k},\quad k\geq 1.$$

Thus

$$\frac{1}{a_k}=\frac{1}{a_k-1}-\frac{1}{a_{k+1}-1}$$

and the sum

$$\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_{n-1}}$$

telescopes to

$$\frac{1}{a_1-1}-\frac{1}{a_n-1}=1-\frac{1}{a_n-1}.$$

Hence the relation (2) is verified.

(4) If $(s_1, s_2, \ldots, s_n)$ is a solution to

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1$$

with $s_1 < s_2 < \cdots < s_n$, then $(s_1, s_2, \ldots, s_{n-1}, s_n + 1, s_n(s_n + 1))$ is a solution to

$$\frac{1}{y_1} + \frac{1}{y_2} + \cdots + \frac{1}{y_{n+1}} = 1$$

and all its components are distinct.

(5) For $a > 1$, the identity

$$\frac{1}{a-1} = \frac{1}{a} + \frac{1}{a^2} + \cdots + \frac{1}{a^m} + \frac{1}{(a-1)a^m}$$

generates various other families of solutions. For example, from

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$$

and $a = 7$, we obtain the solution $\left(2, 3, 7, 7^2, \ldots, 7^{n-3}, 6 \cdot 7^{n-3}\right)$, $n \geq 4$, while from

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{42} = 1$$

we get $\left(2, 3, 7, 43, 43^2, \ldots, 43^{n-4}, 42 \cdot 43^{n-4}\right)$, $n \geq 5$. From the construction above it follows that equation (1) has infinitely many families of solutions with distinct components.

(6) It is not known whether there are infinitely many positive integers $n$ for which equation (1) admits solutions $(x_1, x_2, \ldots, x_n)$, where $x_1, x_2, \ldots, x_n$ are all distinct odd positive integers.

A simple parity argument shows that in this case $n$ must be odd.

There are several known examples of such integers $n$. For instance, if $n = 9$, we have

$$\frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{15} + \frac{1}{33} + \frac{1}{45} + \frac{1}{385} = 1;$$

if $n = 11$,

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{15}+\frac{1}{21}+\frac{1}{27}+\frac{1}{35}+\frac{1}{63}+\frac{1}{105}+\frac{1}{135}=1;$$

if $n = 15$,

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{15}+\frac{1}{21}+\frac{1}{35}+\frac{1}{45}+\frac{1}{55}$$
$$+\frac{1}{77}+\frac{1}{165}+\frac{1}{231}+\frac{1}{385}+\frac{1}{495}+\frac{1}{693}=1;$$

and if $n = 17$,

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{15}+\frac{1}{21}+\frac{1}{35}+\frac{1}{45}+\frac{1}{55}$$
$$+\frac{1}{77}+\frac{1}{165}+\frac{1}{275}+\frac{1}{385}+\frac{1}{495}+\frac{1}{825}+\frac{1}{1925}+\frac{1}{2475}=1.$$

**Example 4.** *Prove that equation*

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

*is solvable in positive integers if and only if* $n \geq 3$.

(Mathematical Reflections)

*Solution.* For $n = 1$, the equation becomes

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

which has no solution, since $\sqrt{2}$ is irrational.

Consider next $n = 2$. Then the equation becomes

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

For $1 \leq i \leq 3$, write $x_i = 3^{n_i}y_i$, where $y_i$ is not divisible by 3. Without loss of generality assume that $n_1 \geq n_2$. Then

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

Because 1 is the only possible quadratic residue modulo 3,

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

Hence the exponents of 3 in the two sides of (3) cannot be equal.

Finally, consider $n \geq 3$. Starting from $5^2 = 4^2 + 3^2$, we get

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

by dividing by $3^2 4^2 5^2$. Multiplying by $\frac{1}{12^2}$, we get

$$\begin{aligned}\frac{1}{12^4} &= \frac{1}{12^2 15^2} + \frac{1}{12^2 20^2} = \frac{1}{12^2 15^2} + \left(\frac{1}{15^2} + \frac{1}{20^2}\right)\frac{1}{20^2} \\ &= \frac{1}{(12\cdot 15)^2} + \frac{1}{(15\cdot 20)^2} + \frac{1}{(20\cdot 20)^2}.\end{aligned}$$

Hence

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

is a solution for $n = 3$. Inductively, assume that $(x_1, \ldots, x_{n+1})$ is a solution to

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

for some $n \geq 3$ and arrive in this manner at

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

completing the proof.

**Remark.** For $n = 1$, we get the equation $\sqrt{2}x_1 = x_2$, and since $\sqrt{2}$ is irrational, there is no solution in this case. For $n = 2$, we have

$$x_2^2 x_3^2 + x_1^2 x_3^2 = 3x_1^2 x_2^2,$$

or equivalently, $a^2 + b^2 = 3c^2$. We can assume that the numbers $a$, $b$, and $c$ are all different from zero and that they are relatively prime,

meaning $\gcd(a, b, c) = 1$. The square of an integer is congruent to 0 or 1 modulo 3, and hence both $a$ and $b$ are divisible by 3. Now, $c$ is also divisible by 3 and we get a contradiction.

For $n = 3$, we have at least one solution:

$$(x_1, x_2, x_3, x_4) = (3, 3, 6, 4),$$

that is,

$$\frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{6^2} = \frac{4}{4^2}.$$

For each integer $n > 3$, we can use the solution for $n = 3$ and get

$$\frac{1}{3^2} + \frac{1}{3^3} + \frac{1}{6^2} + \underbrace{\frac{1}{4^2} + \cdots + \frac{1}{4^2}}_{n-3} = \frac{4}{4^2} + \frac{n-3}{4^2} = \frac{n+1}{4^2}.$$

**Example 5.** *Prove that for all $n \geq 412$ there are positive integers $x_1, \ldots, x_n$ such that*

$$\frac{1}{x_1^3} + \frac{1}{x_2^3} + \cdots + \frac{1}{x_n^3} = 1. \tag{1}$$

*Solution.* We have

$$\frac{1}{a^3} = \frac{1}{(2a)^3} + \cdots + \frac{1}{(2a)^3},$$

where the right-hand side consists of eight summands, so if the equation (1) is solvable in positive integers, then so is the equation

$$\frac{1}{x_1^3} + \frac{1}{x_2^3} + \cdots + \frac{1}{x_{n+7}^3} = 1.$$

Using the method of mathematical induction with pace 7, it suffices to prove the solvability of the equation (1) for $n =$

$412, 413, \ldots, 418$. The key idea is to construct a solution in each of the above cases from smaller ones modulo 7.

Observe that

$$\begin{aligned}
\frac{27}{3^3} &= 1 \text{ and } 27 \equiv 412 \pmod 7,\\
\frac{4}{2^3}+\frac{9}{3^3}+\frac{36}{6^3} &= 1 \text{ and } 4+9+36 = 49 \equiv 413 \pmod 7,\\
\frac{4}{2^3}+\frac{32}{4^3} &= 1 \text{ and } 4+32 = 36 \equiv 414 \pmod 7,\\
\frac{18}{3^3}+\frac{243}{9^3} &= 1 \text{ and } 18+243 = 261 \equiv 415 \pmod 7,\\
\frac{18}{3^3}+\frac{16}{4^3}+\frac{144}{12^3} &= 1 \text{ and } 18+16+144 = 178 \equiv 416 \pmod 7,\\
\frac{4}{2^3}+\frac{16}{4^3}+\frac{36}{6^3}+\frac{144}{12^3} &= 1 \text{ and } 4+16+36+144 = 200 \equiv 417 \pmod 7.
\end{aligned}$$

Finally,

$$\frac{4}{2^3}+\frac{9}{3^3}+\frac{81}{9^3}+\frac{324}{18^3} = 1 \text{ and } 4+9+81+324 = 418.$$

## Exercises and Problems

**1.** Prove that for all integers $n \geq 2$ there are odd integers $x, y$ such that $|x^2 - 17y^2| = 4^n$.

(Titu Andreescu)

**2.** Prove that for all positive integers $n$, the equation

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

is solvable in integers.

(Dorin Andrica)

**3.** Prove that for each positive integer $n$, the equation

$$(x^2 + y^2)(u^2 + v^2 + w^2) = 2009^n$$

is solvable in integers.

(Titu Andreescu)

**4.** The integer $t_k = \frac{k(k+1)}{2}$ is called the $k$th triangular number, $k \geq 1$. Prove that for all positive integers $n \geq 3$ the equation

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1$$

is solvable in triangular numbers.

**5.** Show that for all $n \geq 6$ the equation

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = 1$$

is solvable in integers.

**6.** Prove that for all $s \geq 2$ there exist positive integers $x_0$, $x_1, \ldots, x_s$ such that

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_s^2} = \frac{1}{x_0^2}$$

and $x_0 < x_1 < \cdots < x_s$.

**7.** Prove that for every positive integer $m$ and for all sufficiently large $s$, the equation

$$\frac{1}{x_1^m} + \frac{1}{x_2^m} + \cdots + \frac{1}{x_s^m} = 1$$

has at least one solution in positive integers $x_1, x_2, \ldots, x_s$.

**8.** Prove that for any nonnegative integer $k$ the equation

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

is solvable in positive integers $x, y, z$ with $x < y < z$.

(Titu Andreescu)

**9.** Prove that the equation

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

has infinitely many solutions in positive integers $x, y$.

**10.** Solve in distinct positive integers the equation

$$x_1^2 + x_2^2 + \cdots + x_{2002}^2 = 1335(x_1 + x_2 + \cdots + x_{2002}).$$

(Titu Andreescu)

## 1.6 Fermat's Method of Infinite Descent (FMID)

Pierre de Fermat (1601–1665) is famous for his contributions to mathematics even though he was considered only an amateur mathematician. Fermat received his degree in civil law at the University of Orleans before 1631 and served as a lawyer and then a councillor at Toulouse.

Fermat had an enormous impact on the world of mathematics through his discoveries and methods. He was one of the first mathematicians to use a method of proof called the "infinite descent."

Let $P$ be a property concerning the nonnegative integers and let $(P(n))_{n\geq 1}$ be the sequence of propositions,

$$P(n)\text{: "}n\text{ satisfies property }P\text{."}$$

The following method is useful in proving that proposition $P(n)$ is false for all large enough $n$.

*Let $k$ be a nonnegative integer. Suppose that:*

- *$P(k)$ is not true;*

- *whenever $P(m)$ is true for a positive integer $m > k$, then there must be some smaller $j$, $m > j \geq k$, for which $P(j)$ is true.*

*Then $P(n)$ is false for all $n \geq k$.*

This is just the contrapositive of strong induction, applied to the negation of proposition $P(n)$. In the language of the ladder metaphor, if you know you can't reach any rung without first reaching a lower rung, and you also know you can't reach the bottom rung, then you cannot reach any rung.

The method described above is often called the *finite descent method*.

*Fermat's method of infinite descent* (FMID) can be formulated as follows:

*Let $k$ be a nonnegative integer. Suppose that:*

- *whenever $P(m)$ is true for an integer $m > k$, then there must be some smaller integer $j$, $m > j > k$, for which $P(j)$ is true.*

*Then $P(n)$ is false for all $n > k$.*

That is, if there were an $n$ for which $P(n)$ was true, one could construct a sequence $n > n_1 > n_2 > \cdots$ all of which would be greater than $k$ but for the nonnegative integers, no such infinite descending sequence exists.

Two special cases of FMID are particularly useful in the study of Diophantine equations.

**FMID Variant 1**: *There is no sequence of nonnegative integers $n_1 > n_2 > \cdots$.*

In some situations it is convenient to replace FMID Variant 1 by the following equivalent form: If $n_0$ is the smallest positive integer $n$ for which $P(n)$ is true, then $P(n)$ is false for all $n < n_0$.

**FMID Variant 2**: *If the sequence of nonnegative integers* $(n_i)_{i\geq 1}$ *satisfies the inequalities* $n_1 \geq n_2 \geq \cdots$, *then there exists* $i_0$ *such that* $n_{i_0} = n_{i_0+1} = \cdots$.

**Example 1.** *Solve in nonnegative integers the equation*

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

*Solution.* Note that $(0, 0, 0)$ is a solution. We will prove that there are no other solutions. Assume that $(x_1, y_1, z_1)$ is a nontrivial solution. Since $\sqrt[3]{2}$, $\sqrt[3]{4}$ are both irrational, it is not difficult to see that $x_1 > 0$, $y_1 > 0$, $z_1 > 0$.

From $x_1^3 + 2y_1^3 = 4z_1^3$ it follows that $2 \mid x_1$, so $x_1 = 2x_2$, $x_2 \in \mathbb{Z}_+$. Then $4x_2^3 + y_1^3 = 2z_1^3$, and hence $y_1 = 2y_2$, $y_2 \in \mathbb{Z}_+$. Similarly, $z_1 = 2z_2$, $z_2 \in \mathbb{Z}_+$. We obtain the "new" solution $(x_2, y_2, z_2)$ with $x_1 > x_2$, $y_1 > y_2$, $z_1 > z_2$. Continuing this procedure, we construct a sequence of positive integral solutions $(x_n, y_n, z_n)_{n\geq 1}$ such that $x_1 > x_2 > x_3 > \cdots$. But this contradicts FMID Variant 1.

**Example 2.** *Solve in nonnegative integers the equation*

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

(Putnam Mathematical Competition, reformulated)

*Solution.* Note the solutions $(0, k)$, $k \in \mathbb{Z}_+$, and $(1, 1)$. We will prove that there are no other solutions by using FMID on the prime

factors of $x$. Let $p_1$ be a prime divisor of $x$ and let $q$ be the least positive integer such that $p_1 \mid 2^q - 1$. From Fermat's Little Theorem we have $p_1 \mid 2^{p_1-1} - 1$, and therefore $q \leq p_1 - 1 < p_1$.

Let us prove now that $q \mid x$. If it didn't, then $x = kq + r$, with $0 < r < q$, and

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

It follows that $p_1 \mid 2^r - 1$, which contradicts the minimality of $q$.

Thus $q \mid x$ and $1 < q < p_1$. Now let $p_2$ be a prime divisor of $q$. It is clear that $p_2$ is a divisor of $x$ and $p_2 < p_1$. Continuing this procedure, we construct an infinite decreasing sequence of prime divisors of $x$: $p_1 > p_2 > \cdots$, in contradiction to FMID Variant 1.

**Example 3.** *Find the maximal value of* $m^2 + n^2$ *if* $m$ *and* $n$ *are integers between* 1 *and* 1981 *satisfying* $\left(n^2 - mn - m^2\right)^2 = 1$.

(22nd IMO)

*Solution.* Note that $(m, n) = (1, 1)$ satisfies the relation $\left(n^2 - mn - m^2\right)^2 = 1$. Moreover, if $m = n$, then necessarily $m = n = 1$. Also, if a pair $(m, n)$ satisfies this relation and $0 < m < n$, then $m < n \leq 2m$, and by completing the square we get

$$\begin{aligned} (n^2 - mn - m^2)^2 &= ((n - m)^2 + mn - 2m^2)^2 \\ &= ((n - m)^2 + m(n - m) - m^2)^2 \\ &= (m^2 - m(n - m) - (n - m)^2)^2, \end{aligned}$$

which shows that $(n-m, m)$ satisfies the same relation and $0 < n - m \leq m$.

By FMID Variant 2, the transformation $(m, n) \mapsto (n-m, m)$ must terminate after finitely many steps, and it terminates only when $m = n = 1$. Hence all pairs of numbers satisfying the relation are obtained from $(1, 1)$ by applying the inverse transformation $(m, n) \mapsto (n, m+n)$ several times:

$$(1,1) \mapsto (2,1) \mapsto (3,2) \mapsto (5,3) \mapsto \cdots .$$

The components of all such pairs are Fibonacci numbers $F_n$, where the sequence $(F_n)_{n\geq 0}$ is defined by

$$F_0 = 0,\ F_1 = 1 \text{ and } F_{n+1} = F_n + F_{n-1},\ n \geq 1.$$

Therefore, all pairs consist of consecutive Fibonacci numbers. The largest Fibonacci number less than 1981 is $F_{16} = 1597$, so the answer to the problem is $F_{15}^2 + F_{16}^2 = 3524578$.

**Remark.** In the first step of the previous solution we have used the fact that if a Diophantine equation is quadratic in one variable and we have a solution, then we can always get a second solution by replacing the variable by the other root of the quadratic. This observation is a useful idea in many other problems.

**Example 4.** *Let $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ be two sequences defined recursively as follows:*

$$x_{n+2} = 3x_{n+1} - x_n, \quad x_0 = 1, \quad x_1 = 4,$$

$$y_{n+2} = 3y_{n+1} - y_n, \quad y_0 = 1, \quad y_1 = 2.$$

*1. Prove that $x_n^2 - 5y_n^2 = -4$ for all nonnegative integers $n$.*

2. *Suppose that $a, b$ are two positive integers such that $a^2 - 5b^2 = -4$. Prove that there exists a nonnegative integer $k$ such that $x_k = a$ and $y_k = b$.*

*(Vietnamese Mathematical Olympiad)*

*Solution.* We first prove by induction on $k$ that for $k \geq 0$, we have

$$(x_{k+1}, y_{k+1}) = \left(\frac{3x_k + 5y_k}{2}, \frac{x_k + 3y_k}{2}\right).$$

For $k = 0$, $(4, 2) = \left(\frac{3+5}{2}, \frac{1+3}{2}\right)$, and for $k = 1$, $(11, 5) = \left(\frac{12+10}{2}, \frac{4+6}{2}\right)$.

Next, assume that our formula for $(x_{k+1}, y_{k+1})$ is true for $k$ and $k+1$. Substituting the expressions for $x_{k+2}, x_{k+1}, y_{k+2}, y_{k+1}$ into $(x_{k+3}, y_{k+3}) = (3x_{k+2} - x_{k+1}, 3y_{k+2} - y_{k+1})$, we find that $(x_{k+3}, y_{k+3})$ equals

$$\left(\frac{3}{2}(3x_{k+1} - x_k) + \frac{5}{2}(3y_{k+1} - y_k), \frac{1}{2}(3x_{k+1} - x_k) + \frac{3}{2}(3y_{k+1} - y_k)\right)$$
$$= \left(\frac{1}{2}(3x_{k+2} + 5y_{k+2}), \frac{1}{2}(x_{k+2} + 3y_{k+2})\right).$$

This completes the induction step and the proof of our claim.

**Remark.** We remark that by linearity, $x_{k+1} - (3x_k + 5y_k)/2$ and $y_{k+1} - (x_k + 3y_k)/2$ both satisfy the recurrence $a_{n+2} = 3a_{n+1} - a_n$ and both have $a_0 = a_1 = 0$; hence they are forever zero.

(1) We prove that $x_n^2 - 5y_n^2 = -4$ by induction on $n$. For $n = 0$ we have $1 - 5 + 4 = 0$. Now assume that the result is true for $n$. We prove that it is true for $n+1$. Indeed,

$$\begin{aligned} x_{n+1}^2 - 5y_{n+1}^2 &= \left(\frac{3x_n + 5y_n}{2}\right)^2 - 5\left(\frac{x_n + 3y_n}{2}\right)^2 \\ &= \frac{4x_n^2 - 20y_n^2}{4} = x_n^2 - 5y_n^2 = -4, \end{aligned}$$

as desired.

**Remark.** The sequences $(x_n)_{n\geq 0}$, $(y_n)_{n\geq 0}$ are defined by second-order linear recurrences; hence their general terms have the form

$$\alpha\left(\frac{3+\sqrt{5}}{2}\right)^n+\beta\left(\frac{3-\sqrt{5}}{2}\right)^n, \quad n\geq 0$$

For the first sequence we have $\alpha=\frac{1+\sqrt{5}}{2}$, $\beta=\frac{1-\sqrt{5}}{2}$, and for the second, $\alpha=\frac{1+\sqrt{5}}{2\sqrt{5}}$, $\beta=-\frac{1-\sqrt{5}}{2\sqrt{5}}$.

We obtain

$$x_n=\left(\frac{1+\sqrt{5}}{2}\right)^{2n+1}+\left(\frac{1-\sqrt{5}}{2}\right)^{2n+1},$$
$$y_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{2n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{2n+1}\right].$$

Using these two relations it is not difficult to verify that $x_n^2-5y_n^2=-4$, $n\geq 0$.

Note that $x_n=L_{2n+1}$ and $y_n=F_{2n+1}$, where $(F_m)_{m\geq 1}$, $(L_m)_{m\geq 1}$ are the well-known Fibonacci and Lucas sequences.

(2) Suppose, by way of contradiction, that $a_1^2-5b_1^2=-4$ for integers $a_1,b_1>0$, and that there did not exist $k$ such that $(x_k,y_k)=(a_1,b_1)$.

Let $(a_2,b_2)=\left(\frac{3a_1-5b_1}{2},\frac{3b_1-a_1}{2}\right)$. We argue that $a_2$ and $b_2$ are positive integers. This is true if $a_1$ and $b_1$ are of the same parity, $a_1<3b_1$, and $3a_1<5b_1$. Note that $0=a_1^2-5b_1^2+4\equiv a_1-b_1 \pmod 2$. Next, $a_1^2=5b_1^2-4<9b_1^2$ implies $a_1<3b_1$. In addition, there are no counterexamples with $a_1=1$ or 2. Thus $a_1^2>5$ and $0=5a_1^2-25b_1^2+20<5a_1^2-25b_1^2+4a_1^2$, i.e., $3a_1>5b_1$.

Using the condition $a_1^2 - 5b_1^2 = -4$, some quick algebra shows that $a_2^2 - 5b_2^2 = -4$ as well. However,

$$a_2 + b_2 = \frac{3a_1 - 5b_1}{2} + \frac{3b_1 - a_1}{2} = a_1 - b_1 < a_1 + b_1$$

and $(a_2, b_2) \neq (x_j, y_j)$ for all $j \geq 0$. Continuing this process, we construct an infinite sequence of positive integers

$$a_1 + b_1 > a_2 + b_2 > a_3 + b_3 > \cdots,$$

in contradiction to FMID Variant 1.

**Example 5.** *Solve in positive integers the equation*

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

*Solution.* We will prove first that $z = 5$. Let $(x_1, y_1, z_1)$ be a solution with $z_1 \neq 5$. Then $x_1 \neq y_1$, for otherwise $x_1[x_1(z_1 - 2) - 2] = 1$, which is impossible if $z_1 \neq 5$.

We have

$$\begin{aligned} 0 &= x_1^2 + y_1^2 + x_1 + y_1 + 1 - x_1 y_1 z_1 \\ &= (y_1 z_1 - x_1 - 1)^2 + y_1^2 + (y_1 z_1 - x_1 - 1) + y_1 \\ &\quad + 1 - (y_1 z_1 - x_1 - 1) y_1 z_1; \end{aligned}$$

hence $(x_2, y_2, z_2) = (y_1 z_1 - x_1 - 1, y_1, z_1)$ is also a solution, since $x_1(y_1 z_1 - x_1 - 1) = y_1^2 + y_1 + 1 > 0$ implies $x_2 = y_1 z_1 - x_1 - 1 > 0$.

Note that if $x_1 > y_1$, then $x_1 \geq y_1 + 1$, and that

$$x_1^2 > y_1^2 + y_1 + 1 = x_1(y_1 z_1 - x_1 - 1) = x_1 x_2.$$

Hence $x_1 > x_2$. Continuing this construction, we obtain a sequence of positive integral solutions $(x_k, y_k, z_k)$ with $x_1 > x_2 > x_3 > \cdots$, in contradiction to FMID Variant 1.

This contradiction shows that the assumption $z \neq 5$ is false, so $z = 5$.

It is not difficult to see that both $x$ and $y$ are odd. Performing the substitutions

$$u = \frac{3x-1}{2}, \quad v = \frac{3y-1}{2}, \tag{1}$$

the equation becomes

$$u^2 - 5uv + v^2 = -3. \tag{2}$$

Clearly, $(u_0, v_0) = (1, 1)$ is a solution to (2). Let $(u_1, v_1)$ be another solution with $u_1 > v_1$. Then

$$v_1^2 + (5v_1 - u_1)^2 + 3 = 5v_1(5v_1 - u_1),$$

so $(u_2, v_2) = (v_1, 5v_1 - u_1)$ is also a solution to (2). From

$$(u_1 - v_1)(u_1 - 4v_1) = u_1^2 - 5u_1v_1 + 4v_1^2 = 3v_1^2 - 3 \geq 0,$$

it follows that $u_1 \geq 4v_1$; hence $v_2 = 5v_1 - u_1 \leq v_1$. Starting from $(u_1, v_1)$ we construct the solutions $(u_2, v_2), (u_3, v_3), \ldots$ with $v_1 \geq v_2 \geq v_3 \geq \cdots$. According to FMID Variant 2, it follows that $v_{k+1} = 5v_k - u_k$ and $u_{k+1} = v_k$, $k \geq 1$. Thus

$$u_k = v_{k-1}, \quad k \geq 1,$$
$$v_{k+1} = 5v_k - v_{k-1}, \quad v_0 = 1, \quad v_1 = 4.$$

The sequence $(v_n)_{n\geq 0}$ is defined by a second-order linear recurrence; hence its general term has the form

$$v_n = \alpha\left(\frac{5+\sqrt{21}}{2}\right)^n + \beta\left(\frac{5-\sqrt{21}}{2}\right)^n, \quad n \geq 0.$$

In this case we have $\alpha = \frac{3+\sqrt{21}}{2\sqrt{21}}$ and $\beta = -\frac{3-\sqrt{21}}{2\sqrt{21}}$, and therefore

$$u_n = \frac{1}{\sqrt{21}}\left[\frac{3+\sqrt{21}}{2}\left(\frac{5+\sqrt{21}}{2}\right)^{n-1} - \frac{3-\sqrt{21}}{2}\left(\frac{5-\sqrt{21}}{2}\right)^{n-1}\right], \quad (3)$$

$$v_n = \frac{1}{\sqrt{21}}\left[\frac{3+\sqrt{21}}{2}\left(\frac{5+\sqrt{21}}{2}\right)^{n} - \frac{3-\sqrt{21}}{2}\left(\frac{5-\sqrt{21}}{2}\right)^{n}\right], \quad n \geq 0.$$

Taking into account the relations (1), we obtain that all the solutions to the given equation are $\left(\frac{2u_n+1}{3}, \frac{2v_n+1}{3}, 5\right)$, $n \geq 0$, where $u_n, v_n$ are defined by (3).

## Exercises and Problems

**1.** Find all triples $(x, y, z)$ of positive integer solutions to the equation

$$x^3 + 3y^3 + 9z^3 - 3xyz = 0.$$

(Kürschák Mathematical Competition)

**2.** Find all integers $x, y, z$ satisfying

$$x^2 + y^2 + z^2 - 2xyz = 0.$$

(Korean Mathematical Olympiad)

**3.** Solve the following equation in integers $x, y, z, u$:

$$x^4 + y^4 + z^4 = 9u^4.$$

**4.** Solve the following equation in positive integers:

$$x^2 - y^2 = 2xyz.$$

**5.** Determine all integral solutions to the equation

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

(5th USA Mathematical Olympiad)

**6.** (a) Prove that if there is a triple $(x, y, z)$ of positive integers such that

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

then $z = 3$.

(b) Find all such triples.

**7.** Solve in positive integers $x, y, u, v$ the system of equations

$$\begin{cases} x^2 + 1 = uy, \\ y^2 + 1 = vx. \end{cases}$$

**8.** Find all triples $(x, y, z)$ of positive integers that are solutions to the system of equations

$$\begin{cases} 2x - 2y + z = 0, \\ 2x^3 - 2y^3 + z^3 + 3z = 0. \end{cases}$$

(Titu Andreescu)

**9.** Prove that there are infinitely many triples $(x, y, z)$ of positive integers such that

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

(College Mathematics Journal)

**10.** Find all pairs $(a, b)$ of positive integers such that $ab + a + b$ divides $a^2 + b^2 + 1$.

(Mathematics Magazine)

**11.** Let $a$ be a positive integer. The sequence $(x_n)_{n\geq 1}$ is defined by $x_1 = 1$, $x_2 = a$, and $x_{n+2} = ax_{n+1} + x_n$ for all $n \geq 1$. Prove that $(x, y)$ is a solution to the equation

$$|x^2 + axy - y^2| = 1$$

if and only if there exists an integer $k$ such that $(x, y) = (x_k, x_{k+1})$.

(Romanian Mathematical Olympiad)

**12.** Find all pairs $(m, n)$ of nonnegative integers such that

$$(m + n - 5)^2 = 9mn.$$

(42nd IMO USA Team Selection Test)

**13.** Let $x, y, z$ be positive integers such that $xy - z^2 = 1$. Prove that there are nonnegative integers $a, b, c, d$ such that

$$x = a^2 + b^2, \quad y = c^2 + d^2, \quad z = ac + bd.$$

(20th IMO Shortlist)

## 1.7 Miscellaneous Diophantine Equations

Many elementary Diophantine equations are not of the types described in the previous sections. In what follows we present a few examples of such equations.

**Example 1.** *Solve in positive integers the system of equations*

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

(Titu Andreescu)

*Solution.* The inequalities

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

cannot both be true, because adding them would yield a contradiction. So at least one of the inequalities $x^2 + 3y < (x+2)^2$ and $y^2 + 3x < (y+2)^2$ is true. Without loss of generality, assume that $x^2 + 3y < (x+2)^2$. Then $x^2 < x^2 + 3y < (x+2)^2$ implies $x^2 + 3y = (x+1)^2$ or, $3y = 2x + 1$. We obtain $x = 3k+1$, $y = 2k+1$ for some nonnegative integer $k$ and $y^2 + 3x = 4k^2 + 13k + 4$. For $k > 5$, $(2k+3)^2 < 4k^2 + 13k + 4 < (2k+4)^2$; hence $y^2 + 3x$ cannot be a perfect square. Thus we need only consider $k \in \{0, 1, 2, 3, 4\}$. Only $k = 0$ makes $y^2 + 3x$ a perfect square; hence the unique solution is

$$x = y = 1, \quad u = v = 2.$$

**Example 2.** *Solve the equation*

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

*in distinct positive integers* $x_1, x_2, \ldots, x_n$.

(Titu Andreescu)

*Solution.* Writing the equation in the form

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

yields $x_1 = 1$ and

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

Because $x_2 \neq x_1$, it follows that $x_2 = 2$ and that

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

We have $x_3 \neq x_2$ and $x_3 \neq x_1$; hence $x_3 = 3$. Continuing this procedure (which amounts to a "finite induction"), we obtain

$$x_1 = 1, \quad x_2 = 2, \ \ldots, \ x_{n-1} = n-1.$$

Finally, it follows that $(n-1)(x_n - (n-1)) = n-1$, i.e., $x_n = n$.

**Remark.** Substituting into the equation yields the identity

$$1 + 1 \cdot 1! + 2 \cdot 2! + \cdots + (n-1) \cdot (n-1)! = n!.$$

**Example 3.** *Solve in positive integers the equation*

$$7^x + x^4 + 47 = y^2.$$

*Solution.* If $x$ is odd, then $7^x + x^4 + 47 \equiv 3 \pmod 4$, and since there are no perfect squares of this form, there are no solutions in this case.

Suppose that $x = 2k$, for some positive integer $k$. For $k \geq 4$, we have

$$(7^k)^2 < 7^{2k} + (2k)^4 + 47 < (7^k + 1)^2.$$

Indeed, the left inequality is clear, and the right one is equivalent to $8k^4 + 23 < 7^k$, which can be justified using mathematical induction.

We need only consider $k \in \{1, 2, 3\}$. Only $k = 2$ yields a solution. Thus $x = 4$, $y = 52$ is the unique solution.

**Example 4.** *Let $M$ be the number of integral solutions to the equation*

$$x^2 - y^2 = z^3 - t^3$$

*with the property $0 \leq x, y, z, t \leq 10^6$, and let $N$ be the number of integral solutions to the equation*

$$x^2 - y^2 = z^3 - t^3 + 1$$

*that have the same property. Prove that $M > N$.*

(21st IMO Shortlist)

*Solution.* Write down the two equations in the form

$$x^2 + t^3 = y^2 + z^3, \quad x^2 + t^3 = y^2 + z^3 + 1,$$

and for each $k = 0, 1, 2, \ldots$, denote by $n_k$ the number of integral solutions of the equation $u^2 + v^3 = k$ with the property $0 \leq u, v \leq 10^6$. Clearly, $n_k = 0$ for all $k$ greater than $l = (10^6)^2 + (10^6)^3$. Now a key observation follows:

$$M = n_0^2 + n_1^2 + \cdots + n_l^2 \text{ and } N = n_0 n_1 + n_1 n_2 + \cdots + n_{l-1} n_l. \quad (1)$$

To prove, for example, the second of these equalities, note that to any integral solution to $x^2 + t^3 = y^2 + z^3 + 1$ with $0 \leq x, y, z, t \leq 10^6$ there corresponds a $k$ $(1 \leq k \leq l)$ such that

$$x^2 + t^3 = k, \quad y^2 + z^3 = k - 1. \quad (2)$$

And for any such $k$, the pairs $(x,t)$ and $(y,z)$ satisfying (2) can be chosen independently of one another in $n_k$ and $n_{k-1}$ ways, respectively. Hence for each $k = 1, 2, \ldots, l$ there are $n_{k-1}n_k$ solutions of $x^2 + t^3 = y^2 + z^3 + 1$ with $x^2 + t^3 = y^2 + z^3 + 1 = k$, which implies $N = n_0n_1 + n_1n_2 + \cdots + n_{l-1}n_l$. The proof of the first equality in (1) is essentially the same.

It is not difficult to deduce from (1) that $M > N$. Indeed, a little algebra shows that

$$M - N = \frac{1}{2}[n_0^2 + (n_0 - n_1)^2 + (n_1 - n_2)^2 + \cdots + (n_{l-1} - n_l)^2 + n_l^2] > 0,$$

since $n_0 \neq 0$ (in fact, $n_0 = 1$).

**Example 5.** *(a) Prove that there exist infinitely many triples $(x,y,z)$ of integers satisfying the equation*

$$x^3 + 2y^3 + 4z^3 - 6xyz = 1. \tag{1}$$

*(b) Determine, with proof, all of the integer solutions of (1).*

(USA Proposal for the 38th IMO)

*Solution.* (a) Let $s$ be the real cube root of 2 and $\omega = e^{2\pi i/3}$. Then (1) may be rewritten, by factoring the left side, as

$$\left(x + ys + zs^2\right)\left(x + ys\omega + zs^2\omega^2\right)\left(x + ys\omega^2 + zs^2\omega\right) = 1. \tag{2}$$

Let $(x_1, y_1, z_1) = (1, 1, 1)$, which clearly constitutes a solution of (1). Then it is also clear that the triple $(x_n, y_n, z_n)$ defined by

$$x_n + y_n s + z_n s^2 = \left(x_1 + y_1 s + z_1 s^2\right)^n$$

is also a solution of (1) for any $n \in \mathbb{Z}$ (and are such triples all distinct).

(b) The only solutions are those triples of the form $(x_n, y_n, z_n)$ or $(-x_n, -y_n, -z_n)$ for some $n \in \mathbb{Z}$. More precisely, we show that if $(x, y, z)$ is a solution of (1) with $x + ys + zs^2 > 0$, then $(x, y, z) = (x_n, y_n, z_n)$, where $n$ is the unique integer such that

$$(1 + s + s^2)^n \leq x + ys + zs^2 < (1 + s + s^2)^{n+1}.$$

Define the new solution $(u, v, w)$ by the relation

$$u + vs + ws^2 = (x + ys + zs^2)(1 + s + s^2)^{-n},$$

so that $1 \leq u + vs + ws^2 < 1 + s + s^2$.

We have

$$\begin{aligned} 1 &\geq \Big(u + vs + ws^2\Big)^{-1} \\ &= \Big(u + vs\omega + ws^2\omega^2\Big)\Big(u + vs\omega^2 + ws^2\omega\Big) \\ &= \Big(u^2 - 2vw\Big) + \Big(2w^2 - uv\Big)s + \Big(v^2 - uw\Big)s^2 \\ &= \frac{1}{2}\left[\Big(u - vs\Big)^2 + \Big(vs - ws^2\Big)^2 + \Big(ws^2 - u\Big)^2\right], \end{aligned}$$

and hence $|u - vs|, \Big|vs - ws^2\Big|, \Big|ws^2 - u\Big|$ are all less than or equal to $\sqrt{2}$.

If $w \geq 1$, then $u > ws^2 - \sqrt{2} > 0$ and $v > ws - s^{-1}\sqrt{2} > 0$, so $u + vs + ws^2 \geq 1 + s + s^2$, a contradiction. Similarly, assuming $w \leq -1$ yields $u + vs + ws^2 \leq -\Big(1 + s + s^2\Big)$, a contradiction. Hence $w = 0$, yielding the inequalities

$$|u - vs|, |vs|, |u| \leq \sqrt{2}.$$

The second and third conditions imply $-1 \leq u, v \leq 1$, which yields only the solutions $(u, v, w) = (1, 0, 0)$ or $(-1, 1, 0)$. The second

solution does not satisfy the first condition, so $(u, v, w) = (1, 0, 0)$ and

$$(x, y, z) = (x_n, y_n, z_n),$$

as desired.

## Exercises and Problems

**1.** Prove that the equation $6\Big(6a^2+3b^2+c^2\Big) = 5n^2$ has no solution in integers except $a = b = c = n = 0$.

(Asian Pacific Mathematical Olympiad)

**2.** Determine a positive constant $c$ such that the equation

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

has exactly three solutions $(x, y)$ in positive integers.

(United Kingdom Mathematical Olympiad)

**3.** Find all triples $(x, y, z)$ of positive integers such that $y$ is a prime number, $y$ and 3 do not divide $z$, and $x^3 - y^3 = z^2$.

(Bulgarian Mathematical Olympiad)

**4.** Determine all triples $(x, k, n)$ of positive integers such that

$$3^k - 1 = x^n.$$

(Italian Mathematical Olympiad)

**5.** For a positive integer $n$, prove that the number of integral solutions $(x, y)$ to the equation $x^2 + xy + y^2 = n$ is finite and a multiple of 6.

**6.** Find all positive integers $n$ such that there exist relatively prime positive integers $x$ and $y$ and an integer $k > 1$ satisfying the equation

$$x^k + y^k = 3^n.$$

(Russian Mathematical Olympiad)

**7.** Prove that for each prime $p$ the equation

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

has no integer solutions $(q, n)$ with $q, n > 1$.

(Italian Mathematical Olympiad)

**8.** Determine all pairs $(a, b)$ of integers for which the numbers $a^2 + 4b$ and $b^2 + 4a$ are both perfect squares.

(Asian Pacific Mathematical Olympiad)

**9.** A rectangular parallelepiped has integer dimensions. All of its faces are painted green. The parallelepiped is partitioned into unit cubes by planes parallel to its faces. Find all possible dimensions of the parallelepiped if the number of cubes without a green face is one-third of the total number of cubes.

(Bulgarian Mathematical Olympiad)

**10.** Find all integer positive solutions $(x, y, z, t)$ to the equation

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

such that $\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$.

(Romanian Mathematical Olympiad)

# I.2

# Some Classical Diophantine Equations

## 2.1 Linear Diophantine Equations

An equation of the form

$$a_1x_1 + \cdots + a_nx_n = c, \tag{2.1.1}$$

where $a_1, a_2, \ldots, a_n, b$ are fixed integers, is called a *linear Diophantine equation*. We assume that $n \geq 1$ and that coefficients $a_1, \ldots, a_n$ are all different from zero.

We begin with the case $n = 2$. The main result concerning linear Diophantine equations is the following (see also the lemma in Example 5 of Section 1.3).

**Theorem 2.1.1.** *Let $a, b, c$ be integers, $a$ and $b$ nonzero. Consider the linear Diophantine equation*

$$ax + by = c. \tag{2.1.2}$$

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, 67
DOI 10.1007/978-0-8176-4549-6_2, © Springer Science+Business Media, LLC 2010

1. *The equation (2.1.2) is solvable in integers if and only if* $d = \gcd(a, b)$ *divides* $c$.

2. *If* $(x, y) = (x_0, y_0)$ *is a particular solution to (2.1.2), then every integer solution is of the form*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \tag{2.1.3}$$

*where* $t$ *is an integer.*

3. *If* $c = \gcd(a, b)$ *and* $|a|$ *or* $|b|$ *is different from* 1*, then a particular solution* $(x, y) = (x_0, y_0)$ *to (2.1.3) can be found such that* $|x_0| < |b|$ *and* $|y_0| < |a|$.

*Proof.* 1. If $d$ does not divide $c$, then the equation is clearly not solvable. If $d$ divides $c$, then, dividing both sides of (2.1.2) by $\frac{d}{c}$, it suffices to prove that $d$ is a linear combination with integer coefficients of $a$ and $b$. For this we use the Euclidean algorithm.

Suppose $a = bq + r$ for integers $a, b, r$, and $q$. It is easy to see that every common divisor of $a$ and $b$ is a common divisor of $b$ and $r$, and conversely. Clearly, if $b \mid a$, then $\gcd(a, b) = b$. In general, we have $\gcd(a, b) = \gcd(b, r)$. These observations lead to a straightforward calculation of the gcd of two numbers. To be systematic, we write $a = r_{-1}$ and $b = r_0$ (assumed positive and $a \geq b$):

$$\begin{aligned}
r_{-1} &= r_0 q_0 + r_1, && 0 \leq r_1 < r_0,\\
r_0 &= r_1 q_1 + r_2, && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, && 0 \leq r_3 < r_2,\\
r_2 &= r_3 q_3 + r_4, && 0 \leq r_4 < r_3,\\
&\vdots
\end{aligned}$$

This division process eventually terminates, since the remainders get smaller and smaller,

$$r_{-1} > r_0 > r_1 > r_2 > \cdots,$$

and yet remain nonnegative. In other words, some $r_n$ divides the preceding $r_{n-1}$ (and leaves a remainder $r_{n+1} = 0$).

We obtain

$$\begin{aligned} &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \quad 0 \le r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

From these,

$$r_n = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(r_{-1}, r_0) = \gcd(a, b).$$

The above calculation of $\gcd(a, b)$ can be retraced to give $\gcd(a, b)$ as an integer combination of $a$ and $b$.

Define the integers $x_k$ and $y_k$ recursively by

$$\begin{aligned} x_k &= x_{k-2} - q_{k-1}x_{k-1}, & x_{-1} &= 1, \quad x_0 = 0, \\ y_k &= y_{k-2} - q_{k-1}y_{k-1}, & y_{-1} &= 0, \quad y_0 = 1. \end{aligned}$$

In each of these steps, $r_k = ax_k + by_k$. In particular,

$$\gcd(a, b) = r_n = ax_n + by_n.$$

It can be checked that $(x_i)$ and $(y_i)$ alternate in sign, $|x_{n+1}| = b/\gcd(a, b)$, and $|y_{n+1}| = a/\gcd(a, b)$. It follows that $|x_n| < b$ and $|y_n| < a$ unless $n = 0$ and $q_0 = 1$, that is, unless $a = b = 1$.

2. We have

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 = c.$$

3. The result has already been proven in part 1. □

The central result concerning the general linear Diophantine equation (2.1.1) is the following:

**Theorem 2.1.2.** *The equation (2.1.1) is solvable if and only if*

$$\gcd(a_1, \ldots, a_n) \mid c.$$

*In case of solvability, one can choose $n-1$ solutions such that each solution is an integer linear combination of those $n-1$ solutions.*

*Proof.* Let $d = \gcd(a_1, \ldots, a_n)$. If $c$ is not divisible by $d$, then (2.1.1) is not solvable, since for any integers $x_1, \ldots, x_n$, the left-hand side of (2.1.1) is divisible by $d$ and the right-hand side is not.

Actually, we need to prove that $\gcd(x_1, x_2, \ldots, x_n)$ is a linear combination with integer coefficients of $x_1, x_2, \ldots, x_n$. For $n = 2$ this follows from Theorem 2.1.1. Because

$$\gcd(x_1, \ldots, x_n) = \gcd(\gcd(x_1, \ldots, x_{n-1}), x_n),$$

$\gcd(x_1, \ldots, x_n)$ is a linear combination of $x_n$ and $\gcd(x_1, \ldots, x_{n-1})$. Then inductively $\gcd(x_1, \ldots, x_n)$ is a linear combination of $x_1, \ldots, x_{n-1}, x_n$. □

**Example 1.** *Solve the equation*

$$3x + 4y + 5z = 6.$$

*Solution.* Working modulo 5 we have $3x + 4y \equiv 1 \pmod 5$, and hence

$$3x + 4y = 1 + 5s, \quad s \in \mathbb{Z}.$$

A solution to this equation is $x = -1 + 3s$, $y = 1 - s$. Applying (2.1.3), we obtain $x = -1 + 3s + 4t$, $y = 1 - s - 3t$, $t \in \mathbb{Z}$, and substituting back into the original equation yields $z = 1 - s$. Hence all solutions are

$$(x, y, z) = (-1 + 3s + 4t, 1 - s - 3t, 1 - s), \quad s, t \in \mathbb{Z}.$$

For any positive integers $a_1, \ldots, a_n$ with $\gcd(a_1, \ldots, a_n) = 1$, define $g(a_1, \ldots, a_n)$ to be the greatest positive integer $N$ for which the equation

$$a_1 x_1 + \cdots + a_n x_n = N$$

is not solvable in nonnegative integers. The problem of determining $g(a_1, \ldots, a_n)$ is known as the *Frobenius coin problem* (it was he who posed the problem of finding the largest amount of money that cannot be paid using coins worth $a_1, \ldots, a_n$ cents).

**Example 2.** (Sylvester, 1884) *Let $a$ and $b$ be positive integers with* $\gcd(a, b) = 1$. *Then*

$$g(a, b) = ab - a - b.$$

*Solution.* Suppose that $N > ab - a - b$. From (2.1.3) it follows that the solutions to the equation $ax + by = N$ are of the form $(x, y) = (x_0 + bt, y_0 - at)$, $t \in \mathbb{Z}$. Let $t$ be an integer such that $0 \le y_0 - at \le a - 1$. Then

$$(x_0 + bt)a = N - (y_0 - at)b > ab - a - b - (a - 1)b = -a,$$

which implies $x_0 + bt > -1$, i.e., $x_0 + bt \geq 0$. It follows that in this case the equation $ax + by = N$ is solvable in nonnegative integers. Thus

$$g(a, b) \leq ab - a - b.$$

Now we need only to show that the equation

$$ax + by = ab - a - b$$

is not solvable in nonnegative integers. Otherwise, we have

$$ab = a(x + 1) + b(y + 1).$$

Since $\gcd(a, b) = 1$, we see that $a \mid (y + 1)$ and $b \mid (x + 1)$, which implies $y + 1 \geq a$ and $x + 1 \geq b$. Hence

$$ab = a(x + 1) + b(y + 1) \geq 2ab,$$

and this contradiction shows that

$$g(a, b) \geq ab - a - b.$$

Therefore $g(a, b) = ab - a - b$.

**Remarks.** (1) The case $n = 3$ was first solved explicitly by Selmer and Beyer, using a continued fraction algorithm. Their result was simplified by Rödseth and later by Greenberg.

(2) No general formulas are known for $n \geq 4$. However, some upper bounds have been proven. In 1942, Brauer showed that

$$g(a_1, \ldots, a_n) \leq \sum_{i=1}^{n} a_i \left( \frac{d_{i-1}}{d_i} - 1 \right),$$

where $d_i = \gcd(a_1, \ldots, a_i)$. Erdős and Graham (1972) showed that

$$g(a_1, \ldots, a_n) \leq 2a_{n-1} \left[ \frac{a_n}{n} \right] - a_n,$$

and that

$$\frac{t^2}{n-1} - 5t \le \gamma(n,t) \le \frac{2t^2}{n},$$

where

$$\gamma(n,t) = \max_{0<a_1<\cdots<a_n\le t} g(a_1,\dots,a_n).$$

Suppose that the equation

$$a_1x_1 + \cdots + a_mx_m = n,$$

where $a_1,\dots,a_m > 0$, is solvable in nonnegative integers, and let $A_n$ be the number of its solutions $(x_1,\dots,x_m)$.

**Theorem 2.1.3.** *(1) The generating function of the sequence* $(A_n)_{n\ge1}$ *is*

$$f(x) = \frac{1}{(1-x^{a_1})\dots(1-x^{a_m})}, \quad |x|<1, \tag{2.1.6}$$

*that is,* $A_n$ *is equal to the coefficient of* $x^n$ *in the power series expansion of* $f$*.*

*(2) The following equality holds:*

$$A_n = \frac{1}{n!}f^{(n)}(0). \tag{2.1.7}$$

*Proof.* (1) Using a geometric series, we have

$$\frac{1}{1-x^{a_k}} = 1 + x^{a_k} + x^{2a_k} + \cdots, \quad k = 1,\dots,m;$$

hence

$$\begin{aligned} f(x) &= (1 + x^{a_1} + x^{2a_1} + \cdots)\cdots(1 + x^{a_m} + x^{2a_m} + \cdots) \\ &= 1 + A_1x + \cdots + A_nx^n + \cdots. \end{aligned}$$

(2) Passing to the $n$th derivative, we obtain formula (2.1.7). □

**Example 3.** *Find the number of pairs $(x, y)$ of nonnegative integers such that*

$$x + 2y = n.$$

*Solution.* From Theorem 2.1.3 it follows that the desired number is

$$A_n = \frac{1}{n!} f^{(n)}(0),$$

where

$$f(t) = \frac{1}{(1-t)(1-t^2)}.$$

We have

$$f(t) = \frac{1}{2} \cdot \frac{1}{(t-1)^2} - \frac{1}{4} \cdot \frac{1}{t-1} + \frac{1}{4} \cdot \frac{1}{t+1}$$

hence

$$f^{(n)}(t) = \frac{1}{2} \frac{(-1)^n (n+1)!}{(t-1)^{n+2}} - \frac{1}{4} \frac{(-1)^n n!}{(t-1)^{n+1}} + \frac{1}{4} \frac{(-1)^n n!}{(t+1)^{n+1}}.$$

Thus

$$f^{(n)}(0) = \frac{(n+1)!}{2} + \frac{n!}{4} + \frac{(-1)^n n!}{4}$$

and

$$A_n = \frac{1}{n!} f^{(n)}(0) = \frac{2n + 3 + (-1)^n}{4}.$$

## Exercises and Problems

**1.** Solve the equation

$$6x + 10y - 15z = 1.$$

**2.** Let $a, b, c$ be pairwise relatively prime positive integers. Show that $2abc-ab-bc-ca$ is the largest integer that cannot be expressed in the form $xbc + yca + zab$, where $x, y, z$ are nonnegative integers.

(24th IMO)

**3.** Find the number of triples $(x, y, z)$ of nonnegative integers such that

$$x + y + 2z = n.$$

**4.** Determine the positive integer $n$ such that the equation

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

has exactly 100 solutions $(x, y, z)$ in nonnegative integers.

**5.** Let $a, b, c, d$ be integers such that for all integers $m$ and $n$ there exist integers $x$ and $y$ for which $ax + by = m$ and $cx + dy = n$. Prove that $ad - bc = \pm 1$.

(Eötvös Mathematics Competition)

**6.** Let $n$ be an integer greater than 3 and let $X$ be a $3n^2$-element subset of $\{1, 2, \ldots, n^3\}$. Prove that there exist nine distinct numbers $a_1, a_2, \ldots, a_9$ in $X$ such that the system

$$\begin{cases} a_1x + a_2y + a_3z = 0, \\ a_4x + a_5y + a_6z = 0, \\ a_7x + a_8y + a_9z = 0, \end{cases}$$

is solvable in nonzero integers.

(Romanian Mathematical Olympiad)

**7.** Let

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1q}x_q = 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2q}x_q = 0, \\ \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pq}x_q = 0, \end{cases}$$

be a system of linear equations, where $q = 2p$ and $a_{ij} \in \{-1, 0, 1\}$. Prove that there exists a solution $(x_1, x_2, \ldots, x_q)$ of the system with the following properties:

(a) $x_j$ is an integer for every $j = 1, 2, \ldots, q$;

(b) there exist $j$ such that $x_j \neq 0$;

(c) $|x_j| \leq q$ for every $j = 1, 2, \ldots, q$.

(18th IMO)

## 2.2 Pythagorean Triples and Related Problems

One of the most celebrated Diophantine equations is the *Pythagorean equation*

$$x^2 + y^2 = z^2. \tag{2.2.1}$$

Studied in detail by Pythagoras in connection with the right triangles whose side lengths are all integers, this equation was known even to the ancient Babylonians.

Note first that if the triple of integers $(x_0, y_0, z_0)$ satisfies equation (2.2.1), then all triples of the form $(kx_0, ky_0, kz_0)$, $k \in \mathbb{Z}$, also satisfy (2.2.1). That is why it is sufficient to find solutions $(x, y, z)$ to (2.2.1) with $\gcd(x, y, z) = 1$. This is equivalent to the fact that $x, y, z$ are pairwise relatively prime.

A solution $(x_0, y_0, z_0)$ to (2.2.1) with $x_0, y_0, z_0$ pairwise relatively prime is called a *primitive solution*. It is clear that in a primitive solution exactly one of $x_0$ and $y_0$ is even.

**Theorem 2.2.1.** *Any primitive solution $(x, y, z)$ in positive integers to the equation (2.2.1) with $y$ even is of the form*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{2.2.2}$$

*where $m$ and $n$ are relatively prime positive integers such that $m > n$ and $m + n$ is odd.*

*Proof.* The integers $x$ and $y$ cannot both be odd, for otherwise

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4,$$

a contradiction. Hence exactly one of the integers $x$ and $y$ is even.

The identity

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

shows that the triple given by (2.2.2) is indeed a solution to the equation (2.2.1) and $y$ is even. Because $x$ must be odd, we may assume without loss of generality that $m$ is odd and $n$ is even.

Moreover, if $\gcd\Big(m^2 - n^2, 2mn, m^2 + n^2\Big) = d \geq 2$, then $d$ divides

$$2m^2 = \Big(m^2 + n^2\Big) + \Big(m^2 - n^2\Big)$$

and $d$ divides

$$2n^2 = \Big(m^2 + n^2\Big) - \Big(m^2 - n^2\Big).$$

Because $m$ and $n$ are relatively prime it follows that $d = 2$. Hence $m^2 + n^2$ is even, in contradiction to $m$ odd and $n$ even. It follows that $d = 1$, so the solution (2.2.2) is primitive.

Conversely, let $(x, y, z)$ be a primitive solution to (2.2.1) with $y = 2a$. Then $x$ and $z$ are odd, and consequently the integers $z + x$ and $z - x$ are even. Let $z + x = 2b$ and $z - x = 2c$. We may assume that $b$ and $c$ are relatively prime, for otherwise $z$ and $x$ would have a nontrivial common divisor. On the other hand, $4a^2 = y^2 = z^2 - x^2 = (z + x)(z - x) = 4bc$, i.e., $a^2 = bc$. Since $b$ and $c$ are relatively prime, it follows that $b = m^2$ and $c = n^2$ for some positive integers $m$ and $n$. We obtain that $m + n$ is odd and

$$x = b - c = m^2 - n^2, \quad y = 2mn, \quad z = b + c = m^2 + n^2. \qquad \square$$

A triple $(x, y, z)$ of the form (2.2.2) is called *primitive*. In order to list all primitive solutions to equation (2.2.1), we assign values $2, 3, 4, \ldots$ to $m$ and then for each of these values we take those integers $n$ that are relatively prime to $m$ and less than $m$.

Here is a table of the first 20 primitive solutions listed according to the above-mentioned rule. The last column refers to the area.

| $m$ | $n$ | $x$ | $y$ | $z$ | area |
|---|---|---|---|---|---|
| 2 | 1 | 3 | 4 | 5 | 6 |
| 3 | 2 | 5 | 12 | 13 | 30 |
| 4 | 1 | 15 | 8 | 17 | 60 |
| 4 | 3 | 7 | 24 | 25 | 84 |
| 5 | 2 | 21 | 20 | 29 | 210 |
| 5 | 4 | 9 | 40 | 41 | 180 |
| 6 | 1 | 35 | 12 | 37 | 210 |
| 6 | 5 | 11 | 60 | 61 | 330 |
| 7 | 2 | 45 | 28 | 53 | 630 |
| 7 | 4 | 33 | 56 | 65 | 924 |

| $m$ | $n$ | $x$ | $y$ | $z$ | area |
|---|---|---|---|---|---|
| 7 | 6 | 13 | 84 | 85 | 546 |
| 8 | 1 | 63 | 16 | 65 | 504 |
| 8 | 3 | 55 | 48 | 73 | 1320 |
| 8 | 5 | 39 | 80 | 89 | 1560 |
| 8 | 7 | 15 | 112 | 113 | 840 |
| 9 | 2 | 77 | 36 | 85 | 1386 |
| 9 | 4 | 65 | 72 | 97 | 2340 |
| 9 | 8 | 17 | 144 | 145 | 1224 |
| 10 | 1 | 99 | 20 | 101 | 990 |
| 10 | 3 | 91 | 60 | 109 | 2730 |

**Corollary 2.2.2.** *The general integral solution to (2.2.1) is given by*

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2), \tag{2.2.3}$$

*where* $k, m, n \in \mathbb{Z}$.

The immediate extension to equation (2.2.1) is

$$x^2 + y^2 + z^2 = t^2. \tag{2.2.4}$$

The positive solutions $(x, y, z, t)$ to (2.2.4) represent the dimensions and the length of the diagonal of a rectangular box. We want to find all situations in which these components are all integers.

**Theorem 2.2.3.** *All the solutions to equation (2.2.4) in positive integers* $x, y, z, t$ *with* $y, z$ *even are given by*

$$x = \frac{l^2 + m^2 - n^2}{n}, \quad y = 2l, \quad z = 2m, \quad t = \frac{l^2 + m^2 + n^2}{n}, \tag{2.2.5}$$

*where* $l, m$ *are arbitrary positive integers and* $n$ *is any divisor of* $l^2 + m^2$ *less than* $\sqrt{l^2 + m^2}$. *Every solution is obtained exactly once in this way.*

*Proof.* The identity

$$\left(\frac{l^2 + m^2 - n^2}{n}\right)^2 + (2l)^2 + (2m)^2 = \left(\frac{l^2 + m^2 + n^2}{n}\right)^2$$

shows that the quadruple in (2.2.5) is a solution to equation (2.2.4) and that $y$ and $z$ are even.

Conversely, note that at least two of the integers $x, y, z$ must be even; otherwise, $t^2 \equiv 2, 3 \pmod 4$, a contradiction. Suppose that $y = 2l$, $z = 2m$ for some positive integers $l$ and $m$. Setting $t - x = u$, we obtain

$$x^2 + 4l^2 + 4m^2 = (x + u)^2, \quad \text{or} \quad u^2 = 4(l^2 + m^2) - 2ux.$$

Therefore $u^2$ is even, so $u = 2n$ for some positive integer $n$. It follows that $x = \frac{l^2+m^2-n^2}{n}$ and $t = x + u = x + 2n = \frac{l^2+m^2+n^2}{n}$, where $l, m, n$ are positive integers and $n$ is a divisor of $l^2 + m^2$ less than $\sqrt{l^2 + m^2}$.

It is not difficult to see that every solution $(x, y, z, t)$ to (2.2.4) with $y$ and $z$ even is obtained exactly once from the formulas (2.2.5). Indeed, by (2.2.5) we have $l = \frac{y}{2}$, $m = \frac{z}{2}$, $n = \frac{t-x}{2}$; hence the integers $l, m, n$ are uniquely determined by $(x, y, z, t)$. □

Theorem 2.2.3 not only states the existence of the solutions to equation (2.2.4) but also gives a method for finding these solutions. It is not difficult to see that in order to eliminate the solutions with reversed unknowns we may reject the pairs $(l, m)$ with $l < m$ and consider only those $n$ for which $x$ is odd. Hence we eliminate also the solutions for which $x, y, z, t$ are all even.

Here are the first 10 solutions obtained in this way.

| $l$ | $m$ | $l^2 + m^2$ | $n$ | $x$ | $y$ | $z$ | $t$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 1 | 1 | 2 | 2 | 3 |
| 2 | 2 | 8 | 1 | 7 | 4 | 4 | 9 |
| 3 | 1 | 10 | 1 | 9 | 6 | 2 | 11 |
| 3 | 1 | 10 | 2 | 3 | 6 | 2 | 7 |
| 3 | 3 | 18 | 1 | 17 | 6 | 6 | 19 |
| 3 | 3 | 18 | 2 | 7 | 6 | 6 | 11 |
| 3 | 3 | 18 | 3 | 3 | 6 | 6 | 9 |
| 4 | 2 | 20 | 1 | 19 | 8 | 4 | 21 |
| 4 | 2 | 20 | 4 | 1 | 8 | 4 | 9 |
| 4 | 4 | 32 | 1 | 31 | 8 | 8 | 33 |

**Remarks.** (1) A well-known way to produce "Pythagorean quadruples" is

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

where $l, m, n$ are positive integers. It is also known that not all quadruples are generated in this way; for instance, $(3, 36, 8, 37)$ is excluded. On the other hand, this family of solutions is quite similar to the family of solutions to (2.2.1).

(2) The following formulas produce all Pythagorean quadruples of integers:

$$\begin{aligned} x &= m^2 + n^2 - p^2 - q^2, \\ y &= 2(mp + nq), \\ z &= 2(np - mq), \\ t &= m^2 + n^2 + p^2 + q^2, \end{aligned}$$

where $m, n, p, q$ are arbitrary integers. For a proof that uses Gaussian integers see Section 4.1.

(3) The equation

$$x_1^2 + x_2^2 + \cdots + x_k^2 = x_{k+1}^2 \tag{2.2.6}$$

is the natural extension of (2.2.1) and (2.2.4). From a geometrical point of view, the solutions $(x_1, x_2, \ldots, x_k, x_{k+1})$ represent the dimensions $x_1, x_2, \ldots, x_k$ of a cuboid in $\mathbb{R}^k$ and the length $x_{k+1}$ of its diagonal, respectively. All positive integer solutions $(x_1, x_2, \ldots, x_k, x_{k+1})$ with $\gcd(x_1, x_2, \ldots, x_k) = 1$ to the equation

(2.2.6) are given by

$$\begin{aligned} x_1 &= \frac{1}{q}\Big(m_1^2 + m_2^2 + \cdots + m_{k-1}^2 - m_k^2\Big), \\ x_2 &= \frac{2}{q} m_1 m_k, \\ &\vdots \\ x_k &= \frac{2}{q} m_{k-1} m_k, \\ x_{k+1} &= \frac{1}{q}\Big(m_1^2 + m_2^2 + \cdots + m_{k-1}^2 + m_k^2\Big). \end{aligned}$$

Here $m_1, m_2, \ldots, m_k$ are arbitrary integers and $q > 0$ is taken such that $\gcd(x_1, x_2, \ldots, x_k) = 1$.

(4) For $k = 5$, arguments involving spinors in physics produce Pythagorean hexads:

$$\begin{aligned} x_1 &= m^2 - n^2, \\ x_2 &= 2(n_0 m_1 - n_1 m_0 + m_3 n_2 - m_2 n_3), \\ x_3 &= 2(n_0 m_2 - n_2 m_0 + m_1 n_3 - m_3 n_1), \\ x_4 &= 2(n_0 m_3 - n_3 m_0 + m_2 n_1 - m_1 n_2), \\ x_5 &= 2mn, \\ x_6 &= m^2 + n^2, \end{aligned}$$

where $m, n, m_0, m_1, m_2, m_3, n_0, n_1, n_2, n_3$ are integers such that

$$mn = m_0 n_0 + m_1 n_1 + m_2 n_2 + m_3 n_3.$$

**Example 1.** *(the "negative" Pythagorean equation) Solve in positive integers the equation*

$$x^{-2} + y^{-2} = z^{-2}. \tag{2.2.7}$$

*Solution.* The equation is equivalent to

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

This means that $z \mid xy$ and that $x^2 + y^2$ is a perfect square. Then $x^2 + y^2 = t^2$ for some positive integer $t$, and the equation becomes

$$t = \frac{xy}{z}. \tag{2.2.8}$$

Let $d = \gcd(x, y, t)$. Then $x = ad$, $y = bd$, $t = cd$, where $a, b, c \in \mathbb{Z}_+$ with $\gcd(a, b, c) = 1$. Equation (2.2.8) reduces to

$$z = \frac{abd}{c}. \tag{2.2.9}$$

From the choice of $t$ it follows that

$$a^2 + b^2 = c^2; \tag{2.2.10}$$

hence $a, b, c$ are pairwise relatively prime. Then using (2.2.7), we deduce that $c \mid d$, i.e., $d = kc$, $k \in \mathbb{Z}_+$. We obtain

$$x = ad = kac, \quad y = bd = kbc, \quad t = cd = kc^2, \quad z = kab.$$

Taking into account (2.2.10) and the formulas (2.2.2), we have $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$, where the positive integers $m$ and $n$ satisfy the conditions in Theorem 2.2.1. The solutions to equation (2.2.7) are given by

$$x = k\Big(m^4 - n^4\Big), \quad y = 2kmn\Big(m^2 + n^2\Big), \quad z = 2kmn\Big(m^2 - n^2\Big),$$

where $k, m, n \in \mathbb{Z}_+$ and $m > n$.

**Remark.** If $a, b, c$ are positive integers satisfying

$$\frac{1}{a^2} + \frac{1}{b^2} = \frac{1}{c^2},$$

then $a^4 + b^4 + c^4$ is a perfect square. Indeed,

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

and

$$a^4 + b^4 + c^4 = a^4 + b^4 + c^4 + 2a^2b^2 - 2b^2c^2 - 2c^2a^2 = (a^2 + b^2 - c^2)^2.$$

**Example 2.** *Prove that there are no two positive integers such that the sum and the difference of their squares are also squares.*

*Solution.* The problem is equivalent to showing that the system of equations

$$\begin{cases} x^2 + y^2 = z^2, \\ x^2 - y^2 = w^2, \end{cases} \tag{2.2.11}$$

is not solvable in positive integers.

Assume, for the sake of contradiction, that (2.2.11) is solvable in positive integers and consider a pair $(x, y)$ such that $x^2 + y^2$ is minimal. It is clear that $\gcd(x, y) = 1$. Adding the equations of the system yields

$$2x^2 = z^2 + w^2; \tag{2.2.12}$$

hence $z$ and $w$ have the same parity. It follows that $z + w$ and $z - w$ are both even. Write (2.2.12) in the form

$$x^2 = \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2.$$

Moreover, $\gcd\left(x, \frac{z+w}{2}, \frac{z-w}{2}\right) = 1$. Indeed, if

$$\gcd\left(x, \frac{z+w}{2}, \frac{z-w}{2}\right) = d \geq 2,$$

then $d \mid x$ and $d \Big| \left(\frac{z+w}{2} + \frac{z-w}{2}\right) = z$. From the first equation in (2.2.11) we then obtain $d \mid y$, in contradiction to $\gcd(x, y) = 1$.

Applying Theorem 2.2.1, we get

$$\frac{z-w}{2} = m^2 - n^2, \quad \frac{z+w}{2} = 2mn,$$

or

$$\frac{z-w}{2} = 2mn, \quad \frac{z+w}{2} = m^2 - n^2.$$

Since $2y^2 = z^2 - w^2$, in either case we have

$$2y^2 = 2(m^2 - n^2) \cdot 4mn,$$

and hence

$$y^2 = 4mn(m^2 - n^2).$$

It follows that $y = 2k$, for some positive integer $k$, and that

$$k^2 = mn(m+n)(m-n). \tag{2.2.13}$$

Since $m$ and $n$ are relatively prime and $m+n$ is odd, the integers $m, n, m+n, m-n$ are also pairwise relatively prime; hence from (2.2.13) we deduce that $m = a^2$, $n = b^2$, $m+n = c^2$, and $m-n = d^2$, for some positive integers $a, b, c, d$. But $a^2+b^2 = c^2$ and $a^2-b^2 = d^2$, i.e., $(a, b, c, d)$ is also a solution to the system (2.2.11). Moreover,

$$a^2 + b^2 = m + n < 4mn(m^2 - n^2) = y^2 < x^2 + y^2,$$

in contradiction to the minimality of $x^2 + y^2$.

**Example 3.** *Solve the following equation in positive integers:*

$$x^2 + y^2 = 1997(x - y).$$

*Solution.* The solutions are

$$(x, y) = (170, 145) \quad \text{and} \quad (x, y) = (1827, 145).$$

We have

$$\begin{aligned} x^2 + y^2 &= 1997(x - y), \\ \Big(x + y\Big)^2 + \bigg(\Big(x - y\Big)^2 - 2 \cdot 1997(x - y)\bigg) &= 0 \\ \Big(x + y\Big)^2 + (1997 - x + y)^2 &= 1997^2. \end{aligned}$$

Since $x$ and $y$ are positive integers, $0 < x + y < 1997$ and $0 < 1997 - x + y < 1997$. Thus the problem reduces to solving $a^2 + b^2 = 1997^2$ in positive integers. Since 1997 is a prime, $\gcd(a, b) = 1$. By Pythagorean substitution, there are positive integers $m > n$ such that $\gcd(m, n) = 1$ and

$$1997 = m^2 + n^2, \quad a = 2mn, \quad b = m^2 - n^2.$$

Since $m^2, n^2 \equiv 0, 1, -1 \pmod 5$ and $1997 \equiv 2 \pmod 5$, $m, n = \pm 1 \pmod 5$. Since $m^2, n^2 \equiv 0, 1 \pmod 3$ and $1997 \equiv 2 \pmod 3$, $m, n \equiv \pm 1 \pmod 3$. Therefore $m, n \equiv 1, 4, 11, 14 \pmod{15}$. Since $m > n$, $1997/2 \le m^2 \le 1997$. Thus we need to consider only $m = 34, 41, 44$. The only solution is $(m, n) = (34, 29)$. Thus

$$(a, b) = (1972, 315),$$

which leads to our solution.

**Example 4.** *Find all quadruples $(x, y, z, w)$ such that*

$$x^2 + y^2 + z^2 + xy + yz + zx = 2w^2.$$

*Solution.* Write the equation as

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

From Theorem 2.2.3,

$$x+y=\frac{l^2+m^2-n^2}{n},\quad y+z=2l,\quad z+x=2m,$$
$$2w=\frac{l^2+m^2+n^2}{n},$$

where $n \mid l^2+m^2$. It follows that all desired quadruples are

$$x=m-l+\frac{l^2+m^2-n^2}{2n},\quad y=l-m+\frac{l^2+m^2-n^2}{2n},$$
$$z=l+m-\frac{l^2+m^2-n^2}{2n},\quad w=\frac{l^2+m^2+n^2}{2n},$$

where the positive integers $l,m,n$ are chosen such that $x,y,z$ are all positive and $2n \mid l^2+m^2+n^2$.

## Exercises and Problems

**1.** Prove that the system of equations

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

is not solvable in positive integers.

**2.** Let $m$ and $n$ be distinct positive integers. Show that none of the numbers $2(m^4+n^4)$, $m^4+6m^2n^2+n^4$ is a perfect square.

**3.** Prove that the equation

$$x^2y^2=z^2\Big(z^2-x^2-y^2\Big)$$

has no solution in positive integers.

**4.** Prove that the equation $x^2 + y^2 = \left(a^2 + b^2\right)z^2$, where $a$ and $b$ are nonzero given integers, has infinitely many solutions.

**5.** Find all quadruples $(x, y, z, w)$ of positive integers such that

$$xy + yz + zx = w^2.$$

**6.** Prove that there is no Pythagorean triangle whose area is a perfect square.

**7.** Prove that the number of primitive Pythagorean triangles with a given inradius $r$ is a power of 2 if $r$ is integer.

**8.** (a) Solve the equation $x^2 + y^2 + z^2 - xy - yz - zx = t^2$.

(b) Prove that the equation $u^2 + v^2 + w^2 = 2t^2$ has infinitely many solutions in positive integers.

(Titu Andreescu and Dorin Andrica)

## 2.3 Other Remarkable Equations

### 2.3.1. Some Quadratic Diophantine Equations and Related Problems

We begin by presenting a simple but useful equation that has numerous applications.

**Theorem 2.3.1.** *All integer solutions to the equation*

$$xy = zw$$

*are* $x = mn$, $y = pq$, $z = mp$, $w = nq$, *where* $m, n, p, q$ *are integers and* $\gcd(n, p) = 1$.

*Proof.* Write the equation as $\frac{x}{z} = \frac{w}{y}$ and denote by $\frac{n}{p}$ the corresponding irreducible fraction. Then set

$$m = \frac{x}{n} = \frac{z}{p} \quad \text{and} \quad q = \frac{y}{p} = \frac{w}{n}. \qquad \square$$

**Remarks.** (1) For all positive integers $x, y, z, w$ satisfying $xy = zw$, the integer $N = x + y + z + w$ is composite. Indeed,

$$xN = x^2 + xy + xz + xw = x^2 + zw + xz + xw = (x + z)(x + w)$$

and the conclusion follows.

(2) A special case is the equation $xy = z^2$. All integer solutions to this equation are $x = km^2$, $y = kn^2$, $z = kmn$, where $k, m, n$ are integers and $\gcd(m, n) = 1$.

**Example 1.** *If there are two distinct unordered pairs $(x, y)$ of positive integers satisfying the equation*

$$x^2 + y^2 = n,$$

*then $n$ is composite.*

*Solution.* Let $(a, b)$ and $(c, d)$ be two such solutions. Then $a \neq c$ and $a \neq d$. We may assume without loss of generality that $a > c$. Then

$$(a + c)(a - c) = (d + b)(d - b),$$

so there are positive integers $m, n, p, q$ such that

$$\gcd(n, p) = 1$$

and

$$a + c = mn, \quad a - c = pq, \quad d + b = mp, \quad d - b = nq.$$

Then

$$a = \frac{1}{2}(mn + pq), \quad b = \frac{1}{2}(nq - mp),$$

and

$$4n = 4(a^2 + b^2) = (mn + pq)^2 + (nq - mp)^2 = (m^2 + q^2)(n^2 + p^2).$$

Assume by way of contradiction that $n$ is a prime. Then without loss of generality, $m^2 + q^2 = 2$ or $m^2 + q^2 = 4$. In the first case $m = q = 1$, implying $a = d$, a contradiction. The second case is clearly impossible. Thus $n$ is composite.

**Remark.** All integer solutions to the equation

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

are

$$x = \frac{1}{2}(mn + pq), \quad y = \frac{1}{2}(mp - nq),$$

$$z = \frac{1}{2}(mp + nq), \quad w = \frac{1}{2}(mn - pq),$$

where $m, n, p, q$ are integers.

We continue this section by examining the Diophantine equation

$$x^2 + axy + y^2 = z^2, \tag{2.3.1}$$

where $a$ is a given integer. The Pythagorean equation is a special case of this equation ($a = 0$).

**Theorem 2.3.2.** *All integral solutions to (2.3.1) are given by*

$$\begin{cases} x = k(an^2 - 2mn), \\ y = k(m^2 - n^2), \\ z = \pm k(amn - m^2 - n^2), \end{cases} \qquad \begin{cases} x = k(m^2 - n^2), \\ y = k(an^2 - 2mn), \\ z = \pm k(amn - m^2 - n^2), \end{cases} \tag{2.3.2}$$

*where $m, n \in \mathbb{Z}$ are relatively prime and $k \in \mathbb{Q}$ such that $(a^2 - 4)$ $k \in \mathbb{Z}$.*

*Proof.* Note that the two families of solutions are given by the symmetry of (2.3.1) in $x$ and $y$.

It is not difficult to check that the triples $(x, y, z)$ in (2.3.2) satisfy equation (2.3.1).

Conversely, we need to show that all solutions to (2.3.1) are of the form (2.3.2). In this regard, note that equation (2.3.1) is equivalent to

$$x(x + ay) = (z - y)(z + y). \tag{2.3.3}$$

From Theorem 2.3.1 it follows that

$$x = np, \quad x + ay = mq, \quad z + y = nq, \quad z - y = mp,$$

for some integers $m, n, p, q$.

The result is clear in the case $y = z$, which corresponds to $x = 0$ or $x + ay = 0$. In all other cases (2.3.3) is equivalent to

$$\frac{x}{z - y} = \frac{z + y}{x + ay} = \frac{n}{m}$$

for some nonzero integers $m$ and $n$. The last relations lead to the homogeneous system

$$\begin{cases} mx + ny - nz = 0, \\ nx + (n - am)y - mz = 0, \end{cases}$$

whose solutions are

$$x = \frac{an^2 - 2mn}{amn - m^2 - n^2} z, \quad y = \frac{m^2 - n^2}{amn - m^2 - n^2} z.$$

We choose $z = k\Big(amn - m^2 - n^2\Big)$, where $k \in \mathbb{Q}$, and get the solutions (2.3.2). □

If $k = p/q$ in lowest terms, then

$$q \mid \gcd\Big(an^2 - 2mn, m^2 - n^2, amn - m^2 - n^2\Big),$$

and hence

$$q \mid a\Big(an^2 - 2mn\Big) + 2\Big(m^2 - n^2\Big) + 2\Big(amn - m^2 - n^2\Big) = \Big(a^2 - 4\Big)n^2.$$

Since any prime dividing $n$ cannot divide $m^2 - n^2$, it follows that $q \mid a^2 - 4$ or $\Big(a^2 - 4\Big)k \in \mathbb{Z}$.

**Remarks.** (1) Theorem 2.3.1 solves the third-degree Diophantine equation

$$x^2 + xyw + y^2 = z^2. \tag{2.3.4}$$

The general solution is $(x, y, z, w)$, where $w = a$, $a \in \mathbb{Z}$ and $x, y, z$ are given in (2.3.2).

(2) In a similar manner, we can prove that the equation

$$x^2 + axy + by^2 = z^2 \tag{2.3.5}$$

has infinitely many solutions, one family of which is

$$\begin{cases} x = k\Big(m^2 - bn^2\Big), \\ y = k\Big(an^2 - 2mn\Big), \\ z = \pm k\Big(amn - m^2 - bn^2\Big), \end{cases} \tag{2.3.6}$$

where $m, n \in \mathbb{Z}$ are relatively prime and $k \in \mathbb{Q}$ such that $(a^2 - 4b)k \in \mathbb{Z}$.

Generally, choosing $k \in \mathbb{Z}$ gives integer solutions, but not every integer solution corresponds to an integral $k$. For instance, for $a = 0$ and $b = -21$ the family (2.3.6) is

$$x = k\Big(m^2 + 21n^2\Big), \quad y = -2kmn, \quad z = k\Big(21n^2 - m^2\Big),$$

but the triple $(5, 1, 2)$ is not generated in this way. One reason is the following: equation (2.3.5) is equivalent to

$$(2x + ay)^2 - \Big(a^2 - 4b\Big)y^2 = (2z)^2,$$

and if $a^2-4b$ is not a perfect square, the ring $\mathbb{Z}\left[\sqrt{a^2-4b}\right]$ is not necessarily a unique factorization domain (see Section 4.1).

(3) Using the above remark we can construct an infinite family of solutions to the Diophantine equation

$$x^2+uxy+vy^2=z^2.$$

The solutions are $(x,y,z,u,v)$, where $u=a$, $v=b$, $a,b\in\mathbb{Z}$, and $x,y,z$ are given in (2.3.6).

(4) The solutions in positive integers to equation (2.3.1) can be expressed as follows:

$$\begin{cases} x=k\Big(2mn+an^2\Big), \\ y=k\Big(m^2-n^2\Big), \\ z=k\Big|m^2+amn+n^2\Big|, \end{cases} \qquad \begin{cases} x=k\Big(m^2-n^2\Big), \\ y=k\Big(2mn+an^2\Big), \\ z=k\Big|m^2+amn+n^2\Big| \end{cases} \tag{2.3.7}$$

where $m,n\in\mathbb{Z}_+^*$ are relatively prime, $k\in\mathbb{Q}_+^*$ such that $\Big(a^2-4\Big)k\in\mathbb{Z}$, $n>0$, $2m+an>0$, and $|m|>n$.

Aside from the case $a=0$, for which we obtain the Pythagorean equation, the following two cases are of particular interest:

**The case** $a=1$. Equation (2.3.1) becomes

$$x^2+xy+y^2=z^2. \tag{2.3.8}$$

From (2.3.7) it follows that its positive integer solutions are given by

$$\begin{cases} x=k\Big(2mn+n^2\Big), \\ y=k\Big(m^2-n^2\Big), \\ z=k\Big(m^2+mn+n^2\Big), \end{cases} \qquad \begin{cases} x=k\Big(m^2-n^2\Big), \\ y=k\Big(2mn+n^2\Big), \\ z=k\Big(m^2+mn+n^2\Big), \end{cases} \tag{2.3.9}$$

where $m, n \in \mathbb{Z}_+^*$, $m > n$, are relatively prime and $k \in \mathbb{Q}_+^*$ such that $3k \in \mathbb{Z}$.

The solutions (2.3.9) give all triples of positive integers $(x, y, z)$ that are the side lengths of a triangle whose opposite angle to $z$ is $120°$.

**The case** $a = -1$. Equation (2.3.1) becomes

$$x^2 - xy + y^2 = z^2. \tag{2.3.10}$$

Its positive integral solutions are given by

$$\begin{cases} x = k\Big(2mn - n^2\Big), \\ y = k\Big(m^2 - n^2\Big), \\ z = k\Big(m^2 - mn + n^2\Big), \end{cases} \qquad \begin{cases} x = k\Big(m^2 - n^2\Big), \\ y = k\Big(2mn - n^2\Big), \\ z = k\Big(m^2 - mn + n^2\Big), \end{cases} \tag{2.3.11}$$

where $m, n \in \mathbb{Z}_+^*$, $m > n$, are relatively prime and $k \in \mathbb{Q}_+^*$, such that $3k \in \mathbb{Z}$.

The solutions (2.3.11) characterize all triples of positive integers $(x, y, z)$ that are the side lengths of a triangle whose angle opposite the side of length $z$ is $60°$.

**Example 1.** *Find all triples* $(x, y, z)$ *of positive integers such that*

$$x^2 + xy + y^2 = 49^2.$$

*Solution.* From the general form of the solutions in (2.3.9), the problem reduces to finding all relatively prime positive integers $m, n$ with $m > n$, and $k \in \mathbb{Q}_+$ with $3k \in \mathbb{Z}$ such that

$$k\Big(m^2 + mn + n^2\Big) = 49.$$

In the following table we give all pairs $(m, n)$ satisfying the inequality $m^2 + mn + n^2 \leq 49$, where $m > n$.

| $m$ | $n$ | $m^2 + mn + n^2$ |
|---|---|---|
| 2 | 1 | 7 |
| 3 | 1 | 13 |
| 4 | 1 | 21 |
| 5 | 1 | 31 |
| 6 | 1 | 43 |
| 3 | 2 | 19 |
| 4 | 2 | 28 |
| 5 | 2 | 39 |
| 4 | 3 | 37 |
| 5 | 3 | 49 |

If $k = 1$, from the above table we can see that $m^2 + mn + n^2 = 49$ holds if and only if $m = 5$ and $n = 3$. In this case we obtain the solutions $(x, y) = (39, 16)$ and $(x, y) = (16, 39)$.

If $k = 7$ we obtain that $m^2 + mn + n^2 = 7$ if and only if $m = 2$ and $n = 1$, yielding the solutions $(x, y) = (35, 21)$ and $(x, y) = (21, 35)$.

The cases $k = \frac{1}{3}$ and $k = \frac{49}{3}$ give $m = n$, which is impossible. If $k = \frac{7}{3}$, then we get $m = 4$ and $n = 1$, giving solutions $(x, y) = (35, 21)$, $(21, 35)$.

It is natural to ask in what situations the solutions $(x, y)$ to equations (2.3.8) and (2.3.10) are perfect squares.

**Theorem 2.3.2.** *All nonnegative integral solutions to the equation*

$$x^4 + x^2y^2 + y^4 = z^2 \tag{2.3.12}$$

*are* $(x, y, z) = \left(k, 0, k^2\right)$, $(x, y, z) = \left(0, k, k^2\right)$, $k \in \mathbb{Z}_+$.

*Proof.* We may assume that $\gcd(x, y) = 1$. Then $x$ and $y$ have different parities, for otherwise $z^2 \equiv 3 \pmod 4$. Suppose that $y$ is odd and minimal. Write the equation in the equivalent form

$$4z^2 - \left(2x^2 + y^2\right)^2 = 3y^4, \tag{2.3.13}$$

or $\left(2z + 2x^2 + y^2\right)\left(2z - 2x^2 - y^2\right) = 3y^4$.

We claim that $\gcd\left(2z+2x^2+y^2, 2z-2x^2-y^2\right) = 1$. Indeed, assume that $d$ is a prime dividing both $2z+2x^2+y^2$ and $2z-2x^2-y^2$. Then $d$ is odd and $d$ divides both $z$ and $2x^2 + y^2$. From (2.3.13) it follows that $d \mid 3y$. If $d > 3$, then $d \mid y$ and $d \mid 2x^2$, i.e., $\gcd(x, y) \geq d$, a contradiction. If $d = 3$, it follows that $3 \mid z$, and from (2.3.12) we obtain $3 \mid (2x^2 + y^2)$, so $3 \mid y$. Therefore $3 \mid x$, and so $\gcd(x, y) \geq 3$, a contradiction.

Hence, either $2z + 2x^2 + y^2 = a^4$, $2z - 2x^2 - y^2 = 3b^4$, $y = ab$ or $2z + 2x^2 + y^2 = 3a^4$, $2z - 2x^2 - y^2 = b^4$, $y = ab$, where $a$ and $b$ are both odd positive integers.

In the first situation,

$$4x^2 = a^4 - 2a^2b^2 - 3b^4 \equiv -4 \pmod{16},$$

a contradiction.

In the second case,

$$4x^2 = 3a^4 - 2a^2b^2 - b^4 = \left(a^2 - b^2\right)\left(3a^2 + b^2\right).$$

Since $a$ and $b$ are both odd, it follows that $a^2 - b^2 = c^2$ and $3a^2 + b^2 = 4d^2$, for some positive integers $c$ and $d$. Then $a = p^2 + q^2$, $b = p^2 - q^2$, $p, q \in \mathbb{Z}_+$, and

$$p^4 + p^2q^2 + q^4 = d^2,$$

which contradicts the minimality of $y$.

Therefore $y = 1$, $a = b = 1$, and $x = 0$, yielding the solution $(0, 1, 1)$. Taking into account the symmetry in $x$ and $y$, we also have the solution $(1, 0, 1)$, and the conclusion follows. □

**Example 2.** *Solve in positive integers the system of equations*

$$\begin{cases} 3u^2 + v^2 = 4s^2, \\ u^2 + 3v^2 = 4t^2. \end{cases}$$

*Solution.* Setting $u = x+y$ and $v = x-y$, we obtain the equivalent system

$$\begin{cases} x^2 + xy + y^2 = s^2, \\ x^2 - xy + y^2 = t^2. \end{cases}$$

Multiplying the two equations gives

$$x^4 + x^2y^2 + y^4 = (st)^2.$$

From Theorem 2.3.2 it follows that

$$(x, y, st) = \left(k, 0, k^2\right) \quad \text{or} \quad (x, y, st) = \left(0, k, k^2\right),$$

yielding the solutions

$$(u, v, s, t) = (k, k, k, k), \quad k \in \mathbb{Z}_+.$$

**Theorem 2.3.3.** *All nonnegative integral solutions to the equation*

$$x^4 - x^2y^2 + y^4 = z^2 \tag{2.3.14}$$

*are* $(x, y, z) = \left(k, 0, k^2\right), \left(0, k, k^2\right), \left(k, k, k^2\right)$, $k \in \mathbb{Z}_+$.

*Proof.* We may assume that $\gcd(x, y) = 1$ and that $xy$ is minimal. Write the equation as

$$\left(x^2 - y^2\right)^2 + (xy)^2 = z^2.$$

Suppose first that $x$ and $y$ are not both odd. Then

$$x^2 - y^2 = a^2 - b^2, \quad xy = 2ab,$$

for some positive integers $a$ and $b$, with $\gcd(a, b) = 1$. Let $d_1 = \gcd(x, b)$ and $d_2 = \gcd(y, a)$. We have

$$x = d_1 X, \quad b = d_1 B, \quad y = d_2 Y, \quad a = d_2 A, \quad XY = 2AB.$$

Since $\gcd(X, B) = 1$ and $\gcd(Y, A) = 1$, it follows that

$$(X, Y) = (2A, B) \quad \text{or} \quad (X, Y) = (A, 2B).$$

Hence

$$x = 2d_1 A, \quad b = d_1 B, \quad y = d_2 B, \quad a = d_2 A$$

or

$$x = d_1 A, \quad b = d_1 B, \quad y = 2d_2 B, \quad a = d_2 A.$$

In the first case,

$$4d_1^2 A^2 - d_2^2 B^2 = d_2^2 A^2 - d_1^2 B^2,$$

i.e.,

$$d_1^2\Big(4A^2 + B^2\Big) = d_2^2\Big(A^2 + B^2\Big). \tag{2.3.15}$$

The condition $\gcd(a, b) = 1$ implies $\gcd(A, B) = 1$. Let $\gcd\Big(4A^2 + B^2, A^2 + B^2\Big) = D$. Then $D \mid \Big(4A^2 + B^2 - A^2 - B^2\Big) = 3A^2$, and since $A^2 + B^2 \not\equiv 0 \pmod 3$, it follows that $\gcd(D, 3) = 1$; hence $D \mid A^2$ and $D \mid \Big(A^2 + B^2 - A^2\Big) = B^2$. The condition $\gcd(A, B) = 1$ now implies $D = 1$, and from (2.3.15) we obtain

$$A^2 + B^2 = C^2 \quad \text{and} \quad 4S^2 + B^2 = D^2 \tag{2.3.16}$$

for some positive integers $C$ and $D$.

We may suppose that $B$ is odd, since if $B$ were even, we could set $B = 2B_1$ and have a similar pair of equations. Hence from the second Pythagorean equation in (2.3.16), $B = p^2 - q^2$, $A = pq$, and $p^4 - p^2q^2 + q^4 = C^2$. Also $pq \le a \le xy/2$, and so the method of descent applies, since $p$ and $q$ are not both odd. It follows that $xy = 0$, yielding the solutions $\left(k, 0, k^2\right)$, $\left(0, k, k^2\right)$, $k \in \mathbb{Z}_+$.

The other alternative gives

$$d_1^2A^2 - 4d_2^2B^2 = d_2^2A^2 - d_1^2B^2,$$

and so

$$d_1^2\left(A^2 + B^2\right) = d_2^2\left(A^2 + 4B^2\right).$$

Now $A = p^2 - q^2$, $B = pq$, and $pq \le b \le xy/2$, and so the method of descent applies to the product $xy$.

Suppose next that $x$ and $y$ are both odd. Then

$$xy = a^2 - b^2, \quad x^2 - y^2 = 2ab, \text{ with } \gcd(a, b) = 1,$$

and so $a$ and $b$ are not both odd. Then

$$a^4 - a^2b^2 + b^4 = \left(\frac{x^2 + y^2}{2}\right)^2.$$

Hence $ab = 0$, $x = y$, giving the solution $\left(k, k, k^2\right)$, $k \in \mathbb{Z}_+$. □

**Example 3.** *Prove that four distinct squares cannot form an arithmetic progression.*

*Solution.* Let the squares be $a^2, b^2, c^2, d^2$, arranged in increasing order. Then

$$a^2 + c^2 = 2b^2, \quad b^2 + d^2 = 2c^2.$$

Because of these relations, we may assume without loss of generality that $a, b, c, d$ are all odd. We have

$$a^2\Big(2c^2 - b^2\Big) = d^2\Big(2b^2 - c^2\Big),$$

and so

$$2\Big(a^2c^2 - b^2d^2\Big) = a^2b^2 - c^2d^2.$$

Setting $ac = x$, $bd = y$, $ab + cd = 2z$, $ab - cd = 2w$, we obtain

$$x^2 - y^2 = 2zw, \quad xy = z^2 - w^2,$$

yielding

$$x^4 - x^2y^2 + y^4 = \Big(z^2 + w^2\Big)^2.$$

From Theorem 2.3.3 it follows that $xy = 0$ or $x = y$. The first alternative is impossible. The second implies $w = 0$, so $ab = cd$, which is in contradiction to $a < b < c < d$.

### 2.3.2. Some Higher-Degree Diophantine Equations

**Theorem 2.3.4.** *The equation*

$$x^4 + y^4 = z^2 \tag{2.3.17}$$

*is not solvable in nonzero integers.*

*Proof.* We need only consider $x, y, z > 0$. Assume that (2.3.17) is solvable and let $(x_1, y_1, z_1)$ be a solution with $z_1$ minimal. We may suppose that $\gcd(x_1, y_1, z_1) = 1$, and taking into account that $\Big(x_1^2, y_1^2, z_1\Big)$ is a primitive Pythagorean triple, it follows that

$$\gcd(x_1, y_1) = \gcd(y_1, z_1) = \gcd(z_1, x_1) = 1$$

and that $x_1$ and $y_1$ are of different parities. Assume that $x_1$ is odd and that $y_1$ is even. Note that

$$\gcd\left(z_1 - x_1^2, z_1 + x_1^2\right) = 2. \tag{2.3.18}$$

Indeed, if $d \mid \left(z_1 - x_1^2\right)$ and $d \mid \left(z_1 + x_1^2\right)$, then $d \mid 2z_1$ and $d \mid 2x_1^2$. But $\gcd(z_1, x_1) = 1$ and $z_1$ is odd, so $d = 2$.

Since $y_1^4 = \left(z_1 - x_1^2\right)\left(z_1 + x_1^2\right)$, it follows that one of the numbers $z_1 - x_1^2$ and $z_1 + x_1^2$ is divisible by 2 and not by 4, and that the other is divisible by 8. Therefore $y_1 = 2ab$ and either

$$z_1 - x_1^2 = 2a^4, \quad z_1 + x_1^2 = 8b^4 \tag{2.3.19}$$

or

$$z_1 - x_1^2 = 8b^4, \quad z_1 + x_1^2 = 2a^4, \tag{2.3.20}$$

where in each case $a$ is odd and $\gcd(a, b) = 1$.

The situation (2.3.19) is not possible, because it would imply $x_1^2 = -a^4 + 4b^4$, giving $1 \equiv -1 \pmod 4$, a contradiction. Therefore we have the second alternative, i.e., $z_1 = a^4 + 4b^4$, with $0 < a < z_1$, and

$$4b^4 = \left(a^2 - x_1\right)\left(a^2 + x_1\right).$$

Since $\gcd(a, b) = 1$, we have $\gcd(a, x_1) = 1$, and we see, as in the proof of (2.3.18), that $\gcd\left(a^2 - x_1, a^2 + x_1\right) = 2$. Consequently,

$$a^2 - x_1 = 2x_2^4 \quad \text{and} \quad a^2 + x_1 = 2y_2^4,$$

where $x_2 y_2 = b$. Setting $a = z_2$, we obtain

$$x_2^4 + y_2^4 = z_2^2,$$

with $0 < z_2 < z_1$, which contradicts the minimality of $z_1$. □

**Corollary 2.3.5.** *The equation*

$$x^4 + y^4 = z^4 \tag{2.3.21}$$

*is not solvable in nonzero integers.*

The study of the equation

$$x^3 + y^3 = z^3 \tag{2.3.22}$$

is much more complicated and was first done by Euler.

Let $m$ and $a$ be integers such that $m \neq 0$ and $\gcd(a, m) = 1$. We say that $a$ is a quadratic residue modulo $m$ if the congruence

$$x^2 \equiv a \pmod{m}$$

is solvable. If $p > 2$ is a prime and $\gcd(a, p) = 1$, we introduce the Legendre symbol $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue,} \\ -1 & \text{otherwise.} \end{cases}$$

The following result due to Euler will be useful in what follows: If $p > 2$ is a prime and $\gcd(a, p) = 1$, then

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

**Theorem 2.3.6.** *Let $n$ be a positive integer. The Diophantine equation*

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

*is solvable if and only if all prime factors of $n$ of the form $3k - 1$ have even exponents.*

*Proof.* We note that a prime $p$ can be written in the form $p = x^2 + 3y^2$ if and only if $p = 3$ or $p = 3k + 1$, $k \in \mathbb{Z}_+$. Indeed, we have $3 = 0^2 + 3 \cdot 1^2$. Assume $p > 3$ and $p = x^2 + 3y^2$. Then $\gcd(x, p) = 1$ and $\gcd(y, p) = 1$. Therefore, there exists an integer $y'$ such that $yy' \equiv 1 \pmod{p}$. From the congruence $x^2 \equiv -3y^2 \pmod{p}$ it follows that $(xy')^2 \equiv -3 \pmod{p}$. We use the quadratic reciprocity law (see Theorem 4.3.2). But $\gcd(xy', 3) = 1$ implies $\left(\frac{-3}{p}\right) = 1$, or equivalently $(-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = 1$, i.e., $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$.

From the quadratic reciprocity law we obtain

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

Since $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$, we have $\left(\frac{p}{3}\right) = 1$, i.e., $p \equiv 1 \pmod{3}$.

Conversely, consider $p$ a prime of the form $3k + 1$. Then there exists an integer $a$ such that $a^2 \equiv -3 \pmod{p}$. Moreover, there exist integers $x, y$ such that $0 < x, y < \sqrt{p}$ and $p \mid \left(a^2x^2 - y^2\right)$. It is clear that $\gcd(a, p) = 1$, and if we set $b = [\sqrt{p}]$, then $(b + 1)^2 > p$. There exist $(b + 1)^2$ pairs $(u, v) \in \{0, 1, \ldots, b\} \times \{0, 1, \ldots, b\}$ and $(b + 1)^2$ integers of the form $au + v$, where $u, v \in \{0, 1, \ldots, b\}$. It follows that there exist pairs $(u_1, v_1) \neq (u_2, v_2)$ such that $au_1 + v_1 \equiv au_2 + v_2 \pmod{p}$. Assume $u_1 \geq u_2$ and define $x = u_1 - u_2$, $y = |v_1 - v_2|$. Therefore, $0 < x, y \leq b < \sqrt{p}$ and $ax + y \equiv 0 \pmod{p}$, i.e., $a^2x^2 - y^2 \equiv 0 \pmod{p}$ (see also Theorem 4.4.3). We obtain $p \mid \left(a^2 + 3\right)x^2 - \left(3x^2 + y^2\right)$, that is, $3x^2 + y^2 = lp$, where $l \in \mathbb{Z}_+$. From the inequalities $0 < x^2 < p$, $0 < y^2 < p$, it follows that $l \in \{1, 2, 3\}$.

If $l = 1$, we have $p = 3x^2 + y^2$.

If $l = 2$, the equality $2p = 3x^2 + y^2$ is not possible, since in this case the integers $x, y$ have the same parity and we obtain $2p \equiv 0 \pmod 4$, a contradiction.

If $l = 3$, we have $3p = 3x^2 + y^2$, and therefore $y = 3y_1$ and $p = x^2 + 3y_1^2$.

Now let us note that if $p \geq 3$ is a prime of the form $3k - 1$ and $p \mid x^2 + 3y^2$, then $p \mid x$ and $p \mid y$. Indeed, if $p \nmid x$, we have $\gcd(p, x) = 1$, so there exists an integer $y'$ with the property $yy' \equiv 1 \pmod p$. From $x^2 \equiv -3y^2 \pmod p$ it follows that $(xy')^2 \equiv -3 \pmod p$, i.e., $\left(\frac{-3}{p}\right) = 1$ and $p \equiv 1 \pmod 3$, a contradiction.

To prove the result in Theorem 2.3.6, consider $n = a^2 b$, where $b$ is a square-free integer. It follows that $b = \prod_{i=1}^{m} p_i$, where $p_i = 3$ or $p_i \equiv 1 \pmod 3$. Then $p_i = x_i^2 + 3y_i^2$ and $b = p_1 p_2 \cdots p_m = x^2 + 3y^2$, since it is easy to see that if $n_1 = x_1^2 + 3y_1^2$, $n_2 = x_2^2 + 3y_2^2$, then $n_1 n_2 = (x_1 x_2 + 3y_1 y_2)^2 + 3(x_1 y_2 - x_2 y_1)^2$. Finally, $n = a^2 b = (ax)^2 + 3(ay)^2$. □

**Lemma 2.3.7.** *The Diophantine equation*

$$x^2 + 3y^2 = z^3 \tag{2.3.23}$$

*has solution* $(x_0, y_0, z_0)$ *with* $z_0$ *odd and* $\gcd(x_0, y_0) = 1$ *if and only if there exist integers* $\alpha, \beta$ *such that* $\alpha \not\equiv \beta \pmod 2$, $\gcd(\alpha, 3\beta) = 1$, *and*

$$x_0 = \alpha\left(\alpha^2 - 9\beta^2\right), \quad y_0 = 3\beta\left(\alpha^2 - \beta^2\right), \quad z_0 = \alpha^2 + 3\beta^2.$$

*Proof.* Let $(x_0, y_0, z_0)$ be a triple of integers satisfying the above conditions. From the identity

$$\alpha^2\left(\alpha^2 - 9\beta^2\right)^2 + 3\left(3\beta\left(\alpha^2 - \beta^2\right)\right)^2 = \left(\alpha^2 + 3\beta^2\right)^3$$

it follows that $(x_0, y_0, z_0)$ is a solution to (2.3.23).

Since $\alpha \not\equiv \beta \pmod 2$ we obtain that $z_0$ is odd. From $\gcd(\alpha, 3\beta) = 1$, it follows that

$$\gcd\left(\alpha, 3\beta\left(\alpha^2 - \beta^2\right)\right) = \gcd\left(\alpha, \alpha^2 - \beta^2\right) = \gcd\left(\alpha, -\beta^2\right) = 1$$

and that

$$\gcd\left(\alpha^2 - 9\beta^2, 3\beta\right) = \gcd\left(\alpha^2, 3\beta\right) = 1.$$

Taking into account the condition $\alpha \not\equiv \beta \pmod 2$, we have

$$\gcd\left(\alpha^2 - 9\beta^2, \alpha^2 - \beta^2\right) = \gcd\left(-8\beta^2, \alpha^2 - \beta^2\right)$$
$$\gcd\left(\beta^2, \alpha^2 - \beta^2\right) = \gcd\left(\beta^2, \alpha^2\right) = 1.$$

To prove the converse implication, we will use induction on the number of prime factors of $z_0$, where the triple $(x_0, y_0, z_0)$ is a solution to (2.3.23) such that $z_0$ is odd and $\gcd(x_0, y_0) = 1$.

If $z_0 = 1$, we have $x_0 = \pm 1$, $y_0 = 0$, and $\alpha = \pm 1$, $\beta = 0$. Consider $z_0 > 1$ and let $p$ be a prime divisor of $z_0$. So $z_0 = pt$, where $p$ and $t$ are odd. From the equality

$$(pt)^3 = x_0^2 + 3y_0^2,$$

and using the relation $\gcd(x_0, y_0) = 1$ and the result in Theorem 2.3.6, it follows that $p = 6k + 1$ and there exist integers $\alpha_1, \beta_1$ such that

$$p = \alpha_1^2 + 3\beta_1^2.$$

Since $p$ is a prime and $p = 6k + 1$, we obtain $\gcd(\alpha_1, 3\beta_1) = 1$ and $\alpha_1 \not\equiv \beta_1 \pmod 2$.

From the above relation we get $p^3 = a^2 + 3b^2$, where

$$a = \alpha_1\Big(\alpha_1^2 - 9\beta_1^2\Big), \quad b = 3\beta_1\Big(\alpha_1^2 - \beta_1^2\Big).$$

It is not difficult to see that $a \not\equiv b \pmod 2$ and $\gcd(a, 3b) = 1$. We have

$$\begin{aligned} P^6t^3 = p^3z_0^3 &= \Big(a^2 + 3b^2\Big)\Big(x_0^2 + 3y_0^2\Big) = (ax_0 + 3by_0)^2 + 3(bx_0 - ay_0)^2 \\ &= (ax_0 - 3by_0)^2 + 3(bx_0 + ay_0)^2. \end{aligned}$$

Also

$$\begin{aligned} (bx_0 + ay_0)(bx_0 - ay_0) &= b^2x_0^2 - a^2y_0^2 = b^2x_0^2 - \Big(p^3 - 3b^2\Big)y_0^2 \\ &= b^2\Big(x_0^2 + 3y_0^2\Big) - p^3y_0^2 = b^2z_0^3 - p^3y_0^2 \\ &= b^2p^3t^3 - p^3y_0^2. \end{aligned}$$

Therefore $p^3 \mid (bx_0 + ay_0)(bx_0 - ay_0)$. Since $\gcd(abx_0y_0, p) = 1$, it follows that the relations $p \mid bx_0 + ay_0$ and $p \mid bx_0 - ay_0$ cannot be satisfied simultaneously.

Therefore, there exists $\varepsilon \in \{-1, 1\}$ such that $bx_0 - \varepsilon ay_0 = p^3d$. We obtain $ax_0 + 3\varepsilon by_0 = p^3c$, $t^3 = c^2 + 3d^2$, and

$$x_0 = ac + 3bd, \quad y_0 = \varepsilon(bc - ad).$$

If $z_0$ has in its decomposition $n$ prime factors, then since $z_0 = pt$, it follows that $t$ has $n - 1$ prime factors. From $\gcd(x_0, y_0) = 1$ we obtain $\gcd(c, d) = 1$. Taking into account that $t$ is odd and that it satisfies the induction hypothesis for $n - 1$, we obtain integers $\alpha_2$ and $\beta_2$ satisfying the properties $\alpha_2 \not\equiv \beta_2 \pmod 2$, $\gcd(\alpha_2, 3\beta_2) = 1$,

$c = \alpha_2\left(\alpha_2^2 - 9\beta_2^2\right)$, $d = 3\beta_2\left(\alpha_2^2 - \beta_2^2\right)$ and $t = \alpha_2^2 + 3\beta_2^2$. From the above relations it follows that

$$z_0 = pt = \left(\alpha_1^2+3\beta_1^2\right)\left(\alpha_2^2+3\beta_2^2\right) = (\alpha_1\alpha_2+3\beta_1\beta_2)^2+3(\alpha_1\beta_2-\alpha_2\beta_1)^2.$$

Writing

$$\alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2, \quad \beta = \varepsilon(\alpha_2\beta_1 - \alpha_1\beta_2),$$

we obtain $z_0 = \alpha^2 + 3\beta^2$ and

$$x_0 = \alpha\left(\alpha^2 - 9\beta^2\right), \quad y_0 = 3\beta\left(\alpha^2 - \beta^2\right).$$

Finally, $\alpha - \beta \equiv \alpha_1\alpha_2 + \beta_1\beta_2 - (\alpha_1\beta_2 + \alpha_2\beta_1) \equiv (\alpha_1 - \beta_1)(\alpha_2 - \beta_2) \pmod 2$, so $\alpha \not\equiv \beta \pmod 2$. From $\gcd(x_0, y_0) = 1$ it follows that $\gcd(\alpha, 3\beta) = 1$. □

**Theorem 2.3.8.** *Equation (2.3.22) is not solvable in nonzero integers.*

*Proof.* Assume that (2.3.22) is solvable and let $(x_0, y_0, z_0)$ be a solution with $x_0y_0z_0 \neq 0$ and $|x_0y_0z_0|$ minimal.

It is clear that two of the integers $x_0, y_0, z_0$ are odd. Let us assume that $x_0$ and $y_0$ have this property. Set

$$x_0 + y_0 = 2u \quad \text{and} \quad x_0 - y_0 = 2v,$$

and we can assume that $u > 0$.

We obtain $x_0 = u+v$, $y_0 = u-v$, and from (2.3.22) it follows that

$$2u\left(u^2 + 3v^2\right) = z_0^3. \tag{2.3.24}$$

Since $x_0$ is odd, we have that $u$ and $v$ are of different parities, i.e., $u^2 + 3v^2$ is odd. From $\gcd(x_0, y_0) = 1$ we obtain $\gcd(u, v) = 1$ and $\gcd\left(2u, u^2 + 3v^2\right) = \gcd\left(u, u^2 + 3v^2\right) = \gcd\left(u, 3v^2\right) = \gcd(u, 3)$.

**Case 1.** If $\gcd(u,3)=1$, then from (2.3.24) it follows that

$$2u=t^3,\quad u^2+3v^2=s^3,\quad \text{and}\quad ts=z_0.$$

From Lemma 2.3.7, we obtain that there exist integers $\alpha,\beta$ such that $\gcd(\alpha,3\beta)=1$, $\alpha\not\equiv\beta \pmod 2$, and

$$s=\alpha^2+3\beta^2,\quad u=\alpha\Big(\alpha^2-9\beta^2\Big),\quad v=3\beta\Big(\alpha^2-\beta^2\Big).$$

Therefore, $2u=t^3=(2\alpha)(\alpha-3\beta)(\alpha+3\beta)$. The factors $2\alpha$, $\alpha-3\beta$, $\alpha+3\beta$ are pairwise relatively prime, so

$$2\alpha=z^3,\quad \alpha-3\beta=X^3,\quad \alpha+3\beta=Y^3.$$

We obtain

$$X^3+Y^3=Z^3$$

and $XYZ\neq 0$, i.e., $(X,Y,Z)$ is a nonzero integral solution to (2.3.22). Moreover,

$$\begin{aligned}|XYZ|&=\sqrt[3]{|2\alpha(\alpha^2-9\beta^2)|}=\sqrt[3]{2u}=\sqrt[3]{x_0+y_0}\\&<|\sqrt[3]{x_0y_0}|<|x_0y_0z_0|,\end{aligned}$$

which contradicts the minimality of $|x_0y_0z_0|$.

**Case 2.** If $\gcd(u,3)=3$, then $u=3u_1$, and from (2.3.24) it follows that $z_0=3z_1$ and

$$2u_1(3u_1^2+v^2)=3z_1^3. \tag{2.3.25}$$

Taking into account that $\gcd(u,v)=1$, we obtain $\gcd(v,3)=1$ and $\gcd\Big(3u_1^2+v^2,3\Big)=1$. From (2.3.25) it follows that $u_1=3u_2$, $u_2\in\mathbb{Z}$, and $2u_2\Big(3u_1^2+v^2\Big)=z_1^3$.

Since $\gcd\left(2u_2, 3u_1^2 + v^2\right) = 1$, we obtain

$$2u_2 = m^3 \quad \text{and} \quad 3u_1^2 + v^2 = n^3,$$

where $n$ is an odd integer.

Applying Lemma 2.3.7, it follows that there exist integers $\alpha, \beta$ such that $\gcd(\alpha, 3\beta) = 1$, $\alpha \not\equiv \beta \pmod 2$, and $v = \alpha(\alpha^2 - 9\beta^2)$, $u_1 = 3\beta(\alpha^2 - \beta^2)$. Therefore $u_2 = \beta\left(\alpha^2 - \beta^2\right)$ and $m^3 = 2\beta(\alpha - \beta)(\alpha + \beta)$.

Taking into account that the integers $2\beta$, $\alpha - \beta$, and $\alpha + \beta$ are pairwise relatively prime, we obtain $\alpha - \beta = X^3$, $\alpha + \beta = Z^3$, $2\beta = Y^3$, for some nonzero integers $X, Y, Z$. It follows that

$$X^3 + Y^3 = Z^3$$

and

$$|XYZ| = \sqrt[3]{\left|2\beta\left(\alpha^2 - \beta^2\right)\right|} < \left|\sqrt[3]{2u}\right| = \left|\sqrt[3]{x_0 + y_0}\right| < \left|x_0 y_0 z_0\right|,$$

which contradicts the minimality of $|x_0 y_0 z_0|$. □

**Remarks.** (1) Equations (2.3.21) and (2.3.22) are special cases of Fermat's equation

$$x^n + y^n = z^n, \tag{2.3.26}$$

where $n$ is an integer greater than 2 and $x, y, z$ are nonzero integers.

Fermat's last theorem states that equation (2.3.26) has no nonzero integer solutions for $x, y, z$ when $n > 2$.

Around 1630, Fermat wrote a note in the margin of a page of Diophantus's *Arithmetica*:

"I have discovered a truly remarkable proof which this margin is too small to contain."

Fermat apparently had found a proof only for the case $n = 4$, but when his marginal note was published, this theorem became famous, capturing the attention of the mathematics world and remaining for centuries the last of Fermat's Theorems yet to be proved.

Through the years, many important mathematicians worked on special cases and solved them affirmatively. We mention here Euler ($n = 3$), Sophie Germain ($n$ and $2n + 1$ are primes, $n < 100$, and $x, y, z$ are not divisible by $n$), Dirichlet ($n = 5$, $n = 14$), and Lamé ($n = 7$). Liouville and Kummer developed important mathematical theories in their attempts to prove Fermat's last theorem.

Using techniques based on Kummer's work, Fermat's Last Theorem was proved true, with the help of computers, for $n$ up to 4,000,000 by 1993.

In 1983, a major contribution was made by Gerd Faltings, who proved that for every $n > 2$ there are at most a finite number of relatively prime integers satisfying equation (2.3.26).

The proof of Fermat's last theorem was almost completed in 1993 by Andrew Wiles, a British mathematician working at Princeton in the USA. Wiles gave a series of three lectures at the Isaac Newton Institute in Cambridge, England, the first on Monday, June 21, and the second on June 22. In the final lecture on Wednesday, June 23, 1993, Wiles announced his proof of Fermat's last theorem as a corollary to his main results. His proof turned to be incomplete.

In October, 1994, Wiles sent a new proof to three colleagues, including Faltings. All accepted the new proof, which was essentially simpler than the earlier one.

Pierre de Fermat died in 1665. Today we think of Fermat as a number theorist, in fact as perhaps the most famous number theorist who ever lived. It is therefore surprising to find that Fermat was in fact a lawyer and only an amateur mathematician. Also surprising may be the fact that he published only one mathematical paper in his life, and that was an anonymous article written as an appendix to a colleague's book. But perhaps it is less surprising when we note that there were no mathematical journals at the time, and most scientific communication was carried on by private correspondance.

(2) Euler conjectured that the equation

$$x^n + y^n + z^n = w^n \tag{2.3.27}$$

has no integral solution if $n$ is an integer greater than or equal to 4.

In 1988, Noam Elkies gave the following counterexample:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Subsequently, Roger Frye (1988) found the smallest solution to (2.3.27):

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

**Example 4.** *The equation*

$$x^4 - y^4 = z^2 \tag{2.3.28}$$

*is not solvable in nonzero integers.*

*Solution.* We may assume that $x, y, z > 0$ and consider a solution $(x, y, z)$ with $\gcd(x, y) = 1$ and $x$ minimal. Then $\left(y^2, z, x^2\right)$ is a primitive Pythagorean triple, so we have the following two cases:

*Case* 1: $y^2 = a^2 - b^2$, $z = 2ab$, $x^2 = a^2 + b^2$,

where $a > b > 0$ and $\gcd(a, b) = 1$. It follows that

$$a^4 - b^4 = (xy)^2$$

and $a < x$, contradicting the minimality of $x$.

*Case* 2: $y^2 = 2ab$, $z = a^2 - b^2$, $x^2 = a^2 + b^2$,

where $a > b > 0$ and $\gcd(a, b) = 1$.

Since $(a, b, x)$ is also a primitive Pythagorean triple, we may assume that $a$ is even and $b$ is odd. Then $a = 2p^2$ and $b = q^2$ for some positive integers $p, q$ with $\gcd(p, q) = 1$ and $q \equiv 1 \pmod 2$. It follows that

$$x^2 = 4p^4 + q^4 \quad \text{and} \quad y = 2pq.$$

Hence $\left(2p^2, q^2, x\right)$ is itself a primitive Pythagorean triple, and so

$$p^2 = rs, \quad q^2 = r^2 - s^2$$

for some positive integers $r, s$ with $r > s$ and $\gcd(r, s) = 1$.

Finally, $r = u^2$, $s = v^2$, for some positive integers $u, v$ with $\gcd(u, v) = 1$. Then

$$u^4 - v^4 = q^2$$

and $u = \sqrt{r} \leq p < 2p^2 < x$, which contradicts the minimality of $x$. □

*Alternative Proof.* We may assume that $x, y, z > 0$ and that $\gcd(x, y) = 1$. Write the equation as

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

It is not difficult to see that

$$\gcd\left(x^2 - y^2, x^2 + y^2\right) = 1 \quad \text{or} \quad \gcd\left(x^2 - y^2, x^2 + y^2\right) = 2.$$

In the first case, we obtain the system

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

which, according to Example 2 in Section 2.2, is not solvable.

In the second case, we obtain

$$\begin{cases} x^2 - y^2 = 8r^2, \\ x^2 + y^2 = 2s^2, \end{cases}$$

hence

$$\begin{cases} s^2 + (2r)^2 = x^2, \\ s^2 - (2r)^2 = y^2, \end{cases}$$

which, by the same argument, is not solvable. □

**Example 5.** *Solve in integers the equation*

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

*Solution.* Without loss of generality, we may assume that

$$\gcd(x, y) = 1.$$

Then $x$ and $y$ are both odd, and

$$z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2.$$

From Example 4 it follows that $xyz = 0$ or $x^4 - y^4 = 0$, and so $x = y = z = 0$ or $x^2 = y^2 = z$.

The solutions are $\left(k, k, k^2\right)$, $k \in \mathbb{Z}$.

**Example 6.** *Solve in integers the equation*

$$x^4 + 6x^2y^2 + y^4 = z^2.$$

*Solution.* Let $(x, y, z)$ be a solution to the equation. Then

$$(2x)^4 + 6(2x)^2(2y)^2 + (2y)^4 = (4z)^2.$$

Setting $2x = u + v$, $2y = u - v$, where $u, v \in \mathbb{Z}$, we obtain the equation

$$(u+v)^4 + 6\Big(u^2 - v^2\Big)^2 + (u-v)^4 = 16z^2,$$

which is equivalent to

$$u^4 + v^4 = 2z^2.$$

From the previous example it follows that $(u, v, z) = \Big(k, k, k^2\Big)$, yielding the solutions $(x, y, z) = \Big(k, 0, k^2\Big)$ and $(x, y, z) = \Big(0, k, k^2\Big)$, $k \in \mathbb{Z}$.

**Remark.** Another variant of this problem was given in the second part of Problem 2 in Section 2.2.

## Exercises and Problems

**1.** Let $p$ be a prime. Find all solutions to the equation

$$a + b - c - d = p,$$

where $a, b, c, d$ are positive integers such that $ab = cd$.

(Mathematical Reflections)

**2.** Let $a, b, c$ be integers such that

$$\gcd(a, b, c) = 1 \text{ and } ab + bc + ca = 0.$$

Prove that $|a + b + c|$ can be expressed in the form $x^2 + xy + y^2$, where $x, y$ are integers.

**3.** Prove that the equation $x^2 + xy + y^2 = 36^2$ is not solvable in positive integers.

**4.** Find all pairs of positive integers such that

$$x^2 - xy + y^2 = 727.$$

(Turkish Mathematical Olympiad)

**5.** We say that the positive integer $z$ satisfies property (P) if $z = x^2 + xy + y^2$, for some positive integers $x$ and $y$. Prove that:

(a) if $z$ satisfies property (P), then so does $z^2$;

(b) if $z^2$ satisfies property (P) with the additional condition that $\gcd(x, y) = 1$, then so does $z$.

(Dorin Andrica)

**6.** Solve in integers the equation $x^2 + 3y^2 = 4z^2$.

**7.** Find all triples $(x, y, z)$ of nonnegative integers satisfying the equation $x^4 + 14x^2y^2 + y^4 = z^2$.

(Ion Cucuruzeanu)

**8.** Solve in positive integers the equation

$$3x^4 + 10x^2y^2 + 3y^4 = z^2.$$

**9.** Find all distinct squares $a^2, b^2, c^2$ that form an arithmetic progression.

**10.** Solve in integers the equation $xy\Big(x^2 + y^2\Big) = 2z^2$.

(Titu Andreescu)

**11.** Find all integral triples $(x, y, z)$ satisfying the equation

$$x^4 - 6x^2y^2 + y^4 = z^2.$$

**12.** If $a$ and $b$ are distinct positive integers, then $2a(a^2 + 3b^2)$ is not a cube.

**13.** Prove that equation $x^6 - y^6 = 4z^3$ is not solvable in positive integers.

(Titu Andreescu)

**14.** Prove that the system of equations

$$\begin{cases} x + y = z^2, \\ xy = \dfrac{z^4 - z}{3}, \end{cases}$$

is not solvable in nonzero integers.

(Titu Andreescu)

# I.3

# Pell-Type Equations

In 1909, A. Thue proved the following important theorem:

*Let $f = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ be an irreducible polynomial of degree $\geq 3$ with integral coefficients. Consider the corresponding homogeneous polynomial*

$$F(x, y) = y^n f\left(\frac{x}{y}\right) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n.$$

*For a nonzero integer $m$ the equation $F(x, y) = m$ has either no solution or only a finite number of solutions in integers.*

This result is in contrast to the situation in which the degree of $F$ is 2, or $n = 2$. In this case, if $F(x, y) = x^2 - Dy^2$, where $D$ is a non-square positive integer, then for all nonzero integers $m$, either the general Pell's equation

$$x^2 - Dy^2 = m$$

has no solution or it has infinitely many integral solutions.

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, 117
DOI 10.1007/978-0-8176-4549-6_3, © Springer Science+Business Media, LLC 2010

## 3.1 Pell's Equation: History and Motivation

Euler, after a cursory reading of Wallis's *Opera Mathematica*, mistakenly attributed the first serious study of nontrivial solutions to equations of the form $x^2 - dy^2 = 1$, where $x \neq 1$ and $y \neq 0$, to John Pell. However, there is no evidence that Pell, who taught at the University of Amsterdam, had ever considered solving such equations. They should be probably called Fermat's equations, since it was Fermat who first investigated the properties of nontrivial solutions of many important such equations. Nevertheless, Pell-type equations have a long history and can be traced back to the Greeks. Theon of Smyrna used $x/y$ to approximate $\sqrt{2}$, where $x$ and $y$ are integral solutions to $x^2 - 2y^2 = 1$. In general, if $x^2 = dy^2 + 1$, then $x^2/y^2 = d + 1/y^2$. Hence, for $y$ large, $x/y$ is a good approximation of $\sqrt{d}$, a fact that was well known to Archimedes. Archimedes's *problema bovinum* took two thousand years to solve.

In *Arithmetica*, Diophantus asks for rational solutions to equations of the type $x^2 - dy^2 = 1$. In the case $d = m^2 + 1$, Diophantus offered the integral solution $x = 2m^2 + 1$ and $y = 2m$. Pell-type equations are also found in Hindu mathematics. In the fourth century, the Indian mathematician Baudhayana noted that $x = 577$ and $y = 408$ is a solution of $x^2 - 2y^2 = 1$ and used the fraction $\frac{577}{408}$ to approximate $\sqrt{2}$. In the seventh century, Brahmagupta considered solutions to Pell's equation $x^2 - 92y^2 = 1$, the smallest solution being $x = 1151$ and $y = 120$. In the twelfth century, the Hindu mathematician Bhaskara found the least positive solution to Pell's equation $x^2 - 61y^2 = 1$ to be $x = 1766319049$ and $y = 226153980$.

In 1657, Fermat stated without proof that if $d$ is positive and not the square of an integer, then Pell's equation $x^2 - dy^2 = 1$ has an infinite number of solutions. For if $(x, y)$ is a solution to $x^2 - dy^2 = 1$, then $1^2 = (x^2 - dy^2)^2 = (x^2 + dy^2)^2 - (2xy)^2 d$. Thus, $(x^2 + dy^2, 2xy)$ is also a solution to $x^2 - dy^2 = 1$. Therefore, if Pell's equation has a solution, then it has infinitely many.

In 1657, Fermat challenged William Brouncker, of Castle Lynn in Ireland, and John Wallis to find integral solutions to the equations

$$x^2 - 151y^2 = 1 \quad \text{and} \quad x^2 - 313y^2 = -1.$$

He cautioned them not to submit rational solutions because even the lowest type of arithmetician could devise such answers. Wallis replied with $(1728148040, 140634693)$ as a solution to the first equation. Brouncker replied with $(126862368, 7170685)$ as a solution to the second.

In 1770, Euler showed that no triangular number other than unity is a cube and none but unity is a fourth power. He devised a method, involving solutions to Pell's equations, to determine natural numbers that are both triangular and square.

In 1766, Lagrange proved that the equation $x^2 = dy^2 + 1$ has an infinite number of solutions whenever $d$ is positive and not a square of an integer.

The Diophantine quadratic equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{3.1.1}$$

with integral coefficients $a, b, c, d, e, f$ reduces in its main case to a Pell-type equation. We will sketch the general method of reduction.

Equation (3.1.1) represents a conic in the Cartesian plane, so solving (3.1.1) in integers means finding all lattice points situated on this conic. We will solve equation (3.1.1) by reducing the general equation of the conic to its canonical form. We introduce the discriminant of the equation (3.1.1) as $\Delta = b^2 - 4ac$. When $\Delta < 0$, the conic defined by (3.1.1) is an ellipse, and in this case the given equation has only a finite number of solutions. When $\Delta = 0$, the conic given by (3.1.1) is a parabola. If $2ae - bd = 0$, then equation (3.1.1) becomes $(2ax + by + d)^2 = d^2 - 4af$, which is not difficult to solve. In the case $2ae - bd \neq 0$, by performing the substitutions $X = 2ax + by + d$ and $Y = (4ae - 2bd)y + 4af - d^2$, equation (3.1.1) reduces to $X^2 + Y = 0$, which is easy to solve. The most interesting case is $\Delta > 0$, when the conic defined by (3.1.1) is a hyperbola. Using a sequence of substitutions, equation (3.1.1) reduces to the general Pell-type equation

$$X^2 - DY^2 = N. \tag{3.1.2}$$

To illustrate the process described above, we will consider the equation

$$2x^2 - 6xy + 3y^2 = -1$$

(Berkeley Math Circle 2000–2001 Monthly Contest #4, Problem 4).

Indeed, $\Delta = 12 > 0$; hence the corresponding conic is a hyperbola. The equation can be written as $x^2 - 3(y-x)^2 = 1$, and by performing the substitutions $X = x$ and $Y = y - x$, we reduce it to Pell's equation $X^2 - 3Y^2 = 1$.

## 3.2 Solving Pell's Equation

We will present an elementary approach to solving Pell's equation due to Lagrange. Denote by $(u_0, v_0) = (1, 0)$ the trivial solution to the equation $u^2 - Dv^2 = 1$. The main result is the following.

**Theorem 3.2.1.** *If $D$ is a positive integer that is not a perfect square, then the equation*

$$u^2 - Dv^2 = 1 \tag{3.2.1}$$

*has infinitely many solutions in nonnegative integers, and the general solution is given by $(u_n, v_n)_{n\geq 0}$,*

$$u_{n+1} = u_1 u_n + D v_1 v_n, \quad v_{n+1} = v_1 u_n + u_1 v_n, \tag{3.2.2}$$

*where $(u_1, v_1)$ is the fundamental solution, i.e., the solution with $v_1 > 0$ minimal.*

*Proof.* First, we will prove that equation (3.2.1) has a fundamental solution.

Let $c_1$ be an integer greater than 1. We will show that there exist integers $t_1, w_1 \geq 1$ such that

$$|t_1 - w_1\sqrt{D}| < \frac{1}{c_1}, \quad w_1 \leq c_1.$$

Indeed, considering $l_k = [k\sqrt{D} + 1]$, $k = 0, \ldots, c_1$, yields $0 < l_k - k\sqrt{D} \leq 1$, $k = 0, \ldots, c_1$, and since $\sqrt{D}$ is an irrational number, it follows that $l_{k'} \neq l_{k''}$ whenever $k' \neq k''$.

There exist $i, j, p \in \{0, 1, 2, \ldots, c_1\}$, $i \neq j$, $p \neq 0$, such that

$$\frac{p-1}{c_1} < l_i - i\sqrt{D} \leq \frac{p}{c_1} \quad \text{and} \quad \frac{p-1}{c_1} < l_j - j\sqrt{D} \leq \frac{p}{c_1}$$

because there are $c_1$ intervals of the form $\left(\frac{p-1}{c_1}, \frac{p}{c_1}\right)$, $p = 1, \ldots, c_1$, and $c_1 + 1$ numbers of the form $l_k - k\sqrt{D}$, $k = 0, \ldots, c_1$.

From the inequalities above it follows that $|(l_j - l_i) - (j-i)\sqrt{D}| < \frac{1}{c_1}$, and setting $|l_i - l_j| = t_1$ and $|j - i| = w_1$ yields $|t_1 - w_1\sqrt{D}| < \frac{1}{c_1}$, and $w_1 \leq c_1$.

Multiplying this inequality by $t_1 + w_1\sqrt{D} < 2w_1\sqrt{D} + 1$ gives

$$\left|t_1^2 - Dw_1^2\right| < 2\frac{w_1}{c_1}\sqrt{D} + \frac{1}{c_1} < 2\sqrt{D} + 1.$$

Choosing a positive integer $c_2 > c_1$ such that $|t_1 - w_1\sqrt{D}| > \frac{1}{c_2}$, we obtain positive integers $t_2, w_2$ with $|t_2 - w_2\sqrt{D}| < \frac{1}{c_2}$ and $w_2 \leq c_2$.

As before, we get

$$|t_2^2 - Dw_2^2| < 2\sqrt{D} + 1 \quad \text{and} \quad |t_1 - t_2| + |w_1 - w_2| \neq 0.$$

By continuing this procedure, we obtain a sequence of distinct pairs $(t_n, w_n)_{n\geq 1}$ satisfying the inequalities $|t_n^2 - Dw_n^2| < 2\sqrt{D}+1$ for all positive integers $n$. It follows that the interval $(-2\sqrt{D}-1, 2\sqrt{D}+1)$ contains a nonzero integer $k$ such that there exists a subsequence of $(t_n, w_n)_{n\geq 1}$ satisfying the equation $t^2 - Dw^2 = k$. This subsequence contains at least two pairs $(t_s, w_s)$, $(t_r, w_r)$ for which $t_s \equiv t_r (\mathrm{mod}|k|)$, $w_s \equiv w_r (\mathrm{mod}|k|)$, and $t_s w_r - t_r w_s \neq 0$; otherwise $t_s = t_r$ and $w_s = w_r$, in contradiction to $|t_s - t_r| + |w_s - w_r| \neq 0$.

Let $t_0 = t_s t_r - D w_s w_r$ and let $w_0 = t_s w_r - t_r w_s$. Then

$$t_0^2 - Dw_0^2 = k^2. \tag{3.2.3}$$

On the other hand, $t_0 = t_s t_r - D w_s w_r \equiv t_s^2 - D w_0^2 \equiv 0 (\mathrm{mod}|k|)$, and we see that $w_0 \equiv 0 (\mathrm{mod}|k|)$. The pair $(t, w)$ where $t_0 = t|k|$ and $w_0 = w|k|$ is a nontrivial solution to equation (3.2.1). We show now

that the pair $(u_n, v_n)$ defined by (3.2.2) satisfies equation (3.2.1). We use induction with respect to $n$. Clearly, $(u_1, v_1)$ is a solution to equation (3.2.1). If $(u_n, v_n)$ is a solution to this equation, then

$$\begin{aligned} u_{n+1}^2 - Dv_{n+1}^2 &= (u_1u_n + Dv_1v_n)^2 - D(v_1u_n + u_1v_n)^2 \\ &= (u_1^2 - Dv_1^2)(u_n^2 - Dv_n^2) = 1, \end{aligned}$$

i.e., the pair $(u_{n+1}, v_{n+1})$ is also a solution to the equation (3.2.1).

It is not difficult to see that for all nonnegative integers $n$,

$$u_n + v_n\sqrt{D} = (u_1 + v_1\sqrt{D})^n. \tag{3.2.4}$$

Let $z_n = u_n + v_n\sqrt{D} = (u_1 + v_1\sqrt{D})^n$, $n \geq 0$, and note that

$$z_0 < z_1 < z_2 < \cdots < z_n < \cdots .$$

We will prove now that all solutions to equation (3.2.1) satisfy (3.2.4). Indeed, if equation (3.2.1) had a solution $(u, v)$ such that $z = u + v\sqrt{D}$ is not of the form (3.2.4), then $z_m < z < z_{m+1}$ for some integer $m$. Then

$$1 < (u + v\sqrt{D})(u_m - v_m\sqrt{D}) < u_1 + v_1\sqrt{D},$$

and therefore

$$1 < (uu_m - Dvv_m) + (u_mv - uv_m)\sqrt{D} < u_1 + v_1\sqrt{D}.$$

On the other hand,

$$(uu_m - Dvv_m)^2 - D(u_mv - uv_m)^2 = (u^2 - Dv^2)(u_m^2 - Dv_m^2) = 1,$$

i.e., $(uu_m - Dvv_m, u_mv - uv_m)$ is a solution of (3.2.1) less than $(u_1, v_1)$, contradicting the assumption that $(u_1, v_1)$ was the minimal one. □

**Remarks.** (1) The relations (3.2.2) could be written in the following useful matrix form:

$$\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix},$$

whence

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}. \tag{3.2.5}$$

If

$$\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix},$$

then it is well known that each of $a_n, b_n, c_n, d_n$ is a linear combination of $\lambda_1^n, \lambda_2^n$, where $\lambda_1, \lambda_2$ are the eigenvalues of the matrix

$$\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}.$$

Using (3.2.5), after an easy computation,

$$\begin{aligned} u_n &= \frac{1}{2}[(u_1 + v_1\sqrt{D})^n + (u_1 - v_1\sqrt{D})^n], \\ v_n &= \frac{1}{2\sqrt{D}}[(u_1 + v_1\sqrt{D})^n - (u_1 - v_1\sqrt{D})^n] \end{aligned} \tag{3.2.6}$$

(2) The solutions to Pell's equation given in the form (3.2.4) or (3.2.6) may be used in the approximation of the square roots of positive integers that are not perfect squares. Indeed, if $(u_n, v_n)$ are the solutions of equation (3.2.1), then

$$u_n - v_n\sqrt{D} = \frac{1}{u_n + v_n\sqrt{D}};$$

and so

$$\frac{u_n}{v_n} - \sqrt{D} = \frac{1}{v_n(u_n + v_n\sqrt{D})} < \frac{1}{\sqrt{D}v_n^2} < \frac{1}{v_n^2}.$$

It follows that

$$\lim_{n\to\infty} \frac{u_n}{v_n} = \sqrt{D}; \tag{3.2.7}$$

i.e., the fractions $\frac{u_n}{v_n}$ approximate $\sqrt{D}$ with an error less than $\frac{1}{v_n^2}$.

The main method of determining the fundamental solution to Pell's equation (3.2.1) involves continued fractions.

It is obtained by writing $\sqrt{D}$ as a simple continued fraction:

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

where $a_0 = \lfloor\sqrt{D}\rfloor$ and $a_1, a_2, \ldots$ is a periodic sequence of positive integers. The continued fraction will be denoted by $[a_0, a_1, a_2, \ldots]$. The $k$th convergent of $[a_0, a_1, a_2, \ldots]$ is the number

$$\frac{p_k}{q_k} = [a_0, a_1, a_2, \ldots, a_k]$$

with $p_k, q_k$ relatively prime. Let $a_1, a_2, \ldots, a_m$ be the period for $\sqrt{D}$. The least fundamental solution to Pell's equation turns out to be

$$(x_1, y_1) = \begin{cases} (p_{m-1}, q_{m-1}) & \text{if } m \text{ is even} \\ (p_{2m-1}, q_{2m-1}) & \text{if } m \text{ is odd} \end{cases}$$

For example,

$$\sqrt{3} = [1, 1, 2, 1, 2, \ldots],$$

and so $m = 2$; then $[1, 1] = \frac{2}{1}$. We check $2^2 - 3 \cdot 1^2 = 1$, and clearly $(2, 1)$ is the least positive solution of $x^2 - 3y^2 = 1$. Next, $\sqrt{2} =$

$[1, 2, 2, \dots]$, and so $m = 1$ then $[1, 2] = \frac{3}{2}$. We check $3^2 - 2 \cdot 2^2 = 1$, and again clearly $(3, 2)$ is the least positive solution of $x^2 - 2y^2 = 1$.

We consider it useful to include a table containing the fundamental solutions for $D \leq 103$.

**Example 1.** *Recall that* $t_m = \frac{m(m+1)}{2}$ *denotes the* $m^{th}$ *triangular number,* $m \geq 1$. *Find all triangular numbers that are perfect squares.*

*Solution.* The equation $t_x = y^2$ is equivalent to

$$(2x + 1)^2 - 8y^2 = 1.$$

The Pell's equation

$$u^2 - 8v^2 = 1$$

has the fundamental solution $(u_1, v_1) = (3, 1)$, and by formulas (3.2.6) we obtain

$$u_n = \frac{1}{2}[(3 + \sqrt{8})^n + (3 - \sqrt{8})^n],$$
$$v_n = \frac{1}{2\sqrt{8}}[(3 + \sqrt{8})^n - (3 - \sqrt{8})^n], \ n \geq 1.$$

It follows that

$$2x_n + 1 = u_n = \frac{1}{2}\Big[(\sqrt{2} + 1)^{2n} + (\sqrt{2} - 1)^{2n}\Big],$$

and hence

$$x_n = \left[\frac{(\sqrt{2} + 1)^n - (\sqrt{2} - 1)^n}{2}\right]^2.$$

Every odd $x$ satisfying $t_x = y^2$ is itself a perfect square.

**Example 2.** *Prove that there are infinitely many triples of consecutive integers each of which is a sum of two squares.*

(Putnam Mathematical Competition)

| $D$ | $u_1$ | $v_1$ | $D$ | $u_1$ | $v_1$ | $D$ | $u_1$ | $v_1$ |
|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 2 | 38 | 37 | 6 | 71 | 3480 | 413 |
| 3 | 2 | 1 | 39 | 25 | 4 | 72 | 17 | 2 |
| 5 | 9 | 4 | 40 | 19 | 3 | 73 | 2281249 | 267000 |
| 6 | 5 | 2 | 41 | 2049 | 320 | 74 | 3699 | 430 |
| 7 | 8 | 3 | 42 | 13 | 2 | 75 | 26 | 3 |
| 8 | 3 | 1 | 43 | 3482 | 531 | 76 | 57799 | 6630 |
| 10 | 19 | 6 | 44 | 199 | 30 | 77 | 351 | 40 |
| 11 | 10 | 3 | 45 | 161 | 24 | 78 | 53 | 6 |
| 12 | 7 | 2 | 46 | 24335 | 3588 | 79 | 80 | 9 |
| 13 | 649 | 180 | 47 | 48 | 7 | 80 | 9 | 1 |
| 14 | 15 | 4 | 48 | 7 | 1 | 82 | 163 | 18 |
| 15 | 4 | 1 | 50 | 99 | 14 | 83 | 82 | 9 |
| 17 | 33 | 8 | 51 | 50 | 7 | 84 | 55 | 6 |
| 18 | 17 | 4 | 52 | 649 | 90 | 85 | 285769 | 30996 |
| 19 | 170 | 39 | 53 | 66249 | 9100 | 86 | 10405 | 1122 |
| 20 | 9 | 2 | 54 | 485 | 66 | 87 | 28 | 3 |
| 21 | 55 | 12 | 55 | 89 | 12 | 88 | 197 | 21 |
| 22 | 197 | 42 | 56 | 15 | 2 | 89 | 500001 | 53000 |
| 23 | 24 | 5 | 57 | 151 | 20 | 90 | 19 | 2 |
| 24 | 5 | 1 | 58 | 19603 | 2574 | 91 | 1574 | 165 |
| 26 | 51 | 10 | 59 | 530 | 69 | 92 | 1151 | 120 |
| 27 | 26 | 5 | 60 | 31 | 4 | 93 | 12151 | 1260 |
| 28 | 127 | 24 | 61 | 1766319049 | 226153980 | 94 | 2143295 | 221064 |
| 29 | 9801 | 1820 | 62 | 63 | 8 | 95 | 39 | 4 |
| 30 | 11 | 2 | 63 | 8 | 1 | 96 | 49 | 5 |
| 31 | 1520 | 273 | 65 | 129 | 16 | 97 | 62809633 | 6377352 |
| 32 | 17 | 3 | 66 | 65 | 8 | 98 | 99 | 10 |
| 33 | 23 | 4 | 67 | 48842 | 5967 | 99 | 10 | 1 |
| 34 | 35 | 6 | 68 | 33 | 4 | 101 | 201 | 20 |
| 35 | 6 | 1 | 69 | 7775 | 936 | 102 | 101 | 10 |
| 37 | 73 | 12 | 70 | 251 | 30 | 103 | 227528 | 22419 |

*Solution.* The first triple is $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$, which suggests considering the triples $x^2 - 1$, $x^2$, $x^2 + 1$.

Consider the Pell's equation $x^2 - 2y^2 = 1$, whose solutions are

$$x_n = \frac{1}{2}\Big[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n\Big], \quad y_n = \frac{1}{2\sqrt{2}}\Big[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n\Big],$$

$n \geq 1$. The triples $(x_n^2 - 1, x_n^2, x_n^2 + 1)$ satisfy $x_n^2 - 1 = y_n^2 + y_n^2$, $x_n^2 = x_n^2 + 0^2$, $x_n^2 + 1 = x_n^2 + 1^2$, $n \geq 1$.

**Remark.** In a similar way, we can prove that for any nonsquare positive integer $m \geq 2$ there are infinitely many $(m+1)$-tuples of consecutive positive integers each of which is a sum of $m$ squares.

Indeed, the Pell's equation $x^2 - my^2 = 1$ has solutions $(x_n, y_n)_{n \geq 0}$; hence $(x_n^2 - 1, x_n^2, x_n^2 + 1, \ldots, x_n^2 + m - 1)$ has the desired property for all $n \geq 0$.

**Example 3.** *Prove that there are infinitely many quadruples $(x, y, z, t)$ of positive integers with no common divisor and such that*

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

(Romanian Mathematical Olympiad)

*Solution.* Consider the identity:

$$\Big[1^3 + 2^3 + \cdots + (n-2)^3\Big] + (n-1)^3 + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

and write it in the form

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

It suffices to find positive integers $n$ for which $\frac{n(n+1)}{2}$ is a perfect square.

Let us note that

$$(2n+1)^2 - 2(2x)^2 = 1$$

can be achieved by taking the solutions $(u_k, v_k)$ of the Pell equation $u^2 - 2v^2 = 1$, where $u_1 = 3$, $v_1 = 2$, and $u_k, v_k$ are obtained from the identity

$$(u + \sqrt{2v})^k (u - \sqrt{2v})^k = (u_k + \sqrt{2}v_k)(u_k - \sqrt{2}v_k) = 1.$$

**Remark.** Consider the following identity:

$$(a+1)^4 - (a-1)^4 = 8a^3 + 8a,$$

where $a$ is a positive integer. Take $a = b^3$, where $b$ is an even integer. From the above identity we obtain

$$(b^3+1)^4 = (2b^3)^3 + (2b)^3 + [(b^3-1)^2]^2.$$

Since $b$ is an even number, $b^3 + 1$ and $b^3 - 1$ are odd, and it follows that the numbers $x = 2b^3$, $y = 2b$, $z = (b^3-1)^2$, and $t = b^3 + 1$ have no common divisor greater than 1.

**Example 4.** *Prove that if $m = 2 + 2\sqrt{28n^2+1}$ is an integer for some positive integer $n$, then $m$ is a perfect square.*

(Kürshák Competition)

*Solution.* We start by finding those $n$ for which $m$ is an integer. The pair $\left(\frac{m}{2} - 1, n\right)$ must be a solution of Pell's equation $x^2 - 28y^2 = 1$; whose fundamental solution is $(x_1, y_1) = (127, 24)$; hence

$$\frac{m}{2} - 1 + n\sqrt{28} = (127 + 24\sqrt{28})^k$$

for some positive integer $k$. Now we have

$$m = 2 + (127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k = A^2,$$

where $A = (8 + 3\sqrt{7})^k + (8 - 3\sqrt{7})^k$ is an integer.

**Remark.** Another solution is as follows.

If $2\sqrt{28n^2 + 1} + 2$ is an integer, then $28n^2 + 1 = (2m + 1)^2$ for some nonnegative integer $m$. Then $7n^2 = m(m + 1)$, and since $m$ and $m + 1$ are relatively prime, it follows that either $m = 7s^2$ and $m + 1 = t^2$, or $m = u^2$ and $m + 1 = 7v^2$. The second alternative is not possible, because $u^2 - 7v^2 = -1$ does not have solutions, as can be seen from Theorem 3.4.2. This also follows just by looking mod 7. Thus $m + 1 = t^2$ and

$$2\sqrt{28n^2 + 1} + 2 = 2(2m + 1) + 2 = (2t)^2.$$

**Example 5.** *If $m, n, p$ are positive integers such that*

$$m + n + p - 2\sqrt{mnp} = 1,$$

*then at least one of them is a perfect square.*

(Titu Andreescu, Iurie Boreico)

*Solution.* Write the relation as

$$(m + n + p - 1)^2 = 4mnp$$

and substitute $a = 2m - 1$, $b = 2n - 1$, $c = 2p - 1$. Then

$$(a + b + c + 1)^2 = 2(a + 1)(b + 1)(c + 1),$$

which is equivalent to

$$a^2 + b^2 + c^2 - 2abc = 1.$$

Then

$$(a^2-1)(b^2-1)=(ab-c)^2 \quad \text{and} \quad (b^2-1)(c^2-1)=(bc-a)^2,$$

so there are nonnegative integers $d, u, v$ such that $\sqrt{d} \notin Q$ and

$$a^2-1=du^2, \quad b^2-1=dv^2, \quad c^2-1=dw^2,$$

$$|ab-c|=duv \quad \text{and} \quad |bc-a|=dvw.$$

Let $(x_1, y_1)$ be the fundamental solution to Pell's equation $x^2 - dy^2 = 1$ and let $s = x_1 + y_1\sqrt{d}$. Then according to (3.2.6), all solutions to this equation are $(x_k, y_k)$, $k \geq 0$, where

$$x_k=\frac{1}{2}\left(s^k+\frac{1}{s^k}\right), \quad y_k=\frac{1}{2\sqrt{d}}\left(s^k-\frac{1}{s^k}\right).$$

Hence

$$a=\frac{1}{2}\left(s^{k_1}+\frac{1}{s^{k_1}}\right), \quad b=\frac{1}{2}\left(s^{k_2}+\frac{1}{s^{k_2}}\right), \quad c=\frac{1}{2}\left(s^{k_3}+\frac{1}{s^{k_3}}\right)$$

for some nonnegative integers $k_1, k_2, k_3$.

Suppose $m \geq n \geq p$. Then $k_1 \geq k_2 \geq k_3$ and $ab - c = duv$, implying

$$\begin{aligned} c &= ab-duv \\ &= \frac{1}{4}\left(s^{k_1}+\frac{1}{s^{k_1}}\right)\left(s^{k_2}+\frac{1}{s^{k_2}}\right)-\frac{1}{4}\left(s^{k_1}-\frac{1}{s^{k_1}}\right)\left(s^{k_2}-\frac{1}{s^{k_2}}\right) \\ &= \frac{1}{2}\left(s^{k_1-k_2}+\frac{1}{s^{k_1-k_2}}\right). \end{aligned}$$

It follows that $k_3 = k_1 - k_2$, and so at least one of the numbers $k_1, k_2, k_3$ is even. Suppose $k_1$ is even. Then

$$m=\frac{a+1}{2}=\left[\frac{1}{2}\left(s^{\frac{k_1}{2}}+\frac{1}{s^{\frac{k_1}{2}}}\right)\right]^2.$$

**Remarks.** (1) From the above proof it follows that all positive integer solutions to the equation

$$x + y + z - 2\sqrt{xyz} = 1$$

are

$$x = \frac{1}{2}\left(s^{k_1} + \frac{1}{s^{k_1}}\right), \quad y = \frac{1}{2}\left(s^{k_2} + \frac{1}{s^{k_2}}\right), \quad z = \frac{1}{2}\left(s^{k_3} + \frac{1}{s^{k_3}}\right),$$

where $s = u_1 + v_1\sqrt{d}$, $(u_1, v_1)$ is the fundamental solution to the equation $u^2 - dv^2 = 1$, $\sqrt{d} \notin \mathbb{Q}$, and $k_1, k_2, k_3$ are positive integers such that one of them is the sum of the other two.

(2) Another solution is as follows.

Suppose there is a counterexample, and choose the counterexample $(m, n, p)$ with the least $m + n + p$. We may assume, without loss of generality, that $m \geq n \geq p$.

**Case (a).** $m > n + p - 1$. The equation

$$(m + n + p - 1)^2 = 4mnp$$

is a quadratic equation in $m$, with leading coefficient 1; hence it has another integer solution

$$m' = 4np - 2n - 2p + 2 - m = \frac{(n + p - 1)^2}{m},$$

from Viéte's relations. Since $m > n + p - 1$, it follows that $m' < m$ and, $m'$ is not a perfect square, since $m$ is not. Then $(m', n, p)$ is a counterexample with a smaller sum, contradiction.

**Case (b).** $m = n + p - 1$. By substituting we get

$$4(n + p - 1)^2 = 4np(n + p - 1),$$

so $np = n + p - 1$. It follows that $(n-1)(p-1) = 0$; hence either $n$ or $p$ is 1, which is a perfect square, contradiction.

**Case (c).** $m < n + p - 1$. Consider the function

$$f(x) = (x + n + p - 1)^2 - 4xnp$$

on the interval $[1, n + p - 1)$. Its derivative is

$$2(x+n+p-1) - 4np < 2(2n+2p-2) - 4np = -4(n-1)(p-1) < 0$$

(since $n > 1$, $p > 1$, since $n, p$ are not perfect squares). So $f$ is strictly decreasing, and then

$$\begin{aligned} 0 = f(m) < f(n+p-1) &= 4(n+p-1)^2 - 4np(n+p-1) \\ &= -4(n-1)(p-1)(n+p-1) < 0, \end{aligned}$$

contradiction.

**Example 6.** *Let $m, n, p$ be positive integers such that*

$$m + n + p - 2\sqrt{mnp} = 1.$$

*Prove that at least one of the following is true*

$$m \mid (n+p-1)^2, \quad n \mid (p+m-1)^2, \quad p \mid (m+n-1)^2.$$

(Titu Andreescu, Iurie Boreico)

*Solution.* From Example 5, at least one of the numbers $m, n, p$ is a perfect square, say $p = q^2$. Then from

$$(m + n + p - 1)^2 = 4mnp$$

it follows that

$$\left(\frac{m+n-1}{q} + 1\right)^2 = 4mn;$$

hence $q \mid m+n-1$ and the conclusion follows.

**Remarks. 1.** If $m$ and $n$ are positive integers such that there is a nonzero integer $k$ for which

$$(m+n+k^2)^2 = 4(k^2+1)mn,$$

then exactly one of the integers $m$ and $n$ is a perfect square.

**2.** An easier solution to this problem that proves more is to note that the equation $m+n+p-2\sqrt{mnp}=1$ gives

$$\begin{aligned}(n+p-1)^2 &= (m-2\sqrt{mnp})^2 = m(\sqrt{m}-2\sqrt{np})^2 \\ &= m[m-2(m+n+p-1)+4np];\end{aligned}$$

hence $m \mid (n+p-1)^2$, and similarly the other two assertions also hold.

## Exercises and Problems

**1.** Find all positive integers $n$ such that $\frac{n(n+1)}{3}$ is a perfect square.

(Dorin Andrica)

**2.** Find all triangles having side lengths that are consecutive integers and area also an integer.

**3.** Prove that there are infinitely many triples $(a,b,c)$ of positive integers such that the greatest common divisor of $a$, $b$, and $c$ is 1, and $a^2b^2+b^2c^2+c^2a^2$ is the square of an integer.

**4.** Prove that there are infinitely many positive integers $n$ such that $\lceil\sqrt{2}n\rceil$ is a perfect square.

**5.** Prove that there are infinitely many triples $(a,b,c)$ of integers such that

$$a^4+b^3=c^2$$

and $\gcd(a, c) = 1$.

**6.** Solve in positive integers the equation

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

**7.** Let $a_0 = 0$, $a_1 = 4$, and $a_{n+1} = 18a_n - a_{n-1}$, $n \geq 1$. Prove that $5a_n^2 + 1$ is a perfect square for all $n$.

**8.** Prove that if the difference of two consecutive cubes is $n^2$, then $2n - 1$ is a square.

**9.** Consider the system of equations

$$\begin{cases} x + y = z + u, \\ 2xy = zu. \end{cases}$$

Find the largest value of the real constant $m$ such that $m \leq \frac{x}{y}$ for any positive integral solution $(x, y, z, u)$ of the system, with $x \geq y$.

(42nd IMO Shortlist)

**10.** Prove that the equation $x^2 - Dy^4 = 1$ has no positive integer solution if $D \not\equiv 0, 3, 8, 15 \pmod{16}$ and there is no factorization $D = pq$, where $p > 1$ is odd, $\gcd(p, q) = 1$, and either $p \equiv \pm 1 \pmod{16}$, $p \equiv q \pm 1 \pmod{16}$, or $p \equiv 4q \pm 1 \pmod{16}$.

## 3.3 The Equation $ax^2 - by^2 = 1$

In the present section we will study the more general equation

$$ax^2 - by^2 = 1, \tag{3.3.1}$$

where $a$ and $b$ are positive integers. Taking into account the considerations in Section 3.1, we have $\Delta = 4ab > 0$; hence (3.3.1) can be reduced to a Pell's equation.

**Proposition 3.3.1.** *If $ab = k^2$, where $k$ is an integer greater than 1, then equation (3.3.1) does not have solutions in positive integers.*

*Proof.* Assume that (3.3.1) has a solution $(x, y)$, where $x, y$ are positive integers. Then $ax^2 - by^2 = 1$, and clearly $a$ and $b$ are relatively prime. From the condition $ab = k^2$ it follows that $a = k_1^2$ and $b = k_2^2$ for some positive integers $k_1$ and $k_2$. The relation $k_1^2x^2 - k_2^2y^2 = 1$ can be written as $(k_1x - k_2y)(k_1x + k_2y) = 1$. It follows that

$$1 < k_1x + k_2y = k_1x - k_2y = 1,$$

a contradiction. □

We will call the equation

$$u^2 - abv^2 = 1 \tag{3.3.2}$$

*Pell's resolvent* of (3.3.1).

**Theorem 3.3.2.** *Suppose that equation (3.3.1) has solutions in positive integers and let $(x_0, y_0)$ be its minimal solution, i.e., the one with the least $y_0 > 0$. The general solution to (3.3.1) is $(x_n, y_n)_{n\geq 0}$, where*

$$x_n = x_0u_n + by_0v_n, \quad y_n = x_0u_n + ay_0v_n, \tag{3.3.3}$$

*and $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's resolvent (3.3.2).*

*Proof.* We will prove first that $(x_n, y_n)$ is a solution to equation (3.3.1). Indeed,

$$\begin{aligned} ax_n^2 - by_n^2 &= a(x_0u_n + by_0v_n)^2 - b(y_0u_n + ax_0v_n)^2 \\ &= (ax_0^2 - by_0^2)(u_n^2 - abv_n^2) = 1 \cdot 1 = 1. \end{aligned}$$

Conversely, let $(x, y)$ be a solution to equation (3.3.1). Then $(u, v)$, where $u = ax_0x - by_0y$ and $v = y_0x - x_0y$, is a solution to Pell's

resolvent (3.3.2). Solving the above system of linear equations with unknowns $x$ and $y$ yields $x = x_0u + by_0v$ and $y = y_0u + ax_0v$, i.e., $(x, y)$ has the form (3.3.3). □

**Remarks.** (1) A simple algebraic computation yields the following relation between the fundamental solution $(u_1, v_1)$ to Pell's resolvent and the smallest solution $(x_0, y_0)$ to equation (3.3.1), in case of solvability:

$$u_1 \pm v_1\sqrt{ab} = \left(x_0\sqrt{a} \pm y_0\sqrt{b}\right)^2,$$

where the signs + and − correspond.

(2) Using formulas (3.2.6), from (3.3.3) it follows that

$$\begin{aligned} x_n &= \frac{1}{2}\left(x_0 + \frac{y_0}{a}\sqrt{ab}\right)\left(u_1 + v_1\sqrt{ab}\right)^n \\ &\quad + \frac{1}{2}\left(x_0 - \frac{y_0}{a}\sqrt{ab}\right)\left(u_1 - v_1\sqrt{ab}\right)^n \\ y_n &= \frac{1}{2}\left(y_0 + \frac{x_0}{b}\sqrt{ab}\right)\left(u_1 + v_1\sqrt{ab}\right)^n \\ &\quad + \frac{1}{2}\left(y_0 - \frac{x_0}{a}\sqrt{ab}\right)\left(u_1 - v_1\sqrt{ab}\right)^n \end{aligned} \tag{3.3.4}$$

Taking into account Remark 1, the above formulas can be written as

$$\begin{aligned} x_n &= \frac{1}{2\sqrt{a}}\left[\left(x_0\sqrt{a} + y_0\sqrt{b}\right)^{2n+1} + \left(x_0\sqrt{a} - y_0\sqrt{b}\right)^{2n+1}\right], \\ y_n &= \frac{1}{2\sqrt{b}}\left[\left(x_0\sqrt{a} + y_0\sqrt{b}\right)^{2n+1} - \left(x_0\sqrt{a} - y_0\sqrt{b}\right)^{2n+1}\right]. \end{aligned}$$

(3) The general solution (3.3.3) can be written in the following matrix form:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_0 & by_0 \\ y_0 & ax_0 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$
$$= \begin{pmatrix} x_0 & by_0 \\ y_0 & ax_0 \end{pmatrix} \begin{pmatrix} u_1 & abv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}.$$

**Example 1.** *Solve in positive integers the equation*

$$6x^2 - 5y^2 = 1.$$

*Solution.* Its minimal solution is $(x_0, y_0) = (1, 1)$. The Pell's resolvent is $u^2 - 30v^2 = 1$, whose fundamental solution is $(11, 2)$. The general solution to the equation considered is $x_n = u_n + 5v_n$, $y_n = u_n + 6v_n$, $n = 0, 1, \ldots$, where $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's resolvent, i.e., $u_{n+1} = 11u_n + 60v_n$, $v_{n+1} = 2u_n + 11v_n$, $n = 0, 1, \ldots$, with $u_1 = 11$, $v_1 = 2$.

A closed form for these solutions can be found using the formulas (3.3.4). We obtain

$$x_n = \frac{6+\sqrt{30}}{12}(11+2\sqrt{30})^n + \frac{6-\sqrt{30}}{12}(11-2\sqrt{30})^n,$$
$$y_n = \frac{5+\sqrt{30}}{10}(11+2\sqrt{30})^n + \frac{5-\sqrt{30}}{10}(11-2\sqrt{30})^n.$$

**Example 2.** *Find all positive integers $n$ such that $2n+1$ and $3n+1$ are perfect squares.*

(American Mathematical Monthly)

*Solution.* Let $2n + 1 = x^2$ and $3n + 1 = y^2$. Multiply the first equation by 3 and the second by 2 and subtract them to obtain

$$3x^2 - 2y^2 = 1. \tag{3.3.6}$$

The smallest solution to this equation is $x = y = 1$. Its Pell's resolvent is $u^2 - 6v^2 = 1$, with the fundamental solution $(u_1, v_1) = (5, 2)$. From Theorem 3.3.2, the general solution to equation (3.3.6) is given by $x_m = u_m + 2v_m,\ y_m = u_m + 3v_m,\ m \geq 0$, where

$$u_m = \frac{1}{2}\Big[(5 + 2\sqrt{6})^m + (5 - 2\sqrt{6})^m\Big],$$
$$v_m = \frac{1}{2\sqrt{6}}\Big[(5 + 2\sqrt{6})^m - (5 - 2\sqrt{6})^m\Big].$$

We obtain

$$n = y_m^2 - x_m^2 = (u_m + 3v_m)^2 - (u_m + 2v_m)^2 = v_m(2u_m + 5v_m), \quad m \geq 0.$$

**Example 3.** *Let $a$ and $b$ be square-free positive integers such that both equations $ax^2 - by^2 = \pm 1$ are solvable. Prove that at least one of $a$ and $b$ is 1.*

*Solution.* Suppose $au^2 - bv^2 = 1$ and $ax^2 - by^2 = -1$ for some positive integers $u, v, x$, and $y$. Clearly, $\gcd(a, b) = 1$. Let $z = uy - vx$. We have $v^2x^2 = (uy - z)^2$, hence $(bv^2)(ax^2) = ab(uy - z)^2$. Because $bv^2 = au^2 - 1$ and $ax^2 = by^2 - 1$, we obtain $(au^2 - 1)(by^2 - 1) = ab(uy - z)^2$, that is, $abu^2y^2 - au^2 - by^2 + 1 = abu^2y^2 - 2abuyz + abz^2$. It follows that $au^2 + by^2 + abz^2 - 1 = 2abuyz$. For $m = au^2$, $n = by^2$, $p = abz^2$, we get $m + n + p - 1 = 2\sqrt{mnp}$. Using the result in Example 5 in Section 3.2, at least one of the integers $m = au^2$, $n = by^2$, $p = abz^2$ is a perfect square, that is, at least one of $a$, $b$, $ab$ is a square. Because $a$ and $b$ are square-free and $\gcd(a, b) = 1$, it follows that $a = 1$ or $b = 1$.

## Exercises and Problems

**1.** Prove that there are infinitely many quadruples $(x, y, u, v)$ of positive integers such that $x^2 + y^2 = 6(z^2 + w^2) + 1$, $3 \mid x$, and $2 \mid y$.

(Dorin Andrica)

**2.** (a) Find all positive integers $n$ such that $n + 1$ and $3n + 1$ are simultaneously perfect squares.

(b) If $n_1 < n_2 < \cdots < n_k < \cdots$ are all positive integers satisfying the above property, then $n_k n_{k+1} + 1$ is also a perfect square, $k = 1, 2, \ldots$.

(American Mathematical Monthly)

**3.** Prove that there exist two strictly increasing sequences $(a_n)$ and $(b_n)$ of positive integers such that $a_n(a_n + 1)$ divides $b_n^2 + 1$ for all $n \geq 1$.

(40th IMO Shortlist)

**4.** Let $x$ and $y$ be positive integers such that $x(y+1)$ and $y(x+1)$ are perfect squares. Prove that either $x$ or $y$ is a perfect square.

(Titu Andreescu, Iurie Boreico)

## 3.4 The Negative Pell's Equation

While Pell's equation $x^2 - dy^2 = 1$ is always solvable if the positive integer $d$ is not a perfect square, the equation

$$x^2 - dy^2 = -1 \tag{3.4.1}$$

is solvable only for certain values of $d$. It is an equation of the form $ax^2 - by^2 = 1$, where $a = d$, $b = 1$.

Next, we will find the solutions to equation (3.4.1) using the method outlined in Section 3.3.

Equation (3.4.1) is known as a *negative Pell's equation*. From Theorem 3.3.2 the following result follows:

**Theorem 3.4.1.** *Suppose that equation (3.4.1) has solutions in positive integers and let $(x_0, y_0)$ be its minimal solution. The general solution to (3.4.1) is given by $(x_n, y_n)_{n\geq 0}$, where*

$$x_n = x_0u_n + dy_0v_n, \quad y_n = y_0u_n + x_0v_n, \tag{3.4.2}$$

*and $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's equation $u^2 - dv^2 = 1$.*

**Remarks.** (1) Using formulas (3.4.2) we obtain the solutions to the negative Pell's equation in explicit form:

$$\begin{aligned} x_n &= \frac{1}{2}(x_0 + y_0\sqrt{d})(u_1 + v_1\sqrt{d})^n \\ &\quad + \frac{1}{2}(x_0 - y_0\sqrt{d})(u_1 - v_1\sqrt{d})^n \\ y_n &= \frac{1}{2}\left(y_0 + \frac{x_0}{\sqrt{d}}\right)(u_1 + v_1\sqrt{d})^n \\ &\quad + \frac{1}{2}\left(x_0 - \frac{y_0}{\sqrt{d}}\right)(u_1 - v_1\sqrt{d})^n. \end{aligned} \tag{3.4.3}$$

(2) The matrix form of solution is

$$\begin{aligned} \begin{pmatrix} x_n \\ y_n \end{pmatrix} &= \begin{pmatrix} x_0 & dy_0 \\ y_0 & x_0 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix} \\ &= \begin{pmatrix} x_0 & dy_0 \\ y_0 & x_0 \end{pmatrix} \begin{pmatrix} u_1 & dv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \end{aligned}$$

(3) The sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ given by (3.4.2) or (3.4.3) satisfy the identity

$$x_n = [y_n\sqrt{d}]. \tag{3.4.4}$$

Indeed, $x_n^2 - dy_n^2 = -1$ implies $(y_n\sqrt{d}+x_n)(y_n\sqrt{d}-x_n) = 1$. Since $y_n\sqrt{d} + x_n > 1$, it follows that $0 < y_n\sqrt{d} - x_n < 1$; hence (3.4.4) holds.

**Theorem 3.4.2.** *Let $p$ be a prime. The negative Pell's equation*

$$x^2 - py^2 = -1$$

*is solvable if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

*Proof.* If the considered equation has a solution $(x, y)$, then $p \mid x^2 + 1$. Hence either $p = 2$ or $p \equiv 1 \pmod 4$.

For $p = 2$, $x = y = 1$ is a solution. We show that there is a solution for each prime $p = 4t + 1$. A natural starting point is the existence of an integral solution $(x_0, y_0)$ to the corresponding Pell's equation: $x_0^2 - py_0^2 = 1$. We observe that $x_0$ is odd: otherwise, $y_0^2 \equiv py_0^2 \equiv 3 \pmod 4$. Thus in the relation

$$x_0^2 - 1 = (x_0 - 1)(x_0 + 1) = py_0^2,$$

factors $x_0 + 1$ and $x_0 - 1$ have greatest common divisor 2, and consequently one of them is a doubled square (to be denoted by $2x^2$) and the other one $2p$ times a square (to be denoted by $2py^2$). The case $x_0 + 1 = 2x^2$, $x_0 - 1 = 2py^2$ is impossible because it leads to a smaller solution of Pell's equation: $x^2 - py^2 = 1$. It follows that

$$x_0 - 1 = 2x^2, \quad x_0 + 1 = 2py^2,$$

and therefore $x^2 - py^2 = -1$. □

In case of solvability, the main method of determining the fundamental solution to negative Pell's equation (3.4.1) involves continued fractions. The following table contains the fundamental solutions, in case of solvability, for $d \leq 101$.

| $d$ | $A$ | $B$ | $d$ | $A$ | $B$ | $d$ | $A$ | $B$ |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 37 | 6 | 1 | 73 | 1068 | 125 |
| 5 | 2 | 1 | 41 | 32 | 5 | 74 | 43 | 5 |
| 10 | 3 | 1 | 50 | 7 | 1 | 82 | 9 | 1 |
| 13 | 18 | 5 | 53 | 182 | 25 | 85 | 378 | 41 |
| 17 | 4 | 1 | 58 | 99 | 13 | 89 | 500 | 53 |
| 26 | 5 | 1 | 61 | 29718 | 3805 | 97 | 5604 | 569 |
| 29 | 70 | 13 | 65 | 8 | 1 | 101 | 10 | 1 |

**Example 1.** *Show that the equation*

$$x^2 - 34y^2 = -1$$

*is not solvable.*

*Solution.* The fundamental solution of Pell's resolvent is $(35, 6)$. If the equation $x^2 - 34y^2 = -1$ were solvable and had the fundamental solution $(A, B)$, then $(A + B\sqrt{34})^2 = 35 + 6\sqrt{34}$, i.e., $A^2 + 34B^2 = 35$ and $2AB = 6$. But this system of equations has no solutions in positive integers, and thus our equation is not solvable.

**Example 2.** *Find all pairs of positive integers* $(k, m)$ *such that* $k < m$ *and*

$$1 + 2 + \cdots + k = (k + 1) + (k + 2) + \cdots + m.$$

(College Mathematics Journal)

*Solution.* Adding $1+2+\cdots+k$ to both sides, we get $2k(k+1) = m(m+1)$, which can be rewritten as

$$(2m+1)^2 - 2(2k+1)^2 = -1.$$

The negative Pell's equation $x^2 - 2y^2 = -1$ has $(1,1)$ as its least positive solution. From (3.4.2), its general solution $(x_n, y_n)$ is given by

$$x_n = u_n + 2v_n, \quad y_n = u_n + v_n, \quad n \geq 0,$$

where

$$\begin{aligned} u_n &= \frac{1}{2}\Big[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n\Big], \\ v_n &= \frac{1}{2\sqrt{2}}\Big[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n\Big], \quad n \geq 0. \end{aligned}$$

Then

$$\begin{aligned} x_n &= \frac{1}{2}\Big[(1+\sqrt{2})^{2n-1} + (1-\sqrt{2})^{2n-1}\Big], \\ y_n &= \frac{1}{2\sqrt{2}}\Big[(1+\sqrt{2})^{2n-1} - (1-\sqrt{2})^{2n-1}\Big], \quad n \geq 1. \end{aligned}$$

Since $x^2 - 2y^2 = -1$ implies that $x^2$ is odd, $x$ is of the form $2l+1$. Then $y^2 = 2l^2 + 2l + 1$ implies that $y$ is odd.

The desired pairs are

$$(k,m) = \left(\frac{y_n - 1}{2}, \frac{x_n - 1}{2}\right), \quad n \geq 2.$$

## Exercises and Problems

**1.** Find all pairs $(x,y)$ of positive integers satisfying the equation

$$x^2 - 6xy + y^2 = 1.$$

(Titu Andreescu)

**2.** Prove that there are infinitely many positive integers $n$ such that $n^2+1$ divides $n!$.

(Kvant)

**3.** Let $a_n = \left[\sqrt{n^2+(n+1)^2}\right]$, $n \geq 1$. Prove that there are infinitely many $n$'s such that $a_n - a_{n-1} > 1$ and $a_{n+1} - a_n = 1$.

**4.** Let $k$ be an integer greater than 2. Prove that

$$x^2 - (k^2-4)y^2 = -1$$

is solvable if and only if $k = 3$.

**5.** Prove that if $\frac{a^2+1}{b^2} + 4$ is a perfect square, then this square is 9.

**6.** Find all pairs $(m, n)$ of integers such that $mn+m$ and $mn+n$ are both squares.

(Titu Andreescu, Iurie Boreico)

# I.4

# Some Advanced Methods for Solving Diophantine Equations

A *field* is a set $k$ equipped with two commutative binary operations, addition and multiplication, such that

- $(k, +)$ is an abelian group under addition;
- every nonzero element of $k$ has a multiplicative inverse, and $(k^*, \cdot)$ is an abelian group under multiplication, where $k^* = k \setminus \{0_k\}$;
- $0_k \neq 1_k$;
- the distributive law holds: $(a + b)c = ac + bc$ for all $a, b, c \in k$.

Standard examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ for $p$ prime.

A *commutative ring* is just like a field except that not every nonzero element need have a multiplicative inverse. Examples of commutative rings are $\mathbb{Z}$, $\mathbb{Z}_n$ (the set of residues modulo $n$), $k[x]$ (the set of all polynomials with coefficients in the field $k$).

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, 147
DOI 10.1007/978-0-8176-4549-6_4, © Springer Science+Business Media, LLC 2010

An element of a ring $R$ with a multiplicative inverse is called a *unit*. The set of units of $R$, denoted by $R^*$, is a multiplicative group under the multiplication of $R$. For the previous examples of commutative rings we have

$$\mathbb{Z}^* = \{-1, 1\}, \quad \mathbb{Z}_n^* = \{\widehat{a} \in \mathbb{Z}_n : \ \gcd(a, n) = 1\}, \quad k[x]^* = k \setminus \{0_F\}$$

for $k$ a field.

A *zero-divisor* of a ring $R$ is a nonzero element $r \in R$ such that $rs = 0$ for some nonzero $s \in R$. A commutative ring without zero-divisors is called an *integral domain*. A few examples of rings with zero-divisors are $\mathbb{Z}_n$ for $n$ not prime (for example in $\mathbb{Z}_6$, $\widehat{2} \cdot \widehat{3} = \widehat{0}$). A noncommutative example is in $M_2(\mathbb{Q})$, where, for example,

$$\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Any element that is a unit of a ring will never be a zero-divisor. Examples of integral domains are any field, $\mathbb{Z}$, $k[x]$ where $k$ is any field.

The ring $R$ is called *Euclidean domain* (ED) if there exists a function $\lambda : R - \{0\} \to \mathbb{N}^0$ with the following property: for any two $a, b \in R$, $b \neq 0$, one can find some $c, d \in R$ such that $a = cb + d$ and either $d = 0$, or $\lambda(d) < \lambda(b)$.

For example, the rings $\mathbb{Z}$ and $k[x]$ ($k$ a field) are both Euclidean domains: for $\lambda$ take the absolute value in $\mathbb{Z}$, or the degree of polynomials in $k[x]$.

An *ideal* $I$ of a ring $R$ is a subset of $R$ closed under addition, subtraction, and multiplication by elements of $R$: if $x, y \in I$ and

$r \in R$, then $x + y, x - y, rx \in R$. In other words, $I$ is a subset of $R$ that is an $R$-module, called also an *$R$-submodule*. Further, an ideal $I$ is *principal* if it generated by one element as an $R$-module: for some $a \in I$, $I = \{ra \mid r \in R\}$. We write $I = (a)$.

In a Euclidean domain $R$ every ideal is principal.

A ring $R$ is a *principal ideal domain* (PID) if every ideal in it is principal.

Thus, every ED is also a PID.

For a ring $R$, $a, b \in R$ are *associated* if $a = ub$ for some unit $u \in R$. An element $p \in R$ is *irreducible* if $a \mid p$ implies that $a$ is a unit or $a$ is associated with $p$. A nonunit $p \in R$ is *prime* if $p \neq 0$ and $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Note that irreducible and prime elements do *not* always coincide in rings, but they do so in PIDs, where these notions can be translated easily into the language of ideals.

We similarly defined *greatest common divisors* for two or more elements of $R$. It is *not* true that these exist in arbitrary rings, but they do in PIDs: if $a, b \in R$, then $\gcd(a, b)$ is an element $d$ such that $(a, b) = (d)$.

Finally, two elements are relatively prime if $\gcd(a, b) = 1$. In PIDs this means that $a$ and $b$ generate the whole ring $R$.

In PIDs, the notions of prime and irreducible elements are equivalent.

In a PID $R$, any increasing sequence of ideals eventually stabilizes. Consequently, for any prime element $p$ and any $a \in R$, $a \neq 0$, there is a unique nonnegative integer $n$ such that $p^n \mid a$ but $p^{n+1} \nmid a$.

This $n$ is called the *order* of $p$ in $a$, denoted by $n = \mathrm{ord}_p a$. Note that for any $a, b \neq 0$, $\mathrm{ord}_p ab = \mathrm{ord}_p a + \mathrm{ord}_p b$. Here follows the main theorem of this section, stating that any every is a *unique factorization domain* (UFD). For this, note that a PID can be thought of as a disjoint union of subsets of associated elements. If one element in a subset is prime, then *all* of its associates are also prime. From each such subset consisting of prime elements we choose one representative, and we denote the set of such representatives by $S$.

We have the following important result:

**Theorem.** *Let $R$ be a PID, and let $S$ be a set of representatives of all subsets of associated prime elements in $R$. Then for every $a \in R$, $a \neq 0$,*

$$a = u \prod_p p^{e(p)},$$

*where $u$ is a unit in $R$, and the product is taken over all elements $p \in S$. This factorization is unique up to the choice of $S$ (up to units), and the exponents are uniquely defined by $e(p) = \mathrm{ord}_p a$.*

Note that ED $\Rightarrow$ PID $\Rightarrow$ UFD, but the opposite implications are not true. It is hard to find counterexamples of rings that are PIDs but not EDs. However, consider any ring of polynomials over any field $k$ in more than one variable: $k[x, y]$. This is evidently a UFD, but is certainly not a PID: the ideal generated by the two variables $(x, y)$ is not principal. Further, do not get the wrong idea that *all* rings are UFDs!

You will see some examples in Section 4.2.

## 4.1 The Ring $\mathbb{Z}[i]$ of Gaussian Integers

A *Gaussian integer* is a complex number whose real part and imaginary part are both integers. The Gaussian integers, with ordinary addition and multiplication of complex numbers, form an integral domain, usually denoted by $\mathbb{Z}[i]$. This domain cannot be turned into an ordered ring, since it contains a square root of $-1$. Formally, the set of Gaussian integers is

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

For $\alpha = a + bi$ in $\mathbb{Z}[i]$, set the norm of $\alpha$ to be

$$N(\alpha) = a^2 + b^2,$$

which is a nonnegative integer. This norm is multiplicative ($N(\alpha\beta) = N(\alpha)N(\beta)$) and it gives a measure of the size of elements. For an integer $a \in \mathbb{Z}$, its norm is its square: $N(a) = a^2$. In particular, $N(1) = 1$.

**Theorem 4.1.1.** *The units in $\mathbb{Z}[i]$ are 1, $-1$, $i$, and $-i$, namely the elements of norm 1.*

*Proof.* Because $1 \cdot 1 = 1$, $(-1)(-1) = 1$, and $i(-i) = 1$, these four elements are all units in $\mathbb{Z}[i]$. Conversely, if $u$ is a unit in $\mathbb{Z}[i]$ then $uv = 1$ for some $v$ in $\mathbb{Z}[i]$. Taking the norm of both sides yields $N(u)N(v) = 1$. This last equation is in the positive integers, so $N(u)$ and $N(v)$ both must be 1. Writing $u = a + bi$, we have $a^2 + b^2 = 1$. The only solutions to this in integers are $(a, b) = (\pm 1, 0)$ and $(0, \pm 1)$, which yield the four numbers 1, $-1$, $i$, and $-i$. □

A global way of writing the units in $\mathbb{Z}[i]$ is $i^k$, $k = 0, 1, 2, 3$.

Like $\mathbb{Z}$, there is a division theorem in $\mathbb{Z}[i]$. To measure the size of a remainder under division, we use the norm:

**Theorem 4.1.2.** *For any $\alpha$ and $\beta$ in $\mathbb{Z}[i]$ with $\beta \neq 0$, there are $\gamma$ and $\rho$ in $\mathbb{Z}[i]$ such that*

$$\alpha = \beta\gamma + \rho, \quad N(\rho) \leq \frac{1}{2}N(\beta) < N(\beta).$$

*Proof.* The norm on $\mathbb{Z}[i]$ is closely related to the absolute value on $\mathbb{C}$: $N(a+bi) = |a+bi|^2$. The absolute value on $\mathbb{C}$ is our way of measuring distances in $\mathbb{C}$, and we will take advantage of this.

In $\mathbb{C}$, the farthest a complex number can be from an element of $\mathbb{Z}[i]$ is $1/\sqrt{2}$, since the center points of $1 \times 1$ squares with vertices in $\mathbb{Z}[i]$ are at distance $1/\sqrt{2}$ from the vertices. Now consider the ratio $\alpha/\beta$ as a complex number and place it in a $1 \times 1$ square having vertices in $\mathbb{Z}[i]$. Let $\gamma \in \mathbb{Z}[i]$ be the vertex of the square that is nearest to $\alpha/\beta$, so $|\alpha/\beta - \gamma| \leq 1/\sqrt{2}$. Multiplying through by $|\beta|$, we obtain $|\alpha - \beta\gamma| \leq (1/\sqrt{2})|\beta|$. Squaring both sides and recalling that the squared complex absolute value on $\mathbb{Z}[i]$ is the norm, we obtain

$$N(\alpha - \beta\gamma) \leq \frac{1}{2}N(\beta).$$

Now set $\rho = \alpha - \beta\gamma$. □

**Remark.** Unlike the situation in $\mathbb{Z}$, the quotient and remainder in $\mathbb{Z}[i]$ are not unique. For example, take $\alpha = 37+2i$ and $\beta = 11+2i$. You can check that

$$\alpha = \beta \cdot 3 + (4 - 4i), \quad \alpha = \beta(3 - i) + (2 + 7i).$$

Here both remainders have norm less than $N(\beta) = 125$ (in fact, less than $125/2$). The proof of Theorem 4.1.2 explains geometrically

why the quotient and remainder in $\mathbb{Z}[i]$ are not unique: $\alpha/\beta$ is closer to two vertices in the $1 \times 1$ square containing it than the length of a (half-)diagonal of the square.

This lack of uniqueness in the quotient and remainder is not a major drawback, since the main consequence of the division theorem, such as Euclid's algorithm and unique factorization, do not actually use the uniqueness. The main thing is just having the remainder less (by some measure) than the divisor, and that is what Theorem 4.1.2 says.

**Corollary 4.1.3.** *The ring $\mathbb{Z}[i]$ has unique factorization, and in fact is a principal ideal domain.*

*Proof.* Every domain having a division theorem is a PID and a UFD, by the same proof as in $\mathbb{Z}$. □

Here are some examples of primes in $\mathbb{Z}[i]$:

$$1+i, \quad 3, \quad 1+2i, \quad 1-2i, \quad 7, \quad 11, \quad 2+3i, \quad 2-3i.$$

Note that 2 and 5 are not here, because they are not prime in $\mathbb{Z}[i]$:

$$2 = (1+i)(1-i) \quad \text{and} \quad 5 = (1+2i)(1-2i).$$

**Example 1.** *Using properties of the ring $\mathbb{Z}[i]$ find all Pythagorean triples.*

*Solution.* An elementary approach was featured in Section 2.2. Here we use the uniqueness of the prime factorization in $\mathbb{Z}[i]$.

Suppose that $(x, y, z)$ is a solution to $x^2 + y^2 = z^2$ with $\gcd(x, y) = 1$.

Thus one of $x$ and $y$ is odd and hence $z$ is odd. We can rewrite $x^2 + y^2 = z^2$ in $\mathbb{Z}[i]$ as

$$(x + iy)(x - iy) = z^2. \tag{1}$$

We claim that $\gcd(x + iy, x - iy) = 1$. Indeed, let $d \in \mathbb{Z}[i]$ be irreducible and let $d$ divide $x + iy$ and $x - iy$. Then $d \mid 2x$ and $d \mid 2y$. If $d \mid 2$, this contradicts the fact that $z$ is odd. Hence $d \mid x$ and $d \mid y$. Take norms to conclude that $N(d) \mid x^2$ and $N(d) \mid y^2$. But $\gcd(x, y) = 1$. Hence $x + iy$ and $x - iy$ are relatively prime in $\mathbb{Z}[i]$. Hence $x + iy = u(a + ib)^2$ for some unit $u$ and $a, b \in \mathbb{Z}$. Hence $x + iy = u(a^2 - b^2 + 2abi)$. By taking $u = 1$ we get $x = a^2 - b^2$, $y = 2ab$ and therefore $z = a^2 + b^2$. By taking other values of $u$ we get similar expressions for $x, y, z$.

Conversely, $x = a^2 - b^2$, $y = 2ab$, and $z = a^2 + b^2$ satisfy $x^2 + y^2 = z^2$ for all $a, b \in \mathbb{Z}$. Thus we have found all the Pythagorean triples.

**Example 2.** *Solve the equation*

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

*where $n$ is an integer greater than 1 and $x$, $y$ are relatively prime.*

*Solution.* For $n = 2$, the solutions are the Pythagorean triples discussed extensively in Section 2.2 and Example 1 above. For $n \geq 3$ we use again the uniqueness of prime factorization in the ring $\mathbb{Z}[i]$. We may assume that $x$ and $y$ are relatively prime and write the equation as

$$(x + iy)(x - iy) = z^n.$$

It follows that $\gcd(x + iy, x - iy) = 1$ in $\mathbb{Z}[i]$. Indeed, one easily sees that $\gcd(x + iy, x - iy)$ divides $\gcd(2x, 2y) = 2$. But in $\mathbb{Z}[i]$, the

number $2 = -i(1+i)^2$ is up to units the square of the prime $1+i$, and if $1+i$ divides both factors, then $2 \mid z$ and we get a contradiction mod 8. Hence $x + iy = (a + ib)^n$ for some integers $a$ and $b$ with $a^2 + b^2 = z$. Then $x = A_n$ and $y = B_n$, where

$$A_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n}{2k} a^{n-2k} b^{2k},$$

$$B_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n}{2k+1} a^{n-1-2k} b^{2k+1},$$

and the general solution is given by triples

$$\Big(d^n A_n, d^n B_n, d^2\Big(a^2 + b^2\Big)\Big),$$

where $a, b, d \in \mathbb{Z}$.

The following table contains the first few values of $A_n$ and $B_n$ up to multiplication by an appropriate factor.

| $n$ | $A_n$ | $B_n$ |
|---|---|---|
| 0 | $1$ | $0$ |
| 1 | $a$ | $b$ |
| 2 | $a^2 - b^2$ | $2ab$ |
| 3 | $a^3 - 3ab^2$ | $3a^2b - b^3$ |
| 4 | $a^4 - 6a^2b^2 + b^4$ | $4a^3b - 4ab^3$ |
| 5 | $a^5 - 10a^3b^2 + 5ab^4$ | $5a^4b - 10a^2b^3 + b^5$ |
| 6 | $a^6 - 15a^4b^2 + 15a^2b^4 - b^6$ | $6a^5b - 20a^3b^3 + 6ab^5$ |
| 7 | $a^7 - 21a^5b^2 + 35a^3b^4 - 7ab^6$ | $7a^6b - 35a^4b^3 + 21a^2b^5 - b^7$ |
| 8 | $a^8 - 28a^6b^2 + 70a^4b^4 - 28a^2b^6 + b^8$ | $8a^7b - 56a^5b^3 + 56a^3b^5 - 8ab^7$ |

**Remarks.** (1) The integers $u = a^4 - 6a^2b^2 + b^4$ and $v = a^3b - ab^3$ cannot both be squares of nonzero integers. Indeed, if $u = s^2$ and

$v = t^2$ for some nonzero integers $s$ and $t$, then $s^4 + (2t)^4 = u^2 + (4v)^2 = (a^2 + b^2)^4$, contradicting Fermat's last theorem (see also Corollary 2.3.5).

(2) The integers $u = a^6 - 15a^4b^2 + 15a^2b^4 - b^6$ and $v = 6a^5b - 20a^3b^3 + 6ab^5$ cannot both be cubes of nonzero integers. Indeed, if $u = s^3$ and $v = t^3$, then $s^6 + t^6 = u^2 + v^2 = (a^2 + b^2)^6$, again contradicting Fermat's last theorem.

(3) In general, for $n = 2m$, the integers $A_n$ and $B_n$ cannot both be the $m$th powers of nonzero integers.

**Example 3.** *Solve the equation*

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

*where $n$ is an integer greater than* 1.

*Solution.* (V.A. Lebesgue) For $n$ even, the equation has solutions $(0, 1)$ and $(0, -1)$ only. For $n$ odd, we may assume without loss of generality that $n$ is a prime $p \geq 3$. Indeed, if $n = q \cdot k$, where $q$ is an odd prime, we get an equation of the same type: $x^2 + 1 = (y^k)^q$.

We will use the uniqueness of prime factorization in the Gaussian ring $\mathbb{Z}[i]$.

Clearly, $x$ is even and $y$ is odd. We have $(1 + ix)(1 - ix) = y^p$. Moreover, the integers $1 + ix$ and $1 - ix$ are relatively prime in $\mathbb{Z}[i]$. Indeed, let $z = \gcd(1 + ix, 1 - ix)$, $z = a + bi$. We have $z \mid (1 + ix) + (1 - ix) = 2$; hence $\overline{z} \mid 2$. It follows that $z \cdot \overline{z} \mid 4$, i.e., $a^2 + b^2 \mid 4$. On the other hand, $z \mid 1 + ix$ implies $\overline{z} \mid 1 - ix$, so $a^2 + b^2 \mid 1 + x^2$. But $x$ is even, so $a^2 + b^2$ is odd. Thus $a^2 + b^2 = 1$, implying that $z$ is a unit in $\mathbb{Z}[i]$.

Because $1+ix$ and $1-ix$ are relatively prime, from $(1+ix)(1-ix) = y^p$ it follows that $1 + ix = a(u + iv)^p$, where $a$ is a unit and $u$ and $v$ have different parities. Since $p$ is odd, every unit is a $p$th power and therefore we can drop the unit here; hence we can assume that $1 + ix = (u + iv)^p$. Using the binomial expansion and identifying the real parts, we get

$$1 = u^p - \binom{p}{2}u^{p-2}v^2 + \binom{p}{4}u^{p-4}v^4 - \cdots \pm \binom{p}{p-1}uv^{p-1}.$$

Hence $u \mid 1$, implying $u = \pm 1$, and so $v$ is even. We obtain $u^p \equiv 1 \pmod 4$, and since $p$ is odd, it follows that $u = 1$. Dividing by $v^2 \neq 0$, we get

$$\binom{p}{2} = \binom{p}{4}v^2 - \binom{p}{6}v^4 + \cdots \pm \binom{p}{p-1}v^{p-3}.$$

This is a contradiction, because the exponent of 2 in the left-hand side is less than the exponent of 2 in the right-hand side. Indeed, for $k = 1, 2, \ldots,$ we have

$$\binom{p}{2k}v^{2k-2} = \frac{p(p-1)}{2}\binom{p-2}{2k-2}\frac{2v^{2k-2}}{(2k-1)2k}.$$

In conclusion, for $p \geq 3$, there are no solutions different from the trivial $(0, 1)$.

**Example 4.** *Solve the equation*

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

(Fermat)

*Solution.* Let $x$ be odd. The equation can be written as $(2+ix)(2-ix) = y^3$. We will show that $2 + ix$ and $2 - ix$ are relatively prime in the ring $\mathbb{Z}[i]$. Indeed, let $z = \gcd(2 + ix, 2 - ix)$, $z = c + di$. Then $z$

divides $(2+ix)+(2-ix)=4$ hence; $\overline{z} \mid 4$. It follows that $z\cdot\overline{z}=c^2+d^2$ divides 16. On the other hand, $z \mid 2+ix$ implies $\overline{z} \mid 2-ix$; hence $c^2+d^2 \mid 4+x^2$. But $x$ is odd, so $c^2+d^2=1$, implying that $z$ is a unit in $\mathbb{Z}[i]$.

Because $2+ix$ and $2-ix$ are relatively prime, from $(2+ix)(2-ix)=y^3$ it follows that $2+ix=(a+bi)^3$ for some integers $a$ and $b$. Identifying the real and imaginary parts, we get $a(a^2-3b^2)=2$ and $3a^2b-b^3=x$. The first equation gives $a=\pm 1$ or $a=\pm 2$, yielding $x=\pm 11$ and $y=5$.

If $x$ is even, then $y$ is even. Let $x=2u$ and $y=2v$. The equation becomes $u^2+1=2v^3$, i.e., $(u+i)(u-i)=2v^3$. Because $\gcd(u+i,u-i)=1$ and $2=(1+i)(1-i)$, using again the uniqueness of prime factorization in $\mathbb{Z}[i]$, we obtain

$$u+i=(1+i)(a+bi)^3,$$

for some integers $a$ and $b$.

Identifying the real and imaginary parts, we get

$$a^3-3a^2b-3ab^2+b^3=u \quad \text{and} \quad a^3+3a^2b-3ab^2-b^3=1.$$

The last relation can be written as

$$(a-b)(a^2+4ab+b^2)=1,$$

yielding the systems

$$\begin{cases} a-b=1, \\ a^2+4ab+b^2=1, \end{cases} \quad \text{and} \quad \begin{cases} a-b=-1, \\ a^2+4ab+b^2=-1. \end{cases}$$

The second system has no solutions. Indeed, one can observe that

$$a^2+4ab+b^2=(a+2b)^2-3b^2 \equiv 0,1 \pmod 3.$$

The first system has integer solutions: $(a, b) = (1, 0)$ and $(a, b) = (0, -1)$, yielding $(x, y) = (2, 2)$ and $(x, y) = (-2, 2)$.

**Remark.** The equation $x^2 + k = y^3$, where $k$ is a nonzero integer, is called *Mordell's equation* (after L. Mordell (1888–1972)). Mordell proved in 1922 that for every nonzero integer $k$, the equation only has finitely many integral solutions. The study of this equation is complicated and involves advanced methods. For instance, the integral solutions to $x^2 - 24 = y^3$ are $(\pm 4, -2)$, $(\pm 5, 1)$, $(\pm 32, 10)$, and $(\pm 736844, 8158)$.

The result in Theorem 2.3.1 also holds in the ring $\mathbb{Z}[i]$, that is, the solutions to the equation $xy = zw$ are $x = mn$, $y = pq$, $z = mp$, $w = nq$, where $m, n, p, q \in \mathbb{Z}[i]$ and $\gcd(n, p) = 1$.

**Example 5.** *If $a, b, c, d$ are positive integers such that $a^2 + b^2 = cd$, then there are integers $x, y, z, w, t$ such that*

$$a = t(xz - yw), \quad b = t(xw + yz), \quad c = t(x^2 + y^2), \quad d = t(z^2 + w^2).$$

*Solution.* Let $t = \gcd(a, b, c, d)$, $a = ta_1$, $b = tb_1$, $c = tc_1$, and $d = td_1$. Then

$$a_1^2 + b_1^2 = c_1 d_1,$$

which can be rewritten as

$$(a_1 + b_1 i)(a_1 - b_1 i) = c_1 d_1.$$

From the remark above there are $m, n, p, q \in \mathbb{Z}[i]$ such that

$$a_1 + b_1 i = mn, \quad a_1 - b_1 i = pq, \quad c_1 = np, \quad d_1 = mq. \qquad (1)$$

Because $np$ and $mq$ are positive integers, it follows that $n = k\overline{p}$ and $q = l\overline{m}$ for some positive rational numbers $k$ and $l$. On the other hand, $|mn| = |pq|$ implies $|km\overline{p}| = |lp\overline{m}|$ and $k = l$.

Let $u$ and $v$ be relatively prime positive integers such that $k = \frac{u}{v}$. Then

$$a_1 + b_1 i = \frac{u}{v} m\overline{p}, \quad a_1 - b_1 i = \frac{u}{v} p\overline{m}, \quad c_1 = \frac{u}{v} p\overline{p}, \quad d_1 = \frac{u}{v} m\overline{m}.$$

This means that $u \mid a, b, c, d$ and thus $u = 1$. We also have

$$a_1 + b_1 i = \frac{v}{u} n\overline{q}, \quad a_1 - b_1 i = \frac{v}{u} q\overline{n}, \quad c_1 = \frac{v}{u} n\overline{n}, \quad d_1 = \frac{v}{u} q\overline{q},$$

implying $v \mid a, b, c, d$ and thus $v = 1$. Let $n = x + yi$ and $m = z + wi$, where $x, y, z, w \in \mathbb{Z}$. Then (1) yields

$$a_1 = xz - yw, \quad b_1 = xw + yz, \quad c_1 = x^2 + y^2, \quad d_1 = z^2 + w^2$$

and thus

$$a = t(xz - yw), \quad b = t(xw + yz), \quad c = t(x^2 + y^2), \quad d = t(z^2 + w^2).$$

**Example 6.** *If $a, b, c$ are positive integers such that $ab = c^2 + 1$, then $a$ and $b$ can be written as sums of two integer squares.*

*Solution.* From the previous problem, there are integers $x, y, z, t$ such that

$$t(x^2 + y^2) = a, \quad t(z^2 + w^2) = b, \quad t(xz - yw) = c, \quad t(xw + yz) = 1.$$

This implies $t = 1$ and $a = x^2 + y^2$, $b = z^2 + w^2$.

**Remarks.** (1) We can use the result above to prove in a simple way the well-known fact that every prime $p$ of the form $4k + 1$ can be written as a sum of two squares.

Indeed, by Wilson's theorem,

$$\begin{aligned} -1 &\equiv (p-1)! = 1 \cdot 2 \cdots 4k = (2k)!(2k+1)(2k+2)\cdots 4k \\ &\equiv (2k)!(-1)^{2k}(p-(2k+1))(p-(2k+2))\cdots(p-4k) \\ &= (2k)!(2k)(2k-1)\cdots 1 = ((2k)!)^2 \pmod{p}. \end{aligned}$$

Hence

$$((2k)!)^2 + 1 = ap,$$

for some positive integer $a$, and the conclusion follows.

(2) We can give another solution to Problem 8 in Section 1.4, that is, to prove that the equation $4xy - x - y = z^2$ has no solutions in positive integers. Indeed, from

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

we get

$$4x - 1 = t(u^2 + v^2), \quad 4y - 1 = t(s^2 + w^2), \quad 2z = t(us - vw),$$

with $t(uw + vs) = 1$. Hence $t = 1$, $4x - 1 = u^2 + v^2$, implying $u^2 + v^2 \equiv 3 \pmod 4$, a contradiction.

**Example 7.** *Find all quadruples $(u, v, w, s)$ satisfying the generalized Pythagorean equation*

$$r^2 + u^2 + v^2 = s^2.$$

*Solution.* Write the equation as

$$u^2 + v^2 = s^2 - r^2,$$

that is,

$$u^2 + v^2 = (s + r)(s - r).$$

Applying the result in a previous problem for $a = u$, $b = v$, $c = s - r$, and $d = s + r$, we obtain

$$u = t(xz - yw), \quad v = t(xw + yz),$$

$$s + r = t(x^2 + y^2), \quad s - r = t(z^2 + w^2).$$

For $t = 2$, this yields the solution

$$r = x^2 + y^2 - z^2 - w^2, \quad s = x^2 + y^2 + z^2 + w^2,$$
$$u = 2(xz - yw), \quad v = 2(xw + yz),$$

which is mentioned in Remark 2 after Theorem 2.2.3.

## Exercises and Problems

**1.** Solve the equation

$$x^2 + 4 = y^n,$$

where $n$ is an integer greater than 1.

**2.** Solve the equation

$$x^2 + 9 = y^n,$$

where $n$ is an integer greater than 1.

**3.** Let $p = 4m - 1$ be a prime and let $x$ and $y$ be relatively prime integers such that

$$x^2 + y^2 = z^{2m}$$

for some integer $z$. Prove that $p \mid xy$.

(American Mathematical Monthly)

## 4.2 The Ring of Integers of $\mathbb{Q}[\sqrt{d}]$

Let us consider the field

$$\mathbb{Q}[\sqrt{d}] = \left\{ m + n\sqrt{d} : \ m, n \in \mathbb{Q} \right\},$$

where $d$ is a nonzero square-free integer. An element $\varepsilon \in \mathbb{Q}[\sqrt{d}]$ is called a unit if there exists $\varepsilon_1 \in \mathbb{Q}[\sqrt{d}]$ such that $\varepsilon\varepsilon_1 = \varepsilon_1\varepsilon = 1$.

If $\mu \in \mathbb{Q}[\sqrt{d}]$, $\mu = a + b\sqrt{d}$, we will denote by $\overline{\mu}$ the element $\overline{\mu} = a - b\sqrt{d}$ and will call it the conjugate of $\mu$.

Let us denote by $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Z}$ the norm function: if $\mu = a+b\sqrt{d}$, then

$$N(\mu) = a^2 - db^2 = \mu \cdot \overline{\mu}.$$

**Proposition 4.2.1.** ($N$ is multiplicative) *For all* $\mu_1, \mu_2 \in \mathbb{Q}[\sqrt{d}]$,

$$N(\mu_1\mu_2) = N(\mu_1)N(\mu_2).$$

*Proof.* If $\mu_1 = m_1 + n_1\sqrt{d}$ and $\mu_2 = m_2 + n_2\sqrt{d}$, then

$$\mu_1\mu_2 = (m_1m_2 + dn_1n_2) + (m_1n_2 + m_2n_1)\sqrt{d}$$

and

$$\begin{aligned} N(\mu_1\mu_2) &= (m_1m_2 + dn_1n_2)^2 - d(m_1n_2 + m_2n_1)^2 \\ &= m_1^2m_2^2 + d^2n_1^2n_2^2 - dm_1^2n_2^2 - dm_2^2n_1^2 \\ &= m_1^2(m_2^2 - dn_2^2) - dn_1^2(m_2^2 - dn_2^2) \\ &= (m_1^2 - dn_1^2)(m_2^2 - dn_2^2) = N(\mu_1)N(\mu_2). \end{aligned}$$

**Proposition 4.2.2.** (the conjugate is multiplicative) *For all* $\mu_1, \mu_2 \in \mathbb{Q}[\sqrt{d}]$,

$$\overline{\mu_1\mu_2} = \overline{\mu}_1\overline{\mu}_2.$$

*Proof.* If $\mu_1 = m_1 + n_1\sqrt{d}$ and $\mu_2 = m_2 + n_2\sqrt{d}$, then

$$\mu_1\mu_2 = (m_1m_2 + dn_1n_2) + (m_1n_2 + m_2n_1)\sqrt{d}$$

and

$$\begin{aligned}\overline{\mu_1\mu_2} &= (m_1m_2 + dn_1n_2) - (m_1n_2 + m_2n_1)\sqrt{d} \\ &= (m_1 - n_1\sqrt{d})(m_2 - n_2\sqrt{d}) = \overline{\mu}_1\overline{\mu}_2.\end{aligned}$$

**Remark.** Proposition 4.2.2 gives another proof of the fact that $N$ is multiplicative. Indeed,

$$\begin{aligned}N(\mu_1\mu_2) &= (\mu_1\mu_2)(\overline{\mu_1\mu_2}) = (\mu_1\mu_2)(\overline{\mu}_1\overline{\mu}_2) \\ &= (\mu_1\overline{\mu}_1)(\mu_2\overline{\mu}_2) = N(\mu_1)N(\mu_2).\end{aligned}$$

The important part of these algebraic preliminaries connected to Diophantine equations pertains to the ring of integers of $\mathbb{Q}[\sqrt{d}]$. In this respect we have the following result.

**Theorem 4.2.3.** *If $d \equiv 2, 3 \pmod 4$, then the ring of integers of $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. If $d \equiv 1 \pmod 4$, then the ring of integers of $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Z}[(-1 + \sqrt{d})/2] = \mathbb{Z} + \mathbb{Z}((-1 + \sqrt{d})/2)$.*

In the case of the ring $R = \mathbb{Z}[\sqrt{d}]$, the units $\varepsilon$ are the elements satisfying the relation $N(\varepsilon) = \pm 1$.

Indeed, if $\varepsilon$ is a unit in $R$, then there exists $\varepsilon_1 \in R$ such that $\varepsilon\varepsilon_1 = 1$. Then from Proposition 4.2.1,

$$N(\varepsilon)N(\varepsilon_1) = 1^2 - d0^2 = 1.$$

Since $N(\varepsilon)$ and $N(\varepsilon_1)$ are integers, it follows that $N(\varepsilon) = \pm 1$. Conversely, if $N(\varepsilon) = \pm 1$, then $N(\varepsilon) = \varepsilon\overline{\varepsilon}$ yields $\varepsilon\overline{\varepsilon} = \pm 1$. If $N(\varepsilon) = 1$, then $\varepsilon\overline{\varepsilon} = 1$, and if $N(\varepsilon) = -1$, then $\varepsilon(-\overline{\varepsilon}) = 1$. Both cases show that $\varepsilon$ is a unit in $R$.

One of the main problems is to find all $d$ for which the ring of integers of $\mathbb{Q}[\sqrt{d}]$ is a UFD. This problem was first solved for $d < 0$ by

Kurt Heegner (Diophantine Analysis und Modulfunktionen, Mathematische Zeitschrift, vol. 56, 1952, pp. 227–253) and independently by Stark and A. Baker in 1966. For $d < 0$ the result is the following.

**Theorem 4.2.4.** *The ring of integers in $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ and square-free is a UFD exactly when*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

As an example, consider the ring $\mathbb{Z}[-\sqrt{5}]$, which is the ring of integers in $\mathbb{Q}[\sqrt{-5}]$ because $-5 \equiv 3 \pmod 4$. We have $21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$, two factorizations of 21 showing that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Another example is

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Little is known about the UFD property of $\mathbb{Q}[\sqrt{d}]$ for $d > 0$. What we know is that $\mathbb{Q}[\sqrt{d}]$ is a UFD for $d = 2$, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 33, 37, 41, 53, 57, 61, 69, 73, 77, 89, 93, 97.

In what follows we investigate Pell's equation $x^2 - dy^2 = 1$ using the results involving $\mathbb{Z}[\sqrt{d}]$. Recall that for $\sqrt{d} \notin \mathbb{Q}$ this equation is always solvable and let $(x_1, y_1)$ be its fundamental solution (see Section 3.2).

**Theorem 4.2.5.** *If $z_1 = x_1 + y_1\sqrt{d}$ is the minimal element of $\mathbb{Z}[\sqrt{d}]$, with $z_1 > 1$ and $N(z_1) = 1$, then all elements $z \in \mathbb{Z}[\sqrt{d}]$ with $N(x) = 1$ are given by $z = \pm z_1^n$, $n \in \mathbb{Z}$.*

*Proof.* Suppose $N(z)$ for some $z > 1$. There is a unique integer $k$ such that $z_1^k \le z < z_1^{k+1}$. Then $z' = z \cdot z_1^{-k}$ satisfies $1 \le z' < z_1$ and $N(z') = N(z)N(z_1)^{-k} = N(z) = 1$. From the minimality of $z_1$, it follows that $z' = 1$; hence $z = z_1^k$, $k \in \mathbb{Z}$. □

**Remarks.** (1) If $(x_1, y_1)$ is the fundamental solution to Pell's equation $x^2 - dy^2 = 1$, then all solutions in nonnegative integers to this equation are given by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n = 0, 1, 2, \ldots .$$

(2) The solution $(x_n, y_n)$ can be expressed as

$$x_n = \frac{1}{2}(z_1^n + \overline{z}_1^n), \quad y_n = \frac{1}{2\sqrt{d}}(z_1^n - \overline{z}_1^n),$$

where $\overline{z}_1 = x_1 - y_1\sqrt{d}$ is the conjugate of $z_1$ in $\mathbb{Z}[\sqrt{d}]$.

Concerning the negative Pell's equation $x^2 - dy^2 = -1$ (see Section 3.4), we can derive the following result.

**Theorem 4.2.6.** *The equation $x^2 - dy^2 = -1$ is solvable if and only if the equation $z^2 = z_1$ is solvable in $\mathbb{Z}[\sqrt{d}]$.*

*Proof.* The "if" part is clear.

For the other implication, take the least $z \in \mathbb{Z}[\sqrt{d}]$, $z > 1$, that is a solution to the equation $N(z) = -1$. As in the proof of Theorem 4.2.5 we deduce that $1 \le z < z_1$. But $z^2 < z_1^2$ is a solution to $N(z) = 1$, and hence $z^2 = z_1$. □

Consider the general Pell's equation $N(z) = a$, where $a$ is a nonzero integer. As in Theorem 4.2.5 we can show that all of its solutions are obtained from its solutions $z$ with $1 < z \le z_1$, where $z_1$ is the fundamental solution to Pell's equation $N(z) = 1$. Thus it is always sufficient to check finitely many values of $z = x + y\sqrt{d}$. Moreover, there are simple upper bounds for $x$ and $y$.

**Theorem 4.2.7.** *If the equation $x^2 - dy^2 = a$ is solvable in integers, then there is a solution $z = x + y\sqrt{d}$ with*

$$|x| \le \frac{z_1 + 1}{2\sqrt{z_1}}\sqrt{|a|}$$

*and the corresponding upper bound for* $y = \sqrt{\frac{x^2-a}{d}}$.

*Proof.* Let $z'$ be a solution to $N(z) = a$. There is an integer $m$ such that

$$\sqrt{\frac{|a|}{z_1}} \le z_1^m z' < \sqrt{|a|z_1}.$$

Then $z = z_1^m z' = x + y\sqrt{d}$ is a solution to $N(z) = a$ satisfying

$$2|x| = \left|z + \frac{a}{z}\right| \le \max_{t \in \left[\frac{|a|}{z_1}, \sqrt{|a|z_1|}\right)} \left|t + \frac{|a|}{t}\right| = \frac{z_1 + 1}{\sqrt{z_1}}\sqrt{|a|},$$

where we used the fact that the convex function $t \mapsto t + \dfrac{|a|}{t}$ achieves its maximum at the endpoints of the interval $\left[\sqrt{\dfrac{|a|}{z_1}}, \sqrt{|a|z_1}\right]$. □

For example, for the equation $x^2 - 7y^2 = 2$, the fundamental solution to the corresponding Pell's equation is $z_1 = 8 + 3\sqrt{7}$. We can found solutions $z = x + y\sqrt{7}$ to $N(z) = 2$ from the inequalities

$$x \le \frac{z_1 + 1}{2\sqrt{z_1}}\sqrt{|a|} = \frac{9 + 3\sqrt{7}}{2\sqrt{8 + 3\sqrt{7}}}\sqrt{2} = 3$$

and

$$y = \sqrt{\frac{x^2 - 2}{7}} \le \sqrt{\frac{3^2 - 2}{7}} = 1.$$

The only such solution is $3 + \sqrt{7}$. It follows that all solutions to $x^2 - 7y^2 = 2$ are $(x_n, y_n)$, where

$$x_n + y_n\sqrt{7} = (3 + \sqrt{7})(8 + 3\sqrt{7})^n, \quad n = 0, 1, \ldots$$

A general strategy for solving a certain type of Diophantine equations is summarized below.

**Step 1.** Represent the equation in the form:

$$(a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d}) = e \cdot c^n,$$

where $a_1, b_1, a_2, b_2, c, e \in \mathbb{Z}$, $d \in \mathbb{Z}$, $d < 0$ and square-free, $n \in \mathbb{N}$. Preferably, $e$ should be something simple, like a unit or a prime in the ring of integers in $\mathbb{Q}[\sqrt{d}]$. Some of the above numbers can be constants, while others can be unknowns.

**Step 2.** If $d$ happens to be one of the negative integers in Theorem 4.2.4, we are in good shape. If not, check to see whether you can factor different expressions (possibly on the "other side" of the equation) so as to reduce to Theorem 4.2.4.

**Step 3.** Check $d$ modulo 4 and use Theorem 4.2.3 to decide what the ring of integers of $\mathbb{Q}[\sqrt{d}]$ looks like. From now on, you will work either in $\mathbb{Z}[\sqrt{d}]$ or in $\mathbb{Z}[(-1+\sqrt{d})/2]$, and all arguments about units, primes, and factorization will be made in this ring, which we denote by $\Omega_d$. By now, you should have determined that $\Omega_d$ is a UFD, or else this method won't work.

**Step 4.** Determine all units of $\Omega_d$. The following theorem answers this question in a more general setting, but you may want, instead of memorizing it, to try to remember how to derive its result. Clearly, $\Omega_{-1} = \mathbb{Z}[i]$.

**Theorem 4.2.8.** *Let $d < 0$ be a square-free integer, and let $U_d$ denote the group of units in $\Omega_d$. Then*

1. $U_{-1} = \{1, -1, i, -i\}$;

2. $U_{-3} = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$, *where* $\omega = \frac{-1+\sqrt{-3}}{2}$ *is a third root of unity;*

3. $U_{-d} = \{1, -1\}$ *for* $d < -3$ *or* $d = -2$.

**Step 5.** Investigate whether an integer prime $p \in \mathbb{Z}$ remains prime in $\Omega_d$, and if not, what its prime factorization is.

**Step 6.** Investigate whether $(a_1 + b_1\sqrt{d})$ and $(a_1 - b_1\sqrt{d})$ are relatively prime, and if not, what their common divisors in $\Omega_d$ can be.

In a UFD, $ab = c^n$, where $a, b$ are relatively prime, implies $a = u_1 c_1^n$ and $b = u_2 c_2^n$ for some $u_1, u_2$ units in $R$ and some elements $c_1, c_2 \in R$ such that $u_1 u_2 = 1$ and $c_1 c_2 = c$.

**Example 1.** *The equation* $x^3 - 2 = y^2$ *has* $(3, \pm 5)$ *as its only solutions in integers.*

(Fermat)

*Solution.* Write $x^3 = u^2 + 2 = (y + \sqrt{-2})(y + \sqrt{-2})$. Note that $y$ must be odd (otherwise $y^2 + 2 \equiv 2 \pmod 4$, and no cube is $\equiv 2 \pmod 4$). Now let $\delta = \gcd(y + \sqrt{-2}, y + \sqrt{-2})$. Clearly $\delta \mid 2\sqrt{-2}$ (the difference of these values); thus $\delta$ is a power of $\sqrt{-2}$. On the other hand, if $\sqrt{-2} \mid (y \pm \sqrt{-2})$, then it divides the product of these factors, which is $x^3 = y^2 + 2$. But $x$ is odd; hence $\sqrt{-2} \nmid \delta$.

We have seen that $y + \sqrt{-2}$ and $y + \sqrt{-2}$ are relatively prime and that their product is a cube. Since $\mathbb{Z}[\sqrt{-2}]$ is a UFD, this implies that the factors are cubes up to units. Since the only units are $\pm 1$ and since these are cubes, it follows that $y + \sqrt{-2} = (a + b\sqrt{-2})^3$. Comparing real and imaginary parts, we obtain $y = a^3 - 6ab^2$ and $1 = 3a^2 b - 2b^3$. The last equation shows that $1 = b(3a^2 - 2b^2)$; hence $b = \pm 1$ and therefore $a = \pm 1$. This shows that $y = \pm 5$ and $x = 3$.

**Example 2.** *Solve in integers the equation*

$$x^2 + 8 = y^3.$$

*Solution.* We will prove that the only solution is $(0, 2)$. For $x$ even, $x = 2u$, $y$ is also even, $y = 2v$, and the equation becomes $u^2+2 = 2v^3$. It follows that $u = 2w$, yielding $2w^2 + 1 = v^3$. Using the uniqueness of the prime factorization in $\mathbb{Z}[\sqrt{-2}]$, we have

$$\pm(1 + w\sqrt{-2}) = (a + b\sqrt{-2})^3 \tag{1}$$

for some integers $a$ and $b$.

Identifying the rational parts, it follows that $\pm 1 = a^3 - 6ab^2$. Hence $a \mid 1$; so $a = \pm 1$ and $b = 0$. Passing to norms in (1) we get $v^3 = 1 + 2w^2 = (a^2 + 2b^2)^3$; therefore $v = a^2 + 2b^2$. In this case we get $v = 1$; hence $y = 2$ and $x = 0$.

For $x$ odd, the equation is equivalent to

$$x^2 + 16 = y^3 + 2^3 = (y + 2)(y^2 - 2y + 4),$$

and since $y$ is also odd, one of the factors $y + 2$ and $y^2 - 2y + 4$ is of the form $4m + 3$, contradicting the result in Theorem 4.4.2.

**Example 3.** *Euler's approach to Fermat's last theorem for $n = 3$.*

This case was completely solved in Section 2.3.2. We discuss here Euler's attempt to prove that the equation $x^3 + y^3 = z^3$ has no nontrivial solutions by using properties of the field $\mathbb{Q}[\sqrt{-3}]$.

Euler started with $\gcd(x, y, z) = 1$. If both $x$ and $y$ are odd, then $x+y$ and $x-y$ are both even, say $2p$ and $2q$, respectively, so $x = p+q$, $y = p - q$, and

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

Since $x$ and $y$ are odd and relatively prime, $p$ and $q$ must be of opposite parities and relatively prime. And since $x^3 + y^3 = z^3$,

$2p(p^2 + 3q^2)$ must be a cube. A similar argument yields the same conclusion if $z$ is odd and one of $x$ and $y$ is even.

At this point we want to show that both $2p$ and $p^2+3q^2$ are cubes. If $3 \nmid p$, this follows easily by noting that $2p$ and $p^2+3q^2$ are relatively prime; if $3 \mid p$, then we must write $p = 3s$, and then rewrite

$$2p(p^2 + 3q^2) = 3^2 \cdot 2s(3s^2 + q^2),$$

from which we infer that $3^2 \cdot 2s$ and $3s^2 + q^2$ are relatively prime. Each must therefore be a cube.

Euler noted that one way in which both $2p$ and $p^2 + 3q^2$ are cubes is for $p$ and $q$ to have the forms

$$p = a(a - 3b)(a + 3b), \quad q = 3b(a - b)(a + b) \tag{1}$$

(a similar expression is found for $s$ and $q$ when $p$ is a multiple of 3). If this is indeed the case, then $a$ and $b$ must be relatively prime, because $p$ and $q$ are relatively prime, and must have opposite parities. From here one shows that $2a$, $a-3b$, and $a+3b$ must be pairwise relatively prime. Because $2p = 2a(a - 3b)(a + 3b)$ is a cube, each of $2a$, $a - 3b$, and $a + 3b$ must be a cube. Then $(a - 3b) + (a + 3b) = 2a$ gives a new solution to the Fermat equation, one with $2a < z^3$, setting up the infinite descent and thus proving the result. A similar argument is used when $3 \mid p$.

At this point, of course, we need to show that the only way for $2p$ and $p^2 + 3q^2$ to be both cubes is for $p$ and $q$ to be expressible as in (1). It is here that the argument presented by Euler fails (he had, however, other results on quadratic forms that he could have used to establish this claim about $p$ and $q$). Euler factors $p^2 + 3q^2 =$

$(p+q\sqrt{-3})(p-q\sqrt{-3})$ and proceeds to work in $\mathbb{Z}[\sqrt{-3}]$. Because

$$(p+q\sqrt{-3})+(p-q\sqrt{-3})=2p,$$
$$(p+q\sqrt{-3})+(p-q\sqrt{-3})=2q\sqrt{-3},$$

any common divisor of $(p+q\sqrt{-3})$ and $(p-q\sqrt{-3})$ would be a divisor of $2p$ and of $2q\sqrt{-3}$. One can show that both 2 and $\sqrt{-3}$ are irreducible in $\mathbb{Z}[\sqrt{-3}]$ (see the argument to follow). Since $p$ and $q$ have opposite parities it follows that 2 does not divide $p+q\sqrt{-3}$, and from the fact that $3\nmid p$ one deduces that $\sqrt{-3}$ does not divide $p+q\sqrt{-3}$ either. Accordingly, any common divisor of $p+q\sqrt{-3}$ and $p-q\sqrt{-3}$ must in fact be a common divisor of both $p$ and $q$, which are relatively prime. Hence $p+q\sqrt{-3}$ and $p-q\sqrt{-3}$ have no common divisors in $\mathbb{Z}[\sqrt{-3}]$ other than 1 and $-1$. Because their product is a cube, Euler concludes that each must be a cube, so in fact we have

$$p+q\sqrt{-3}=(a+b\sqrt{-3})^3,$$
$$p-q\sqrt{-3}=(a-b\sqrt{-3})^3$$

for some integers $a$ and $b$. It now follows that

$$\begin{aligned} p+q\sqrt{-3} &= a^3+3a^2b\sqrt{-3}-9ab^2-3b^3\sqrt{-3} \\ &= (a^3-9ab^2)+(3a^2b-3b^3)\sqrt{-3}, \end{aligned}$$

from which the desired equations (1) follow.

The problem, of course, is that hidden in that argument is an assumption of unique factorization: we know that $p-q\sqrt{-3}$ and $p+q\sqrt{-3}$ have no common divisors in $\mathbb{Z}[\sqrt{-3}]$ (other than 1 and $-1$) and that their product is a cube. If we have unique factorization

into irreducibles in $\mathbb{Z}[\sqrt{-3}]$, then we are able to conclude that each factor must itself be a cube. But in fact we do not have uniqueness:

$$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = (2)(2),$$

and each of the numbers 2, $1+\sqrt{-3}$, and $1-\sqrt{-3}$ is irreducible in $\mathbb{Z}[\sqrt{-3}]$. Thus, Euler's argument breaks down.

Let us show, for example, that $1+\sqrt{-3}$ is indeed irreducible in $\mathbb{Z}[\sqrt{-3}]$. Assuming the contrary, we have $1+\sqrt{-3} = ab$, for some $a, b \in \mathbb{Z}[\sqrt{-3}]$ that are not units. Then $N(1+\sqrt{-3}) = N(a \cdot b) = N(a) \cdot N(b)$, and so $4 = N(a) \cdot N(b)$, implying $N(a) = N(b) = 2$. But if, for instance, $a = u + v\sqrt{-3}$, then $u^2 + 3v^2 = 2$, a contradiction.

**Example 4.** *Let $S$ be the set of positive integers of the form $a^2 + 2b^2$, where $a$ and $b$ are integers and $b \neq 0$. Prove that if $p$ is a prime and $p^2 \in S$, then $p \in S$.*

(Romanian Mathematical Olympiad)

*Solution.* It is clear that $p > 2$, since $4 \notin S$. Because $p$ is odd, from $p^2 = a^2 + 2b^2$ it follows that $a$ is odd, $b$ is even, and $\gcd(a, b) = 1$. From

$$(p-a)(p+a) = 2b^2,$$

we get

$$p - a = 2^m A, \quad p + a = 2^n B, \tag{1}$$

where $A$ and $B$ are odd, $m \geq 1$, $n \geq 1$, and $m+n$ is odd. By adding the equalities (1) we obtain

$$2p = 2^m A + 2^n B = 2^{\min\{m,n\}} C,$$

where $C$ is again odd. It follows that $\min\{m, n\} = 1$ and if one of the two exponents is 1, the other one is an even number. We need to consider two cases.

**Case 1.** $m = 1$, $n = 2r$ with $r \geq 1$. It follows that $p - a = 2A$, $p + a = 2^{2r}B$, and so

$$p^2 - a^2 = 2^{2r+1}AB = 2b^2.$$

From this we deduce $2^{2r}AB = b^2$. Also, from (1) it is easy to see that $\gcd(A, B) = 1$. Hence $A$ and $B$ are perfect squares: $A = \alpha^2$, $B = \beta^2$. Using (1) again we obtain

$$p - a = 2\alpha^2, \quad p + a = 2^{2r}\beta^2. \tag{2}$$

Adding the equalities (2), we get

$$p = \alpha^2 + 2(2^{r-1}\beta)^2.$$

**Case 2.** $n = 1$, $m = 2s$ with $s \geq 1$. Then $p-a = 2^{2r}A$, $p+a = 2B$, and so

$$p^2 - a^2 = 2b^2 = 2^{2r+1}AB.$$

Similarly, we obtain $b^2 = 2^sAB$, $A = \alpha^2$, $B = \beta^2$, and finally

$$p = \beta^2 + 2(2^{s-1}\alpha)^2.$$

**Remark.** The problem comes from a well-known fact: the ring $\mathbb{Z}[\sqrt{-2}]$ is a UFD.

We know that the units in this ring are $\pm 1$. If $p$ is a prime that is not is $S$, then $p$ is irreducible and hence a prime in the ring $\mathbb{Z}[\sqrt{-2}]$. Indeed, from

$$p = (a + b\sqrt{-2})(c + d\sqrt{-2})$$

we obtain

$$N(p) = p^2 = (a^2 + 2b^2)(c^2 + 2d^2),$$

and since $p \notin S$,

$$a^2 + 2b^2 = 1 \quad \text{or} \quad c^2 + 2d^2 = 1.$$

It follows that, for example, $a + b\sqrt{-2} = 1$ and $p$ is irreducible.

Now let

$$p^2 = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2}).$$

Using the fact that $p$ is a prime, it follows that $p \mid a + b\sqrt{-2}$ or $p \mid a - b\sqrt{-2}$. This is a contradiction, because $p \mid a$ and $p \mid b$ implies $a = pa_1$, $b = pb_1$, and $p = a_1^2 + 2b_1^2$.

**Example 5.** *Let $a > b > c > d$ be positive integers and suppose*

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

*Prove that $ab + cd$ is not a prime.*

(42nd IMO)

*Solution.* The equation is equivalent to

$$a^2 - ac + c^2 = b^2 + bd + d^2.$$

We will work in the ring of integers of $\mathbb{Q}[\sqrt{-3}]$ and use the following result.

**Lemma.** *Let $u, v, w, s$ be nonzero elements of the ring of integers of $\mathbb{Q}[\sqrt{-3}]$ such that $uv = ws$. Then $u = xy$, $v = zt$, $w = xz$, and $s = yt$ for some integers $x, y, z, t$ of $\mathbb{Q}[\sqrt{-3}]$ with* $\gcd(y, z) = 1$.

*Proof.* We have $\frac{u}{w} = \frac{s}{v} = \frac{y}{z}$, where $\gcd(y, z) = 1$.

Then $uz = wy$; hence $y \mid u$, yielding $u = xy$ and $w = xz$ for some integer $x$ of $\mathbb{Q}[\sqrt{-3}]$. Similarly, $z \mid v$, and hence $v = zt$ and $s = yt$, for some integer $t \in \mathbb{Q}[\sqrt{-3}]$. □

The condition $a^2 - ac + c^2 = b^2 + bd + d^2$ translates as

$$(a - cw)(a - c\overline{w}) = (b + dw)(b + d\overline{w}),$$

where $w$ is the primitive cubic root of unity $\frac{-1+i\sqrt{3}}{2}$.

The lemma gives us the existence of $x, y, z, t$ with $\gcd(y, z) = 1$, $a - cw = xy$, $a - c\overline{w} = zt$, $b + dw = xz$, $b - d\overline{w} = yt$. Then $\frac{a-cw}{b+dw} = \frac{y}{z}$ and $\frac{a-c\overline{w}}{b+d\overline{w}} = \frac{z}{y}$. On the other hand, $a - c\overline{w} = \overline{a - cw}$, $b + d\overline{w} = \overline{b + dw}$, and $\frac{a-c\overline{w}}{b+d\overline{w}} = \frac{\overline{y}}{\overline{z}}$. So $\frac{z}{y} = \frac{\overline{y}}{\overline{z}}$. Since $\gcd(y, z) = \gcd(\overline{y}, \overline{z}) = 1$, we deduce $z = \overline{y}$. Then $t = \overline{x}$, since $xy = a - cw$, $t\overline{y} = a - c\overline{w}$ are conjugates.

The conditions now read $a - c\overline{w} = \overline{xy}$, $a + c\overline{w} = \overline{xy}$, $b + d\overline{w} = x\overline{y}$, $b - d\overline{w} = \overline{y}x$. Routine computations yield

$$a = \frac{\overline{xy}w - xy\overline{w}}{\sqrt{3}i}, \quad b = \frac{\overline{x}yw - x\overline{yw}}{\sqrt{3}i}, \quad c = \frac{\overline{xy} - xy}{\sqrt{3}i}, \quad d = \frac{x\overline{y} - \overline{x}y}{\sqrt{3}i}.$$

Then $ab + cd$ equals

$$\begin{aligned} &-\frac{1}{3}(\overline{xy}w - xy\overline{w})(\overline{x}yw - x\overline{yw}) - (\overline{xy} - xy)(x\overline{y} - \overline{x}y) \\ &= -\frac{1}{3}y\overline{y}(x^2(w-1) + \overline{x}^2(\overline{w} - 1) = \frac{1}{3}N(y)\sqrt{3}i(x^2\overline{w} - \overline{x}^2 w). \end{aligned}$$

If $x^2\overline{w} = \frac{u - v\sqrt{3}i}{2}$, then $x^2\overline{w} - \overline{x}^2 w = -\sqrt{3}iv$, so $ab + cd = N(y)v$. Therefore if $ab + cd$ is a prime, then either $N(y) = 1$ or $v = 1$. Let us prove that $N(y) > 1$. We must analyze the cases $y \in \{1, -1, w, -w, \overline{w}, -\overline{w}\}$. Let us take them one by one: $y = \pm 1$ means $a = b$, and $y = \pm w$ means $b = c$. Next, $y = \pm\overline{w}$ means $a + d = 0$, which is impossible, so indeed $N(y) > 1$. Finally, if $v = 1$, then set

$x = \frac{k+li\sqrt{3}}{2}$, so

$$x^2\overline{w} = \frac{3l^2 - k^2 + 6kl - \sqrt{3}i(k^2 - 3l^2 - 2kl)}{8},$$

so $v = 1$ means $k^2 - 3l^2 + 2kl = (k+l)^2 - 4l^2 = 4$, which is possible only for $l = 0$ and $k = \pm 2$, which is impossible, since $k$ and $l$ must be of the same parity.

## Exercises and Problems

**1.** Find all pairs $(x, y)$ of positive integers such that

$$13^x + 3 = y^2.$$

(Mathematical Reflections)

**2.** Solve the equation

$$x^2 + 3 = y^n,$$

where $n$ is an integer greater than 1.

**3.** Solve the equation

$$x^2 + 11 = 3^n,$$

where $n$ is an integer greater than 1.

**4.** Solve the equation

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

**5.** Let $a$ and $b$ be positive integers such that $b = x^2 - dy^2$ for some integers $x, y, d$ with $d = a^2 - 1$. Prove that if $b < 2(a+1)$, then $b$ is a perfect square.

## 4.3 Quadratic Reciprocity and Diophantine Equations

An integer satisfying $\gcd(a, m) = 1$ is called a *quadratic residue* modulo $m$ if $x^2 \equiv a \pmod{m}$ for some integer $x$. Otherwise, it is called a *quadratic nonresidue* modulo $m$.

For example, 2 is a quadratic residue modulo 7 because, for instance, $3^2 \equiv 2 \pmod{7}$, while 3 is a nonresidue modulo 7.

Let $p$ be an odd prime. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

The basic properties of Legendre symbol are given in the following theorem.

**Theorem 4.3.1.** *Let $p$ be an odd prime. Then*

1. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$,
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
3. $\left(\frac{a^2}{p}\right) = 1,\ a \not\equiv 0 \pmod{p}$,
4. $a \equiv b \pmod{p}$ *implies* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
5. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

*Proof.* (1) Note that by Fermat's little theorem, the polynomial $x^{p-1}-1$ has all the nonzero numbers mod $p$ as roots mod $p$. Factoring this as $x^{p-1}-1=(x^{(p-1)/2}-1)(x^{(p-1)/2}+1)$, we see that $\frac{p-1}{2}$ of the nonzero residue classes are roots of the first factor and hence have $a^{(p-1)/2}\equiv 1 \pmod{p}$, and the same number are roots of the second factor and have $a^{(p-1)/2}\equiv -1 \pmod{p}$. If $a$ is a quadratic residue, then $a\equiv b^2 \pmod{p}$ for some $b$ and $a^{(p-1)/2}\equiv b^{p-1}\equiv 1 \pmod{p}$. Since there are $\frac{p-1}{2}$ quadratic residues mod $p$, these must be the only elements with $a^{(p-1)/2}\equiv 1 \pmod{p}$, and the quadratic nonresidues must have $a^{(p-1)/2}\equiv -1 \pmod{p}$. Thus in either case,

$$\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \pmod{p}.$$

(2) From (1) we get

$$(ab)^{\frac{p-1}{2}}\equiv\left(\frac{ab}{p}\right) \pmod{p}$$

and

$$(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Therefore

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(3) We obtain from (2)

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

(4) Follows directly from the definition.

(5) Follows from (1) with $a=-1$. □

The most important result about quadratic residues is Gauss's law of quadratic reciprocity.

**Theorem 4.3.2.** *Let $p$ and $q$ be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

For a proof of this result we refer the reader to [HaWr].

Here are some immediate consequences of the law of quadratic reciprocity. Let $p$ and $q$ be distinct odd primes. Then

1. if $p \equiv q \equiv 1 \pmod 4$, then $p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic residue modulo $p$.

2. if $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ or vice versa, then $p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic residue modulo $p$.

3. if $p \equiv q \equiv 3 \pmod 4$, then $p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic nonresidue modulo $p$.

We will show how quadratic residues can be used in the study of certain Diophantine equations.

**Example 1.** *Prove that $x^2 - 17y^2 = 12$ is not solvable in integers.*

*Solution.* Looking modulo 17 we have $x^2 \equiv 12 \pmod{17}$, while by the facts about the Legendre symbol and the law of quadratic reciprocity, we have

$$\begin{aligned}\left(\frac{12}{17}\right) &= \left(\frac{3}{17}\right)\left(\frac{4}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{2^2}{17}\right) = \left(\frac{3}{17}\right)\\ &= \left(\frac{17}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{2}{3}\right) = -1,\end{aligned}$$

a contradiction.

**Example 2.** *Let $p$ and $q$ be distinct primes, each congruent to* 3 modulo 4. *Then the equation*

$$x^2 - py^2 = q$$

*has no integral solution.*

*Solution.* Indeed, this equation is solvable only if $q$ is a quadratic residue modulo $p$ and $p$ is a quadratic residue modulo $q$. But this is not possible, according to consequence (3) of the law of quadratic reciprocity.

**Example 3.** *The equation $x^2-3y^2=p$ has no solution in integers when $p=2$ or $p=3$.*

*Solution.* Looking modulo 3 at the equation $x^2-3y^2=2$, we get $x^2\equiv -1 \pmod 3$, a contradiction. Reducing the equation $x^2-3y^2=3$ modulo 4, we obtain $x^2+y^2\equiv 3 \pmod 4$, a contradiction.

## Exercises and Problems

**1.** For a prime $p$, the equation $x^2-3y^2=p$ has solutions in integers if and only if $p\equiv 1 \pmod{12}$.

**2.** Let $p$ be a prime of the form $4k+3$. Prove that exactly one of the equations $x^2-py^2=\pm 2$ is solvable.

**3.** Let $p$ be a prime of the form $8k+7$. Prove that the equation $x^2-py^2=2$ is solvable.

## 4.4 Divisors of Certain Forms

In this section we will discuss possible divisors of expressions of the type $a^2+b^2$, $a^2+2b^2$, and $a^2-2b^2$, where $a$ and $b$ are integers. This method goes back to Fermat and Lagrange and has multiple applications in the study of Diophantine equations.

### 4.4.1 Divisors of $a^2 + b^2$

**Theorem 4.4.1.** *Each odd prime divisor of $a^2 + 1$ is of the form $4k + 1$.*

*Proof.* Suppose $p \mid a^2 + 1$, where $p = 4m + 3$. Then $a^2 \equiv -1 \pmod{p}$, implying $a^{p-1} = (a^2)^{2m+1} \equiv -1 \pmod{p}$, contradicting Fermat's little theorem. □

**Theorem 4.4.2.** *(1) Let $a$ and $b$ be relatively prime integers and let $p$ be an odd prime dividing $a^2 + b^2$. Then $p \equiv 1 \pmod{4}$.*

*(2) If $p \equiv 3 \pmod{4}$ is a prime divisor of $a^2 + b^2$, then $p \mid a$ and $p \mid b$.*

*Proof.* (1) Assume $p \mid a^2 + b^2$, with $p = 4m + 3$. Hence $a^2 \equiv -b^2 \pmod{p}$, implying $a^{2m+1} \equiv (-b^2)^{2m+1}$, that is, $a^{p-1} \equiv -b^{p-1} \pmod{p}$. On the other hand, $\gcd(a, b) = 1$ implies $p \nmid a$ and $p \nmid b$, and using Fermat's little theorem again, we obtain $1 \equiv -1 \pmod{p}$, a contradiction.

(2) If $\gcd(a, p) = 1$, then $\gcd(b, p) = 1$, and from Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ and $b^{p-1} \equiv 1 \pmod{p}$. On the other hand, if $p = 4m + 3$, from $p \mid a^2 + b^2$ we get $a^2 \equiv -b^2 \pmod{p}$, implying $(a^2)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}} \pmod{p}$, i.e., $a^{p-1} \equiv -b^{p-1} \pmod{p}$. We reach again $1 \equiv -1 \pmod{p}$, a contradiction.

Thus $p \mid a$ and $p \mid b$. □

**Remark.** It is clear that statement (2) implies Theorem 4.4.1 and statement (1) in Theorem 4.4.2.

**Theorem 4.4.3.** (Thue's lemma). *If $n$ is an integer greater than 1 and $a$ is an integer relatively prime to $n$, then $n \mid ax \pm y$ for some positive integers $x$ and $y$ less than $\sqrt{n}$ and a choice of the signs $+$ and $-$.*

*Proof.* Assume that $n$ is not a perfect square. Let $t = \lfloor \sqrt{n} \rfloor + 1$ and let $S = \{ax + y \mid 0 \leq x,\ y \leq t-1\}$. Clearly, $S$ has $t^2$ elements. Because $t^2 > n$, from the pigeonhole principle it follows that there exist two distinct elements in $S$, $ax_1 + y_1$ and $ax_2 + y_2$, such that $ax_1 + y_1 \equiv ax_2 + y_2 \pmod{n}$, $x_1 > x_2$, that is, $a(x_1 - x_2) \equiv y_2 - y_1 \pmod{n}$. Now take $x = x_1 - x_2$ and $y = |y_2 - y_1|$. It is clear that $x$ and $y$ are nonzero, since $\gcd(a, n) = 1$. For this choice, it is clear that $n \mid ax \pm y$ and $0 < x, y < \sqrt{n}$. If $n$ is a perfect square, then set $n = d^2$. In this case, if one of $x$ and $y$ is $d$, then the other is a multiple of $d$ and hence is also $d$. But then $a = d \pm 1$. For $a = d - 1$, we take $x = 1$, $y = d - 1$, and the minus sign. For $a = d + 1$ we take $x = d - 1$, $y = 1$, and the plus sign. □

In the study of certain Diophantine equations we use some of these results as follows: if one side of the equation can be written as $x^2 + a^2$ with $\gcd(x, a) = 1$, while the other side has a divisor of the form $4k + 3$, then the equation is not solvable in integers.

**Example 1.** *Let $n$ be an odd integer greater than 1. Prove that the equation*

$$x^n + 2^{n-1} = y^2$$

*is not solvable in odd positive integers.*

(Ion Cucurezeanu)

*Solution.* Write the equation as

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

The left-hand side of this equation has a prime divisor of the form $4k + 3$. Indeed, if $x$ is of this form, then at least a prime divisor

of $x^n + 2^n$ is of the form $4k + 3$. If $x$ is of the form $4k + 1$, then $x + 2$ divides $x^n + 2^n$ and is of the form $4k + 3$. In each case, since $\gcd(y, 2^{\frac{n-1}{2}}) = 1$ and $y^2 + 2^{n-1}$ has a prime divisor of the form $4k+3$, we get a contradiction to the result in Theorem 4.4.2.(1).

**Example 2.** *Prove that the equation*

$$x^3 - x^2 + 8 = y^2$$

*is not solvable in integers.*

(Ion Cucurezeanu)

*Solution.* For $x$ odd, write the equation as

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

It is clear that $\gcd(x, y) = 1$. If $x = 4k + 1$, then $x + 2 = 4k + 3$ has a prime divisor of this form that divides $x^2 + y^2$, impossible. If $x = 4k + 3$, then $x^2 - 2x + 4$ is of the form $4m + 3$, and by the same argument, we again get a contradiction.

For $x = 2u$, the equation becomes

$$2u^3 - u^2 + 2 = z^2.$$

If $u$ is odd, then the left-hand side is congruent to 3 (mod 4), and so it cannot be a perfect square. If $u$ is even, then the left-hand side is congruent to 2 (mod 4) and again cannot be a perfect square.

**Example 3.** *Solve in integers the equation*

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

(Balkan Mathematical Olympiad)

*Solution.* Looking mod 8 it follows that $y$ and $x$ are odd. Because $x$ divides $y^2+2^2$, it cannot be of the form $4k+3$. Hence $x=4k+1$ and the equation can be written as

$$x^5+2^5=y^2+6^2.$$

If $3\nmid y$, we again reach a contradiction ($x+2=4k+3$ is a divisor of $y^2+6^2$ and $\gcd(y,6)=1$).

If $y=3y_1$, then $x^5+2^5=3^2(y_1^2+4)$. We will prove that if

$$d=\gcd\left(x+2,\frac{x^5+2^5}{x+2}\right),$$

then $d\mid 5$. Indeed, from the identities

$$a^5+b^5=(a+b)^5-5ab(a^2+ab+b^2)$$

and

$$a^2+ab+b^2=(a+b)^2-ab,$$

it follows that

$$\frac{a^5+b^5}{a+b}=(a+b)^4-5ab(a+b)^2+5a^2b^2.$$

For $a=x$ and $b=2$, $d\mid a+b$ and $d\mid\frac{a^5+b^5}{a+b}$; hence $d\mid 5a^2b^2=5\cdot(2x)^2$. But $\gcd(x+2,2x)=1$, as $x$ is odd, so $\gcd(d,(2x)^2)=1$ and so $d\mid 5$. It follows that at least one of the numbers $x+2$ and $\frac{x^5+2^5}{x+2}$ does not divide 3, and since both are congruent to 3 (mod 4), $y_1^2+4$ has a prime divisor of the form $4k+3$, contradicting Theorem 4.4.2.(1). In conclusion, the equation is not solvable in integers.

**Example 4.** *Prove that for no integer $n$ is $n^7+7$ a perfect square.*

(Titu Andreescu)

*Solution.* For $n$ even, $n^7+7 \equiv 3 \pmod 4$, so it cannot be a perfect square. For $n \equiv 3 \pmod 4$, $n^7+7 \equiv 2 \pmod 4$, so again it cannot be a perfect square. For $n \equiv 1 \pmod 4$, if $n^7+7 = q^2$, for some integer $q$, then $n^7+2^7 = q^2+11^2$, so $n+2$ is a divisor of $q^2+11^2$, $n+2 \equiv 3 \pmod 4$, and if $\gcd(q,11) = 1$, this contradicts Theorem 4.4.2.(1). If $q$ is divisible by 11, then $q = 11q_1$ and $n^7+2^7 = 11^2(q_1^2+1)$. We will prove that if $d = \gcd\left(n+2, \frac{n^7+2^7}{n+2}\right)$, then $d \mid 7$. Indeed, from the identities

$$a^7+b^7 = (a+b)^7 - 7ab(a+b)(a^2+ab+b^2)^2$$

and

$$a^2+ab+b^2 = (a+b)^2 - ab,$$

it follows that

$$\frac{a^7+b^7}{a+b} = (a+b)^6 - 7ab(a+b)^4 + 14a^2b^2(a+b)^2 - 7a^3b^3.$$

For $a = n$ and $b = 2$, $d \mid a+b$ and $d \mid \frac{a^7+b^7}{a+b}$; hence $d \mid 7a^3b^3 = 7 \cdot (2n)^3$. But $\gcd(n+2, 2n) = 1$, since $n$ is odd, so $\gcd(d, (2n)^3) = 1$ and so $d \mid 7$. It follows that at least one of the numbers $n+2$ and $\frac{n^7+2^7}{n+2}$ does not divide 11, and since both are congruent to 3 (mod 4), $q_1^2+1$ has a divisor of the form $4k+3$, contradicting Theorem 4.4.1.

### 4.4.2 Divisors of $a^2+2b^2$

**Theorem 4.4.4.** *An odd prime $p$ can be written as $p = a^2+2b^2$ for some integers $a$ and $b$ if and only if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.*

*Proof.* If $p = a^2+2b^2$, then $a^2 \equiv -2b^2 \pmod p$. Let $b'$ be an integer for which $bb' \equiv 1 \pmod p$. Then $(ab')^2 \equiv -2 \pmod p$, that

is, $\left(\frac{-2}{p}\right) = 1$. It follows that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}};$$

hence $\left(-\frac{2}{p}\right) = 1$ if and only if $\frac{p-1}{2} + \frac{p^2-1}{8} = 2k$, for some integer $k$. This is equivalent to $\frac{(p-1)(p+5)}{8} = 2k$, which amounts to $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

Conversely, suppose $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. Then $\left(\frac{-2}{p}\right) = 1$ and $a^2 \equiv -2 \pmod p$ for some integer $a$. Using Thue's lemma (Theorem 4.4.3), it follows that there exist integers $x$ and $y$, with $0 < x, y < \sqrt{p}$, such that $p \mid ax \pm y$ for a choice of signs $+$ and $-$. Therefore $p \mid a^2x^2 - y^2$, and so $p \mid (a^2+2)x^2 - (2x^2+y^2)$. But $p \mid a^2 + 2$, implying $2x^2 + y^2 = pk$, $k \in \mathbb{Z}$, and $0 < 2x^2 + y^2 < 3p$, yielding $k \in \{1, 2\}$.

For $k = 1$, we get $p = 2x^2 + y^2$ and we are done. For $k = 2$, $2p = 2x^2 + y^2$; hence $2 \mid y$. Then we can write $y = 2y$, so $p = x^2 + 2y^2$, and we are done again.

**Remarks.** (1) The result in the theorem above shows that each prime $p$ that is congruent to 1 or 3 modulo 8 is not irreducible in the ring $\mathbb{Z}[\sqrt{-2}]$.

(2) If $p$ is a prime of the form $8k - 1$ or $8k - 3$ and $p \mid a^2 + 2b^2$, then $p \mid a$ and $p \mid b$.

Indeed, if $p \nmid a$, then $p \nmid b$ and we can find an integer $b'$ such that $bb' \equiv 1 \pmod p$. From $a^2 \equiv -2b^2 \pmod p$, it follows that $(ab')^2 \equiv -2 \pmod p$. Because $\gcd(ab', p) = 1$, we get $\left(\frac{-2}{p}\right) = 1$, yielding $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$, a contradiction.

We can use the above results in the study of certain Diophantine equations as follows:

If one side of an equation can be written as $x^2 + 2y^2$ with $\gcd(x, y) = 1$, while the other side has a prime divisor congruent to $-1$ or $-3$ modulo 8, then the equation is not solvable in integers.

**Example 1.** *Prove that the equation*

$$x^3 - 3 = 2y^2$$

*is not solvable in integers.*

(Ion Cucurezeanu)

*Solution.* Write the equation in the equivalent form

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

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

Note that both right-hand sides are not divisible by 8. Because $x$ is odd, we need to examine the cases $x = 8k \pm 1$ and $x = 8k \pm 3$.

If $x = 8k + 1$, the left-hand side of (i) is divisible by 8, a contradiction. The same is true for (ii) when $x = 8k - 1$.

If $x = 8k \pm 3$, $x^2 - x + 1$ is of the form $8m - 1$ or $8m - 3$, and has a prime divisor of this form, so, according to Theorem 4.4.4, cannot divide $y^2 + 2$.

### 4.4.3 Divisors of $a^2 - 2b^2$

**Theorem 4.4.5.** *An odd prime $p$ can be written as $p = a^2 - 2b^2$ for some integers $a$ and $b$ if and only if $p \equiv 1 \pmod 8$ or $p \equiv -1 \pmod 8$.*

*Proof.* Indeed, if $p = a^2 - 2b^2$, then $a^2 \equiv 2b^2 \pmod p$. Let $b'$ be an integer such that $bb' \equiv 1 \pmod 8$, so $(ab')^2 \equiv 2 \pmod p$, yielding

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

and we have $\left(\frac{2}{p}\right) = 1$ if only if $p \equiv 1 \pmod 8$, or $p \equiv -1 \pmod 8$.

Conversely, if $p \equiv 1 \pmod 8$, or $p \equiv -1 \pmod 8$, by Thue's lemma we can find positive integers $x$ and $y$ with $0 < x, y < \sqrt{p}$ such that $p \mid a^2x^2 - y^2$, where $a$ is an integer such that $a^2 \equiv 2 \pmod p$. Hence $p \mid (a^2 - 2)x^2 + 2x^2 - y^2$, so $p \mid 2x^2 - y^2$. We obtain $0 < 2x^2 - y^2 < 2p$, yielding $p = 2x^2 - y^2$. □

**Remarks.** (1) If $p$ is a prime of the form $8k - 3$ or $8k + 3$, and $p \mid a^2 - 2b^2$, then $p \mid a$ and $p \mid b$.

(2) If $p$ is a prime congruent to $\pm 1 \pmod 8$, then the general Pell equation $x^2 - 2y^2 = p$ is solvable.

In order to prove the property in the first remark, suppose $p \nmid a$. Then $p \nmid b$, and hence $bb' \equiv 1 \pmod p$ for some integer $b'$. It follows that $(ab')^2 \equiv 2 \pmod p$. Because $\gcd(ab', p) = 1$, we have $\left(\frac{2}{p}\right) = 1$; hence $p \equiv \pm 1 \pmod 8$, a contradiction.

We can use the result in Theorem 4.4.5 as follows:

If one side of an equation can be written as $x^2 - 2y^2$, with $\gcd(x, y) = 1$, while the other side has a prime divisor congruent to $\pm 3 \pmod 8$, then the equation is not solvable in integers.

**Example 1.** *Consider the equation*

$$8xy - (x + y) = z^2.$$

*Prove that:*

*(1) It is not solvable in positive integers.*

*(2) The equation has infinitely many solutions in negative integers.*

*Solution.* (1) Write the equation as

$$(8x-1)(8y-1) = 8z^2 + 1$$

and assume that it is solvable in positive integers. Because $8x-1 \geq 7$, it has a prime divisor of the form $8m-1$ or $8m-3$, and according to Theorem 4.4.4, $8x-1$ cannot divide $2(2z)^2+1$, a contradiction.

(2) The triples $(x, y, z)$, where

$$x = -1, \quad y = -9n^2 - 2n, \quad z = -9n - 1,$$

where $n$ is any positive integer, are negative integer solutions.

## Exercises and Problems

**1.** Let $p$ be a prime of the form $4k+3$. Prove that the system of equations

$$\begin{cases} (p-1)x^2 + y^2 = u^2, \\ x^2 + (p-1)y^2 = v^2, \end{cases}$$

is not solvable in nonzero integers.

**2.** Prove that the equation $x^2 + y^2 = z^n + 2^n$ is not solvable if $\gcd(x, y) = 1$ and $n$ is an odd integer greater than 1.

(Ion Cucurezeanu)

**3.** Prove that for any integer $n$ greater than 1, the equation

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

is not solvable.

(Ion Cucurezeanu)

# Part II

# Solutions to Exercises and Problems

# II.1

# Solutions to Elementary Methods for Solving Diophantine Equations

## 1.1 The Factoring Method

**1.** *Solve the following equation in integers* $x, y$ :

$$x^2 + 6xy + 8y^2 + 3x + 6y = 2.$$

*Solution.* Write the equation in the form

$$(x + 2y)(x + 4y) + 3(x + 2y) = 2 \quad \text{or} \quad (x + 2y)(x + 4y + 3) = 2.$$

We obtain the solutions $(0, -1)$, $(3, -2)$, $(3, -1)$, $(6, -2)$.

**2.** *For each positive integer* $n$*, let* $s(n)$ *denote the number of ordered pairs* $(x, y)$ *of positive integers for which*

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

*Find all positive integers* $n$ *for which* $s(n) = 5$.

(Indian Mathematical Olympiad)

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, 193
DOI 10.1007/978-0-8176-4549-6_5, © Springer Science+Business Media, LLC 2010

*Solution.* Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. From the remark in Example 2, it follows that $(2\alpha_1 + 1) \cdots (2\alpha_k + 1) = 5$. Hence $k = 1$ and $\alpha_1 = 2$. Thus $n = p^2$, where $p$ is a prime.

**3.** *Let $p$ and $q$ be distinct prime numbers. Find the number of pairs of positive integers $x, y$ that satisfy the equation*

$$\frac{p}{x} + \frac{q}{y} = 1.$$

(KöMaL)

*Solution.* The equation is equivalent to $(x - p)(y - q) = pq$. There are four solutions:

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

**Remark.** For the equation

$$\frac{m}{x} + \frac{n}{y} = 1,$$

where $m$ and $n$ are positive integers, denote by $s(m, n)$ the number of all solutions in positive integers. For any positive integer $N > 1$ denote by $\tau(N)$ the number of all its divisors. We have $s(m, n) = \tau(mn)$ with the convention $\tau(1) = 0$.

If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where some of the exponents can be zero, it follows that

$$s(m, n) = (\alpha_1 + \beta_1 + 1)(\alpha_2 + \beta_2 + 1) \cdots (\alpha_k + \beta_k + 1).$$

**4.** *Find the positive integer solutions to the equation*

$$x^3 - y^3 = xy + 61.$$

(Russian Mathematical Olympiad)

*First Solution.* Multiplying the equation by 27 and subtracting 1 from both sides, we obtain

$$(3x)^3 + (-3y)^3 + (-1)^3 - 3(3x)(-3y)(-1) = 1642.$$

The left-hand side is of the form $a^3 + b^3 + c^3 - 3abc$, and as we have seen in Example 5, it factors as

$$(3x - 3y - 1)(9x^2 + 9y^2 + 1 + 9xy + 3x - 3y) = 2 \cdot 823.$$

Since the second factor in the left-hand side is larger than the first, taking into account that 823 is a prime and that $3x - 3y - 1 \equiv 2 \pmod 3$, it follows that $3x - 3y - 1 = 2$ and that

$$9x^2 + 9y^2 + 1 + 9xy + 3x - 3y = 823.$$

The solution is $(6, 5)$.

*Second Solution.* It is clear that $x > y$. Let $x - y = d$, so $x = y + d$. The equation is equivalent to $3y^2d + 3yd^2 + d^3 = y^2 + dy + 61$. We get $(3d - 1)y^2 + (3d^2 - 1)y + d^3 = 61$. The last relation implies $d^3 < 61$; hence $d = 1, 2, 3$.

If $d = 1$, then $2y^2 + 2y + 1 = 6$, yielding $y = 5$ and $x = 6$.

If $d = 2$ and $d = 3$, then the equation in $y$ has no integral solutions.

**5.** *Solve the Diophantine equation*

$$x - y^4 = 4,$$

*where $x$ is a prime.*

*Solution.* The equation is equivalent to $x = (y^2 + 2)^2 - (2y)^2$, i.e.,

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

If $y \neq \pm 1$, $x$ is a product of two integers greater than 1; hence it is not a prime. The solutions are $(5, 1)$, $(5, -1)$.

**6.** *Find all pairs of integers $(x, y)$ such that*

$$x^6 + 3x^3 + 1 = y^4.$$

(Romanian Mathematical Olympiad)

*Solution.* Write the equation in the form $(x^3+1)^2+(x^3+1) = y^4+1$, or equivalently, $(2x^3 + 3)^2 - 4y^4 = 5$. We obtain the systems

$$\begin{cases} 2x^3 - 2y^2 + 3 = 1, \\ 2x^3 + 2y^2 + 3 = 5, \end{cases} \quad \begin{cases} 2x^3 - 2y^2 + 3 = -1, \\ 2x^3 + 2y^2 + 3 = -5, \end{cases}$$

$$\begin{cases} 2x^3 - 2y^2 + 3 = 5, \\ 2x^3 + 2y^2 + 3 = 1, \end{cases} \quad \begin{cases} 2x^3 - 2y^2 + 3 = -5, \\ 2x^3 + 2y^2 + 3 = -1. \end{cases}$$

The solutions are $(0, 1)$, $(0, -1)$.

**7.** *Solve the following equation in nonzero integers $x, y$:*

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

(16th USA Mathematical Olympiad)

*Solution.* The equation is equivalent to the following quadratic equation in $y$:

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

This equation has integral solutions if and only if its discriminant $x(x + 1)^2(x - 8)$ is a perfect square. It follows that $x(x - 8) = z^2$ or $(x-4)^2-z^2 = 16$. This leads to the equation $(x-z-4)(x+z-4) = 16$.

We obtain $x \in \{-1, 8, 9\}$; hence the solutions are $(-1, -1)$, $(8, -10)$, $(9, -6)$, $(9, -21)$.

**8.** *Find all integers $a, b, c$ with $1 < a < b < c$ such that the number $(a-1)(b-1)(c-1)$ is a divisor of $abc - 1$.*

(33rd IMO)

*Solution.* It is convenient to let $a-1 = x$, $b-1 = y$, and $c-1 = z$. Then $1 \le x < y < z$ and $xyz \mid (xy + yz + zx + x + y + z)$.

The idea of a solution is to point out that we cannot have $xyz \le xy+yz+zx+x+y+z$ for infinitely many triples $(x, y, z)$ of positive integers. Let $f(x, y, z)$ be the quotient of the required divisibility.

From the algebraic form

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

we can see that $f$ is a decreasing function in each of the variables $x, y, z$. By symmetry and because $x, y, z$ are distinct numbers,

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

Thus, if the divisibility is fulfilled we can have either $f(x, y, z) = 1$ or $f(x, y, z) = 2$. So, we have to solve in positive integers the equations

$$xy + yz + zx + x + y + z = kxyz \tag{1}$$

where $k = 1$ or $k = 2$.

Observe that $f(3, 4, 5) = \frac{59}{60} < 1$. Thus $x \in \{1, 2\}$. Also $f(2, 3, 4) = \frac{35}{24} < 2$. Thus, for $x = 2$, we necessarily have $k = 1$. The conclusion is that only three equations have to be considered in (1).

*Case 1*: $x = 1$ and $k = 1$. We obtain the equation

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

It has no solutions.

*Case 2*: $x = 1$ and $k = 2$. We obtain the equation

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

Write it in the form $(y - 2)(z - 2) = 5$ and obtain $y - 2 = 1$, $z - 2 = 5$. It has unique solution: $y = 3$, $z = 7$.

*Case 3*: $x = 2$ and $k = 1$. We obtain the equation

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

By writing it in the form $(y-3)(z-3) = 11$, we obtain $y-3 = 1$, $z - 3 = 11$. Thus, it has a unique solution: $y = 4$, $z = 14$.

From *Case 2* and *Case 3* we obtain respectively $a = 2$, $b = 4$, $c = 8$, and $a = 3$, $b = 5$, $c = 15$. These are the solutions to the problem.

**9.** *Find all right triangles with integer side lengths such that their areas and perimeters are equal.*

*Solution.* Let $x, y$ be the lengths of the legs and let $z$ be the length of the hypotenuse. Then $z = \sqrt{x^2 + y^2}$ by the Pythagorean theorem. Equating the area and perimeter yields

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

Multiply by 2, isolate the radical, and square. This yields

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

or

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

We have

$$x^2y^2 - 4xy(x+y) + 8xy = 0.$$

Clearly, we should divide out by $xy$, since it is never equal to zero. We get

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

Add 8 to both sides to make the left-hand side factor. We now have

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

and since the variables are integers, there are only finitely many possibilities. The only solutions $(x, y)$ are $(6, 8), (8, 6), (5, 12), (12, 5)$, which yield just two right triangles, namely the 6-8-10 and the 5-12-13 triangles.

**10.** *Solve the following system in integers* $x, y, z, u, v$ :

$$\begin{cases} x+y+z+u+v = xyuv + (x+y)(u+v), \\ xy+z+uv = xy(u+v) + uv(x+y). \end{cases}$$

(Titu Andreescu)

*Solution.* Subtracting the second equation from the first yields

$$(x+y-xy) + (u+v-uv) = (x+y-xy)(u+v-uv),$$

or

$$[(x+y-xy)-1][(u+v-uv)-1] = 1,$$

which is equivalent to $(1-x)(1-y)(1-u)(1-v) = 1$. The last equation has solutions $(0,0,0,0), (0,0,2,2), (0,2,0,2), (0,2,2,0)$,

$(2,0,0,2), (2,0,2,0), (2,2,0,0), (2,2,2,2)$. The solutions $(x,y,z,u,v)$ of the system are: $(0,0,0,0,0)$, $(0,0,-4,2,2)$, $(0,2,0,0,2)$, $(0,2,0,2,0)$, $(2,0,0,0,2)$, $(2,0,0,2,0)$, $(2,2,-4,0,0)$, $(2,2,24,2,2)$.

**11.** *Prove that the equation $x(x+1) = p^{2n}y(y+1)$ is not solvable in positive integers, where $p$ is a prime and $n$ is a positive integer.*

*Solution.* We have $p^{2n} \mid x$ or $p^{2n} \mid x+1$; hence in any case $p^{2n} \leq x+1$. The equation can be written as $(2x+1)^2-1 = p^{2n}(2y+1)^2-p^{2n}$; hence

$$\begin{aligned} p^{2n}-1 &= p^{2n}(2y+1)^2-(2x+1)^2 \\ &= [p^n(2y+1)+(2x+1)][p^n(2y+1)-(2x+1)]; \end{aligned}$$

hence $p^{2n}-1 > (2x+1)\cdot 1$, contradicting $p^{2n} \leq x+1$.

**Remark.** The conclusion does not remain true if the exponent of $p$ is not even. For example the equation

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

has solutions $(x,y) = (15,5)$ and $(x,y) = (32,11)$.

**12.** *Find all triples $(x,y,p)$, where $x$ and $y$ are positive integers and $p$ is a prime satisfying the equation*

$$x^5+x^4+1 = p^y.$$

(Titu Andreescu)

*Solution.* Clearly, $(x,y,p) = (1,1,3)$ and $(x,y,p) = (2,2,7)$ are solutions. We have

$$\begin{aligned} x^5+x^4+1 &= x^5+x^4+x^3-(x^3-1) = x^3(x^2+x+1)-(x^3-1) \\ &= (x^2+x+1)(x^3-x+1); \end{aligned}$$

hence we can write the equation as

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

and let $d = \gcd(x^2 + x + 1, x^3 - x + 1)$. Then $d$ divides

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

so $d$ divides $x^2 + x - 1 - (x - 2)(x + 3) = 7$. Hence $d = 7$ for $x > 1$, so $p = 7$. It follows that for $x > 2$, $x^2 + x + 1 = 7^a$ and $x^3 - x + 1 = 7^b$ for some integers $a \geq 2$ and $b \geq 2$. This means that 49 divides $x^2 + x + 1$ and $x^3 - x + 1$, contradicting $d = 7$. Thus $(1, 1, 3)$ and $(2, 2, 7)$ are the only solutions.

**13.** *Find all pairs $(x, y)$ of integers such that*

$$xy + \frac{x^3 + y^3}{3} = 2007.$$

(Titu Andreescu)

*Solution.* Write the equation as

$$x^3 + y^3 + 3xy = 6021,$$

or equivalently,

$$x^3 + y^3 + (-1)^3 - 3xy(-1) = 6020.$$

It follows that

$$(x + y - 1)(x^2 + y^2 + 1 - xy + x + y) = 6020,$$

which can be written as

$$(x + y - 1)[(x + y)(x + y + 1) + 1 - 3xy] = 2^2 \cdot 5 \cdot 7 \cdot 43.$$

Because

$$(x+y)(x+y+1)+1-3xy > x+y-1,$$

out of the 24 factors of 6020, only 12 can be potential candidates for $x+y-1$.

Also, since $6020 \equiv 2 \pmod 3$, we can easily observe that only when $x+y-1 \equiv 2 \pmod 3$ will we have integer solutions for $xy$. This again reduces the number of possible candidates for $x+y-1$, now to only five, namely 2, 5, 14, 20, and 35. Examining each of them, we find that only $x+y-1=20$ gives integer solutions for $(x,y)$. Hence using $x+y-1=20$, we find the solutions $(3,18)$ and $(18,3)$. Both satisfy the given equation.

## 1.2 Solving Diophantine Equations Using Inequalities

**1.** *Solve in positive integers the equation*

$$3(xy+yz+zx)=4xyz.$$

*Solution.* The equation is equivalent to $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{4}{3}$. Considering $x \le y \le z$, it follows that $\frac{3}{x} \ge \frac{4}{3}$, i.e., $x \le \frac{9}{4}$. Therefore $x \in \{1,2\}$. Analyzing the two, cases we obtain the solutions $(1,4,12)$, $(1,6,6)$, $(2,2,3)$ and all their permutations.

**2.** *Find all triples of positive integers $(x,y,z)$ such that*

$$xy+yz+zx-xyz=2.$$

*First Solution.* Let $u=x-1$, $v=y-1$, $w=z-1$. The equation becomes $u+v+w=uvw$. We either have $(u,v,w)=(0,0,0)$ or

$uvw \neq 0$. In the latter case the equation is equivalent to

$$\frac{1}{vw} + \frac{1}{wu} + \frac{1}{uv} = 1,$$

which is of the type $\frac{1}{m} + \frac{1}{n} + \frac{1}{p} = 1$. Assuming $m \leq n \leq p$, we obtain the solutions $(m, n, p) = (2, 3, 6)$, (2,4,4), (3,3,3). The last two situations are not possible, since $(uvw)^2 = 32$ and $(uvw)^2 = 27$, respectively. We obtain $vw = 2$, $wu = 3$, $uv = 6$, yielding $uvw = 6$, and $u = 3$, $v = 2$, $w = 1$. The solutions $(x, y, z)$ are $(1, 1, 1)$ and $(4, 3, 2)$ and all permutations.

*Second Solution.* From the equation it follows that $xy + yz + zx > xyz$; hence $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} > 1$. Assuming that $x \leq y \leq z$, from the last relation we obtain $\frac{3}{x} > 1$, that is, $x \in \{1, 2\}$.

If $x = 1$, then the equation becomes $y + z = 2$; hence $y = z = 1$, giving the solution $(1, 1, 1)$.

If $x = 2$, then the equation is equivalent to $2y + 2z - yz = 2$; hence $(y - 2)(z - 2) = 2$, giving the solution $(2, 3, 4)$.

**3.** *Determine all triples of positive integers $(x, y, z)$ that are solutions to the equation*

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

(Romanian Mathematical Olympiad)

*Solution.* The inequalities $(x + y)^2 < (x + y)^2 + 3x + y + 1 < (x + y + 2)^2$ imply $(x + y)^2 + 3x + y + 1 = (x + y + 1)^2$. It follows that $x = y = k \in \mathbb{Z}_+$; hence all the solutions are $(k, k, 2k + 1)$.

**4.** *Determine all pairs of integers $(x, y)$ that satisfy the equation*

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

(Australian Mathematical Olympiad)

*Solution.* We have $(x+1)^4-(x-1)^4 = 8x^3+8x$. Suppose a pair $(x,y)$ of integers is a solution and assume $x \geq 1$. Then $(2x)^3 < (x+1)^4-(x-1)^4 < (2x+1)^3$. Hence $2x < y < 2x+1$, a contradiction. Therefore for every solution $(x,y)$, the integer $x$ must be nonpositive. Now observe that if $(x,y)$ is a solution, then $(-x,-y)$ is also a solution; hence $-x$ must be nonpositive. Therefore $(0,0)$ is the only solution.

**5.** *Prove that all the equations*

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

*where* $a \in \{3,4,5\}$, $b \in \{4,5,\ldots,12\}$, $c \in \{1,2,\ldots,8\}$, *are not solvable in positive integers.*

(Dorin Andrica)

*Solution.* The given conditions imply $x^6+3x^4+3x^2+1 < y^3 < x^6+6x^4+12x^2+8$, i.e., $(x^2+1)^3 < y^3 < (x^2+2)^3$, which shows that each of the considered equations is not solvable.

**6.** *Solve in positive integers the equation*

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

*Solution.* Note that this is the equality case in the AM–GM inequality

$$x^2y+y^2z+z^2x \geq 3\sqrt[3]{(x^2y)(y^2z)(z^2x)}.$$

Hence we must have $x^2y = y^2z = z^2x$, which implies $x^2 = yz$, $y^2 = zx$, $z^2 = xy$, i.e., $(x-y)^2+(y-z)^2+(z-x)^2 = 0$. The solutions are $(k,k,k)$, $k \in \mathbb{Z}_+$.

**7.** *Find all integer solutions to the equation*

$$(x^2 - y^2)^2 = 1 + 16y.$$

(Russian Mathematical Olympiad)

*Solution.* The solutions are $(\pm 1, 0)$, $(\pm 4, 3)$, $(\pm 4, 5)$. We must have $y \geq 0$. Since the right-hand side is nonzero, so then must be the left hand side; hence $|x| \geq |y| + 1$ or $|x| \leq |y| - 1$. In either case, $(x^2 - y^2)^2 \geq (2y - 1)^2$, so $(2y - 1)^2 \leq 1 + 16y$, and hence $y \leq 5$. Trying all such values of $y$ yields the above solutions.

**8.** *Find all integers* $(a, b, c, x, y, z)$ *such that*

$$a + b + c = xyz$$

$$x + y + z = abc$$

*and* $a \geq b \geq c \geq 1$, $x \geq y \geq z \geq 1$.

(Polish Mathematical Olympiad)

*First Solution.* First we claim that at least one of $bc$ and $yz$ is less than 3. If $bc = 3$, then $b = 3$, $c = 1$, $a + b + c < 3a = abc$; if $bc > 3$, then $abc > 3a \geq a + b + c$. Thus for $bc \geq 3$, we have $abc > a + b + c$ and

$$3x \geq x + y + z = abc > a + b + c = xyz \;\Rightarrow\; 3 > yz.$$

This proves our claim. Without loss of generality, suppose that $yz = 1$ or 2.

If $yz = 1$, then $y = z = 1$. We have

$$abc = x + y + z = x + 2 = xyz + 2 = a + b + c + 2.$$

If $c \geq 2$, then $bc \geq 4$ and $4a \leq abc = a+b+c+2 \leq 4a$; thus $a = b = c = 2$. We obtain the solutions $(2,2,2,6,1,1)$ and $(6,1,1,2,2,2)$. If $c = 1$, then $ab = a+b+3$. If $b \geq 3$, then $3a \leq ab = a+b+3 \leq 3a \Rightarrow a = b = 3$. We obtain the solutions $(3,3,1,7,1,1)$ and $(7,1,1,3,3,1)$. If $b = 2$, we have $a = 5$ and obtain the solutions $(5,2,1,8,1,1)$ and $(8,1,1,5,2,1)$. If $b = 1$, we have $a = a+4$, which is impossible.

If $yz = 2$, then $y = 2$, $z = 1$. We have

$$2abc = 2(x+y+z) = 2x+6 = xyz+6 = a+b+c+6 \leq 3a+6.$$

If $c \geq 2$, then $8a \leq 2abc \leq 3a+6 \Rightarrow 5a < 6$, which contradicts the fact that $a \geq c$. Thus $c = 1$, and $2ab = a+b+7$. If $b \geq 3$, then $6a \leq 2ab = a+b+7 \Rightarrow a \leq b/5 + 7/5$, which contradicts the fact that $a \geq b$. If $b = 2$, then $4a = 2ab = a+9$ and $a = 3$. We obtain the solution $(3,2,1,3,2,1)$. If $b = 1$, we have $a = 8$, repeating the solution $(8,1,1,5,2,1)$.

*Second Solution.* Let

$$A = (ab-1)(c-1), \quad B = (a-1)(b-1),$$
$$X = (xy-1)(z-1), \quad Y = (x-1)(y-1).$$

Thus $A, B, X, Y$ are nonnegative integers such that

$$A+B+X+Y = 4.$$

Clearly, neither of $c$ and $z$ can be greater than 2; that would force either $A$ or $X$ to be greater than 4, and contradict the fact that $A+B+X+Y = 4$.

If $c = 2$, we have $a, b \geq 2$ and $A \geq 3$, $B \geq 1$. Thus $A = 3$, $B = 1$, $X = Y = 0$. This yields the solution $(2, 2, 2, 6, 1, 1)$. Similarly, if $z = 2$, we have $(6, 1, 1, 2, 2, 2)$ as a solution.

Now we suppose that $c = z = 1$. We have $A = X = 0$ and $B + Y = 4$. Without loss of generality, suppose that $Y \leq B$, (i.e., $Y = 0, 1, 2$).

If $Y = 0$, we have $B = (a-1)(b-1) = 4$. This leads to the solutions $(5, 2, 1, 8, 1, 1)$ and $(3, 3, 1, 7, 1, 1)$. By symmetry, we also have the solutions $(8, 1, 1, 5, 2, 1)$ and $(7, 1, 1, 3, 3, 1)$.

If $Y = 1$, then $x = y = 2$ and $B = (a-1)(b-1) = 3 \Rightarrow a = 4$, $b = 2$, but $a + b + c = 7 \neq xyz$.

If $Y = 2$, then $(x-1)(y-1) = (a-1)(b-1) = 2 \Rightarrow a = x = 3$, $b = y = 2$. We obtain $(3, 2, 1, 3, 2, 1)$ as our last solution.

**9.** *Let $x, y, z, u,$ and $v$ be positive integers such that*

$$xyzuv = x + y + z + u + v.$$

*Find the maximum possible value of* $\max\{x, y, z, u, v\}$.

*First Solution.* Suppose that $x \leq y \leq z \leq u \leq v$. We need to find the maximum value of $v$. Since

$$v < x + y + z + u + v \leq 5v,$$

then $v < xyzuv \leq 5v$ or $1 < xyzu \leq 5$. Hence $(x, y, z, u) = (1, 1, 1, 2)$, $(1, 1, 1, 3)$, $(1, 1, 1, 4)$, $(1, 1, 2, 2)$, or $(1, 1, 1, 5)$, which leads to $\max\{v\} = 5$.

*Second Solution.* Note that

$$1 = \frac{1}{yzuv} + \frac{1}{zuvx} + \frac{1}{uvxy} + \frac{1}{vxyz} + \frac{1}{xyzu}$$

$$\leq \frac{1}{uv} + \frac{1}{uv} + \frac{1}{uv} + \frac{1}{v} + \frac{1}{u} = \frac{3+u+v}{uv}.$$

Therefore, $uv \leq 3+u+v$ or $(u-1)(v-1) \leq 4$. If $u=1$, then $x=y=z=1$ and $4+v=v$, which is impossible. Thus $u-1 \geq 1$ and $v-1 \leq 4$ or $v \leq 5$. It is easy to see that $(1,1,1,2,5)$ is a solution. Therefore $\max\{v\} = 5$.

**Remark.** The second solution can be used to determine the maximum value of $\max\{x_1, x_2, \ldots, x_n\}$ when $x_1, x_2, \ldots, x_n$ are positive integers such that

$$x_1 x_2 \cdots x_n = x_1 + x_2 + \cdots + x_n.$$

**10.** *Solve in distinct positive integers the equation*

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

(Titu Andreescu)

*First Solution.* Without loss of generality, assume that $x < y < z < w$. Then $x \geq 1$, $y \geq 2$, $z \geq 3$, $w \geq 4$.

We have

$$x^2 + y^2 + z^2 + w^2 = 3(x+y+z+w)$$

$$1 \leq y - x, \quad 9 \leq 3z, \quad 20 \leq 5w.$$

Adding up the last relations yields

$$(x-1)^2 + (y-2)^2 + (z-3)^2 + (w-4)^2 \leq 0;$$

hence $x = 1$, $y = 2$, $z = 3$, $w = 4$.

All solutions to the given equation are $(1, 2, 3, 4)$ and their permutations.

*Second Solution.* Note that the Cauchy–Schwarz inequality (noting that $x, y, z$, and $w$ distinct precludes equality) gives

$$(x + y + z + w)^2 < 4(x^2 + y^2 + z^2 + w^2) = 12(x + y + z + w);$$

hence $x + y + z + w \leq 11$. This leaves only two possibilities if we assume without loss of generality, that $x < y < z < w$, namely $(1, 2, 3, 4)$, which works, and $(1, 2, 3, 5)$ which fails.

**11.** *Find all positive integers $x, y, z, t$ such that*

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

*for some integer $n \geq 2$.*

*Solution.* There are no solutions. From the first equation we get $x^n = z^n - y < z^n$, thus $x < z$ or $x + 1 \leq z$. The same equation gives

$$y = z^n - x^n \geq (x + 1)^n - x^n = \binom{n}{1} x^{n-1} + \binom{n}{2} x^{n-2} + \cdots > x,$$

i.e., $y > x$. Similarly, using the second equation one gets $y < x$, contradiction.

**12.** *Find all pairs $(x, y)$ of positive integers such that $x^y = y^x$.*

*First Solution.* Obviously, all the pairs $(n, n)$, $n \geq 1$, are solutions. We explore whether there are any others. Assume, without loss of generality, that $x < y$ and let $y = x + t$ for some integer $t > 0$. The equation becomes

$$x^{x+t} = (x + t)^x \quad \text{or} \quad x^t = \left(1 + \frac{t}{x}\right)^x < e^t < 3^t.$$

Thus $x < 3$. Since $x$ is an integer, $x = 1$ or $x = 2$.

If $x = 1$, then $y = 1$.

If $x = 2$, we have $2^y = y^2$, which has the solutions $y = 2$, $y = 4$. For $y > 4$ an induction argument shows that $2^y > y^2$. Thus, the solutions are $(n, n)$, $n \geq 1$, $(2, 4)$ and $(4, 2)$.

*Second Solution.* Since $f(t) = \frac{\ln t}{t}$ is decreasing on $[e, \infty)$, we have $x^y > y^x$ if $y > x \geq e$. This forces $x = y$ or one of $x$ and $y$ (without loss of generality $x$) to be 1 or 2, and we can follow the end of the previous solution.

**13.** *Solve in positive integers the equation* $x^y + y = y^x + x$.

*First Solution.* Obvious solutions: $(n, n)$, $(1, n)$, $(n, 1)$. Let $x < y$, $y = x + t$ for some integer $t > 0$. We have

$$x^{x+t} + x + t = (x + t)^x + x,$$

or

$$x^t + \frac{t}{x^x} = \left(1 + \frac{t}{x}\right)^x < 3^t;$$

thus $x < 3$.

The situation $x = 1$ has already been taken care of. Let then $x = 2$. The equation becomes

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

which admits $t = 0$ and $t = 1$ as solutions. For $t \geq 2$ an induction argument shows that

$$2^t > 1 + \frac{3t}{4} + \frac{t^2}{4}.$$

Now, for $t = 0$ we get $x = y = 2$, and for $t = 1$ we have $x = 2$, $y = 3$. The solutions are $(n, n)$, $(1, n)$, $(n, 1)$, $(2, 3)$, $(3, 2)$, $n \geq 1$.

*Second Solution.* The function $f(t) = \frac{\ln t}{t}$ is decreasing on $[e, \infty)$; hence $x^y + y > y^x + x$ if $xy \geq e$. We get $x = y$ or, without loss of generality, $x = 1$, $x = 2$, $x = 3$, and we continue as in the previous solution.

**14.** *Let $a$ and $b$ be positive integers such that $ab+1$ divides $a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is the square of an integer.*

(29th IMO)

*Solution.* Let $(a, b)$ be a pair of integers satisfying the hypothesis. Then $(a, b)$ is a solution of the Diophantine equation

$$a^2 - kab + b^2 = k. \tag{1}$$

If $a = 0$ or $b = 0$, then $k$ is a perfect square. Hence we may consider $a \neq 0$ and $b \neq 0$. In this case $a$ and $b$ have the same sign. Indeed, if $ab < 0$, we obtain

$$a^2 - kab + b^2 > k. \tag{2}$$

We may assume that $a > 0$, $b > 0$ and therefore $k > 0$. If $a = b$, from $(2 - k)a^2 = k > 0$ we deduce $k = 1$. Finally, we suppose that $a > b > 0$ and let $(a, b)$ be a solution of (1) with $b$ minimal. It is easy to see that $(b, kb - a)$ is also a solution of (1). If $kb = a$, $k$ is a perfect square. Otherwise, $kb - a > 0$, because it has the same sign as $b$. We claim that $kb - a < b$. Indeed,

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

The last inequality follows from

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

Therefore $(b, kb-a)$ is a solution, which contradicts the minimality of the solution $(a, b)$. Hence $k$ is a perfect square.

**15.** *Find all integers $n$ for which the equation*

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

*is solvable in positive integers.*

(American Mathematical Monthly, reformulation)

*Solution.* We will prove that $n$ is one the numbers 1, 2, 3, 4, 5, 6, 8, and 9.

Let

$$F(x,y,z) = (x+y+z)^2/(xyz).$$

Fix $n$ and suppose $n = F(x,y,z)$, with $x \le y \le z$ and $z$ minimal for that choice of $n$. From

$$nxyz = (x+y+z)^2 = (x+y)^2 + 2(x+y)z + z^2,$$

we infer that $z \mid (x+y)^2$. If $z > x+y$, then $(x+y)^2/z < z$ and

$$F\left(x, y, \frac{(x+y)^2}{z}\right) = \frac{\dfrac{(x+y)^2}{z^2}(x+y+z)^2}{xy\dfrac{(x+y)^2}{z}} = \frac{(x+y+z)^2}{xyz} = n.$$

Thus the minimality of $z$ implies that $x+y \ge z$. Now

$$\begin{aligned} n &= \frac{x}{yz} + \frac{y}{xz} + \frac{z}{xy} + \frac{2}{x} + \frac{2}{y} + \frac{2}{z} \\ &\le \frac{1}{z} + \frac{1}{x} + \left(\frac{1}{y} + \frac{1}{x}\right) + \frac{2}{x} + \frac{2}{y} + \frac{2}{z} \\ &\le \frac{7}{x} + \frac{3}{z}. \end{aligned}$$

This implies that $z = 1$ (and $n = 9$) or that $z \geq 2$ (and $n \leq 8$). Thus $n \leq 9$.

We next prove that $n \neq 7$. The inequality $7 \leq 7/x + 3/z$ prohibits $x \geq 2$. With $x = 1$, $x + y \geq z$ yields $y \leq z \leq y + 1$. When $z = y$ we have $(1+2y)^2 = 7y^2$, and when $z = y+1$ we have $(2+2y)^2 = 7y(y+1)$, neither of which has an integer solution.

Finally, $F(9,9,9) = 1$, $F(4,4,8) = 2$, $F(3,3,3) = 3$, $F(2,2,4) = 4$, $F(1,4,5) = 5$, $F(1,2,3) = 6$, $F(1,1,2) = 8$, and $F(1,1,1) = 9$.

## 1.3 The Parametric Method

**1.** *Prove that the equation*

$$x^2 = y^3 + z^5$$

*has infinitely many solutions in positive integers.*

*Solution.* A family of solutions is given by

$$x_n = n^{10}(n+1)^8, \quad y_n = n^7(n+1)^5, \quad z_n = n^4(n+1)^3, \quad n \in \mathbb{Z}_+.$$

**2.** *Show that the equation*

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

*has infinitely many relatively prime integral solutions.*

(United Kingdom Mathematical Olympiad)

*Solution.* We will use Lagrange's identity (see Remark 1 in Example 2) and the following two well-known results:

(1) There are infinitely many primes of the form $4k + 1$.

(2) Each prime of the form $4k+1$ is representable as the sum of two perfect squares (see the remark in the solution of Problem 12, Section 1.5, for a nice proof). Take any prime $p$ of the form $4k+1$. By (2), it can be represented as the sum of two perfect squares. The same holds for $p^4+1$, and Lagrange's identity shows that $p^5+p = p(p^4+1)$ is also representable as a sum of two perfect squares. Let $p^5+p = u^2+v^2$. Then $x = u$, $y = v$, $z = p$ is a solution of the given equation. Since $p$ is a prime, $x, y$, and $z$ are relatively prime. Now it suffices to note that (see (1)) the primes of the form $4k+1$ are infinite in number.

**Remarks. 1.** The same argument holds for the equation

$$x^2 + y^2 = z^{2n+1} + z,$$

where $n$ is a positive integer.

**2.** We can directly take $x = a(a^2+b^2)^2 - b$, $y = b(a^2+b^2)^2 + a$, and $z = a^2 + b^2$ for relatively prime $a$ and $b$.

**3.** Prove that for each integer $n \geq 2$ the equation

$$x^n + y^n = z^{n+1}$$

has infinitely many solutions in positive integers.

*Solution.* A family of solutions is given by

$$x_k = k^n + 1, \quad y_k = k(k^n+1), \quad z_k = k^n + 1, \quad k \in \mathbb{Z}_+.$$

**4.** Prove that the equation

$$x^n + y^n + z^n + u^n = v^{n-1}, \ n \geq 2,$$

has infinitely many solutions $(x, y, z, u, v)$ in positive integers.

(Dorin Andrica)

*Solution.* Let $(x_{k_1}, y_{k_1}, z_{k_1})$ and $(x_{k_2}, y_{k_2}, z_{k_2})$ be two solutions to the equation in Example 4. Then

$$x_{k_1}^n + y_{k_1}^n = z_{k_1}^{n-1}, \quad x_{k_2}^n + y_{k_2}^n = z_{k_2}^{n-1},$$

and by multiplying the last two relations we obtain

$$(x_{k_1}x_{k_2})^n + (x_{k_1}y_{k_2})^n + (y_{k_1}x_{k_2})^n + (y_{k_1}y_{k_2})^n = (z_{k_1}z_{k_2})^{n-1}.$$

Hence a family of solutions is given by

$$(x_{k_1}x_{k_2}, x_{k_1}y_{k_2}, y_{k_1}x_{k_2}, y_{k_1}y_{k_2}, z_{k_1}z_{k_2}),$$

where $k_1, k_2 \in \mathbb{Z}_+$.

**Remark.** One can simply take

$$x = a(a^n + b^n + c^n + d^n)^{n-2}, \quad y = b(a^n + b^n + c^n + d^n)^{n-2},$$
$$z = c(a^n + b^n + c^n + d^n)^{n-2}, \quad u = d(a^n + b^n + c^n + d^n)^{n-2},$$

and

$$v = (a^n + b^n + c^n + d^n)^{n+1}$$

for arbitrary integers $a, b, c, d$.

**5.** *Let $a, b, c, d$ be positive integers with $\gcd(a, b) = 1$. Prove that the system of equations*

$$\begin{cases} ax - yz - c = 0, \\ bx - yt + d = 0, \end{cases}$$

*has infinitely many solutions in positive integers.*

(Titu Andreescu)

*Solution.* Using the lemma and the remark in Example 5, there exist infinitely many pairs $(u_n, v_n)$, $n \geq 1$, of positive integers such that $au_n - bv_n = 1$. Then

$$x_n = cu_n + dv_n, \quad y_n = ad + bc, \quad z_n = v_n, \quad t_n = u_n, \quad n \in \mathbb{Z}_+,$$

are solutions of the system.

**Remark.** One can simply take $y = 1$, $z = ax - c$, and $t = bx + d$ for $x$ large enough that this gives a positive $z$.

**6.** *Find all triples of integers $(x, y, z)$ such that*

$$xy(z + 1) = (x + 1)(y + 1)z.$$

*Solution.* Writing the equation in the equivalent form

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

shows that $\frac{xy}{x+y+1}$ must be an integer. Let $x + y + 1 = u$. It follows that $\frac{x(u-x-1)}{u} \in \mathbb{Z}$, or equivalently, $\frac{x(x+1)}{u} = v \in \mathbb{Z}$. All solutions are given by

$$x = w, \quad y = u - w - 1, \quad z = w - v,$$

where $u, v, w \in \mathbb{Z}$ and $v$ is any divisor of $w(w+1)$ and $u = w(w+1)/v$.

**7.** *Solve in integers the equation*

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

*First Solution.* The equation is equivalent to

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

It follows that

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

The solutions are

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

*Second Solution.* Write the equation in the form

$$x(x - z) = y(y - x).$$

Let $d = \gcd(x, y)$. Then $x = d\alpha$, $y = d\beta$, where $\gcd(\alpha, \beta) = 1$. It follows that $y - x = k\alpha$ and $x - z = k\beta$. Since $\gcd(\alpha, \beta - \alpha) = 1$, $k\alpha = y - x = d\beta - d\alpha = d(\beta - \alpha)$ implies $\beta - \alpha \mid k$. Setting $k = m(\beta - \alpha)$, we obtain $d = m\alpha$; hence

$$x = m\alpha^2, \quad y = m\alpha\beta, \quad z = m(\alpha^2 + \alpha\beta - \beta^2), \quad m, \alpha, \beta \in \mathbb{Z}.$$

**8.** *Prove that the equation*

$$x^3 + y^3 + z^3 + w^3 = 2008$$

*has infinitely many solutions in integers.*

(Titu Andreescu)

*Solution.* For each integer $n$, the quadruple

$$(10 + 60n^3, 10 - 60n^3, 2, -60n^2)$$

is a solution to the given equation.

**9.** *Prove that there are infinitely many quadruples of positive integers $(x, y, z, w)$ such that*

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

(Titu Andreescu)

*Solution.* Note that $2002 = 3^4 + 5^4 + 6^4$. A family of solutions is given by

$$x_k = 3 \cdot 2002^k, \quad y_k = 5 \cdot 2002^k, \quad z_k = 6 \cdot 2002^k,$$
$$w_k = 4k + 1, \quad k \in \mathbb{Z}_+.$$

**10.** *Prove that each of the following equations has infinitely many solutions in integers* $(x, y, z, u)$ *such that* $\gcd(x, y, z, u) = 1$ *:*

$$x^2 + y^2 + z^2 = 2u^2,$$
$$x^4 + y^4 + z^4 = 2u^2.$$

*Solution.* A family of solutions to the first equation is given by

$$(3m^2 + 2mn - n^2, 3m^2 - 2mn - n^2, 4mn, 3m^2 + n^2), \quad m, n \in \mathbb{Z}_+,$$

$$\gcd(m, n) = 1.$$

A family of solutions to the second equation is

$$(m + n, m - n, 2m, 3m^2 + n^2), \quad m, n \in \mathbb{Z}_+, \quad \gcd(m, n) = 1.$$

**Remark.** Note that the equation

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

has also infinitely many solutions with $\gcd(x, y, z, u) = 1$. A family of such solutions is given by

$$\begin{cases} x = a^2 + 2ac - 2bc - b^2, \\ y = b^2 - 2ab - 2ac - c^2, \\ z = c^2 + 2ab + 2bc - a^2, \\ u = a^2 + b^2 + c^2 - ab + ac + bc, \end{cases}$$

where $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$.

**11.** *Prove that there are infinitely many quadruples of positive integers $(x, y, u, v)$ such that $xy + 1$, $xu + 1$, $xv + 1$, $yu + 1$, $yv + 1$, $uv + 1$ are all perfect squares.*

*Solution.* A family of solutions is

$$(n, n + 2, 4n + 4, 4(n + 1)(2n + 1)(2n + 3)), \quad n \in \mathbb{Z}_+.$$

## 1.4 The Modular Arithmetic Method

**1.** *Show that the equation*

$$(x + 1)^2 + (x + 2)^2 + \cdots + (x + 99)^2 = y^z$$

*is not solvable in integers $x, y, z$, with $z > 1$.*

(Hungarian Mathematical Olympiad)

*Solution.* We notice that

$$\begin{aligned} y^z &= (x + 1)^2 + (x + 2)^2 + \cdots + (x + 99)^2 \\ &= 99x^2 + 2(1 + 2 + \cdots + 99)x + (1^2 + 2^2 + \cdots + 99^2) \\ &= 99x^2 + \frac{2 \cdot 99 \cdot 100}{2}x + \frac{99 \cdot 100 \cdot 199}{6} \\ &= 33(3x^2 + 300x + 50 \cdot 199), \end{aligned}$$

which implies that $3 \mid y$. Since $z \geq 2$, $3^2 \mid y^z$, but $3^2$ does not divide $33(3x^2 + 300x + 50 \cdot 199)$, a contradiction.

**2.** *Find all pairs of positive integers $(x, y)$ for which*

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

(Titu Andreescu)

*Solution.* For $y$ greater than 5, $y!$ is divisible by 9, so $y! + 2001$ gives the residue 3 (mod 9), which is not a quadratic residue. Hence the only candidates are $y = 1, 2, 3, 4, 5$. Only $y = 4$ passes, giving $x = 45$.

**3.** *Prove that the equation*

$$x^3 + y^4 = 7$$

*has no solution in integers.*

*Solution.* For any integers $x, y$ we have $x^3 \equiv 0, 1, 5, 8, 12 \pmod{13}$ and $y^4 \equiv 0, 1, 3, 9 \pmod{13}$. Thus $x^3 + y^4 \not\equiv 7 \pmod{13}$.

**4.** *Find all pairs of positive integers $(x, y)$ satisfying the equation*

$$3^x - 2^y = 7.$$

*Solution.* Let us assume first that $y \geq 3$. Reducing modulo 8, we deduce that $3^x$ must give the residue 7. However, $3^x$ can be congruent only to 3 or 1 (mod 8), depending on the parity of $x$. We are left with the cases $y = 1$ and $y = 2$, which are immediate. The only solution is $x = 2$, $y = 1$.

**5.** *Determine all nonnegative integral solutions $(x_1, x_2, \ldots, x_{14})$, if any, apart from permutations, to the Diophantine equation*

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

(8th USA Mathematical Olympiad)

*Solution.* We show that the congruence

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

has no solution, which will mean that the given equation is also not solvable. Indeed, if an integer $n$ is even, then $n = 2k$ for $k \in \mathbb{Z}$, and thus $n^4 = 16k^4 \equiv 0 \pmod{16}$. If $n$ is odd, then

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

since the numbers $n-1, n+1$, and $n^2+1$ are even and one of the integers $n-1, n+1$ must even be divisible by 4. This means that $n^4$ is congruent to 0 modulo 16 for even $n$, and congruent to 1 modulo 16 for odd $n$. Therefore, if exactly $r$ of the numbers $x_1, x_2, \ldots, x_{14}$ are odd, then

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

Now $15999 = 16000 - 1 \equiv 15 \pmod{16}$, and since $0 \leq r \leq 14$, the congruence

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

cannot have a solution, and thus neither can the given equation be solvable.

**6.** *Find all pairs of integers $(x, y)$ such that*

$$x^3 - 4xy + y^3 = -1.$$

(G.M. Bucharest)

*First Solution.* Multiply both sides of the equation by 27 and then add 64 to each of them to obtain

$$27x^3 + 27y^3 + 4^3 - 4 \cdot 27xy = 37. \tag{1}$$

Using the algebraic identity

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca),$$

equation (1) is equivalent to

$$(3x + 3y + 4)(9x^2 + 9y^2 + 16 - 9xy - 12x - 12y) = 37. \qquad (2)$$

Since 37 is a prime and the second factor of the product in the left-hand side equals

$$\frac{1}{2}\Big[(3x - 3y)^2 + (3x - 4)^2 + (3y - 4)^2\Big] \geq 0,$$

it follows that $3x + 3y + 4 > 0$; hence from (2), $3x + 3y + 4 = 1$ or $3x + 3y + 4 = 37$. The latter is not possible since it would imply $x+y = 11$ and $(3x-3y)^2+(3x-4)^2+(3y-4)^2 = 2$, which cannot hold simultaneously ($x$ and $y$ have different parities; hence $|3x-3y| \geq 3$).

Thus $3x + 3y + 4 = 1$ and $9x^2 + 9y^2 + 16 - 9xy - 12x - 12y = 37$. We obtain the solutions $(-1, 0)$ and $(0, -1)$.

**Remark.** Compare this solution to that of Problem 4, Section 1.1.

*Second Solution.* Let $x + y = s$ and $xy = p$. The equation becomes $s^3 - 3sp - 4p + 1 = 0$, which is equivalent to

$$p = \frac{s^3 + 1}{3s + 4}.$$

Since $p \in \mathbb{Z}$, it follows that $27p \in \mathbb{Z}$, i.e.,

$$\frac{27s^3 + 27}{3s + 4} \in \mathbb{Z}.$$

This implies

$$9s^2 - 12s + 16 - \frac{37}{3s + 4} \in \mathbb{Z},$$

so $3s + 4 | 37$. Hence $3s + 4 \in \{-1, 1, 37, -37\}$, thus $s \in \{-1, 11\}$.

If $s = 11$, then $p = \frac{11^3+1}{37} \notin \mathbb{Z}$.

If $s = -1$, then $p = 0$ and we obtain the solutions $(-1, 0)$, $(0, -1)$.

**7.** *Find all triples $(x, y, z)$ of nonnegative integers such that*

$$5^x 7^y + 4 = 3^z.$$

(Bulgarian Mathematical Olympiad)

*Solution.* Either $x$ or $y$ is nonzero, and looking at the equality modulo 4 or modulo 7, we conclude that $z$ must be even (in the first case it must be of the form $4k+2$, in the second of the form $6k+4$). Set $z = 2z_1$ and rewrite the equation as $5^x 7^y = (3^{z_1} - 2)(3^{z_1} + 2)$. The two factors are divisible only by powers of 5 and 7, and since their difference is 4, they must be relatively prime. Hence either $3^{z_1} + 2 = 5^x$ and $3^{z_1} - 2 = 7^y$ or $3^{z_1} + 2 = 7^y$ and $3^{z_1} - 2 = 5^x$.

In the first case, assuming $y \geq 1$, by subtracting the two equalities we get $5^x - 7^y = 4$. Looking at residues mod 7, we conclude that $x$ is of the form $6k + 2$; hence even. But then, with $x = 2x_1$, we have $7^y = (5^{x_1} - 2)(5^{x_1} + 2)$. This is impossible, since the difference between the two factors is 4, and so they cannot both be powers of 7. It follows that $y = 0$, and consequently $x = 1$, $x = 2$.

In the second case, again by subtracting the equalities we find that $7^y - 5^x = 4$. Looking modulo 5, we conclude that $y$ must be even, and the same argument as above works mutatis mutandis to show that there are no solutions in this case.

**8.** *Prove that the equation*

$$4xy - x - y = z^2$$

*has no solution in positive integers.*

(Euler)

*Solution.* The equation is equivalent to

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

Let $p$ be a prime divisor of $4x-1$. Then $4z^2 \equiv -1 \pmod{p}$ i.e., $(2z)^2 \equiv -1 \pmod{p}$. From Fermat's little theorem, we obtain $(2z)^{p-1} \equiv 1 \pmod{p}$.

Hence

$$1 \equiv (2z)^{p-1} \equiv ((2z)^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

and therefore $p \equiv 1 \pmod{4}$.

Thus any prime divisors of $4x-1$ must be congruent to $1 \pmod{4}$; hence $4x - 1 \equiv 1 \pmod{4}$, a contradiction.

**9.** *Prove that the system of equations*

$$\begin{cases} x^2 + 6y^2 = z^2, \\ 6x^2 + y^2 = t^2, \end{cases}$$

*has no nontrivial integer solutions.*

*Solution.* Suppose that the system has a nontrivial solution. Then, dividing by the common divisor of $x, y, z, t$, we can assume that these four numbers have no common factor. We add the two equations to get $7(x^2 + y^2) = z^2 + t^2$. The quadratic residues modulo 7 are 0, 1, 2, 4. An easy check shows that the only way two residues can add up to 0 is if they are both equal to 0. Hence $z = 7z_0$ and $t = 7t_0$ for some integers $z_0$ and $t_0$. But then $x^2 + y^2 = 7(z_0^2 + t_0^2)$, which, by the same argument, implies that $x$ and $y$ are also divisible by 7. Thus each of $x, y, z$, and $t$ is divisible by 7, a contradiction. Hence the system has no nontrivial solutions.

**10.** *Find all pairs $(a, b)$ of positive integers that satisfy the equation*

$$a^{b^2} = b^a.$$

(37th IMO)

*First Solution.* We show that the only solutions are $(1, 1)$, $(16, 2)$, and $(27, 3)$.

Let $(a, b)$ be a solution to the equation, and let $d$ be the greatest common divisor of $a$ and $b$. We can then write $a = du$ and $b = dv$, where $u$ and $v$ are relatively prime positive integers. The given equation is then equivalent to

$$(du)^{dv^2} = (dv)^u. \tag{1}$$

We compare the exponents in (1) by examining three cases.

*Case 1.* If $dv^2 = u$, then (1) implies that $u = v$. Because $u$ and $v$ are relatively prime, we have $u = v = 1$. Since $dv^2 = u$, we find that $d = 1$. Hence $(a, b) = (1, 1)$, which is a solution.

*Case 2.* If $dv^2 > u$, rewrite (1) in the form

$$d^{dv^2-u}u^{dv^2} = v^u \tag{2}$$

to see that $u^{dv^2}$ divides $v^u$. Because $u$ and $v$ are relatively prime, we must have $u = 1$. Equation (2) then becomes

$$d^{dv^2-1} = v. \tag{3}$$

If $d = 1$, then from (3) we get $v = 1$, and the inequality $dv^2 > u$ fails to hold. If $d \geq 2$, then

$$d^{dv^2-1} \geq 2^{2v^2-1} \geq 2^{2v-1} > v \quad \text{for } v = 1, 2, 3, \ldots.$$

This contradicts (3), so there are no solutions in this case.

*Case 3.* If $dv^2 < u$, then $d < u$. Rewrite (1) as

$$u^{dv^2} = d^{u-dv^2}v^u \tag{4}$$

and note that $v^u$ divides $u^{dv^2}$. Because $u$ and $v$ are relatively prime, it follows that $v = 1$, so (4) becomes

$$u^d = d^{u-d}. \tag{5}$$

As noted earlier, $d < u$, so the exponents in (5) must satisfy $d < u - d$. Also, by (5), any prime divisor $p$ of $d$ is also a prime divisor of $u$. Let $\alpha$ and $\beta$ be the largest integers such that $p^\alpha \mid u$ and $p^\beta \mid d$. Then from (5), we have $\alpha d = \beta(u - d)$, and hence $\alpha > \beta$. It follows that $d \mid u$, so we have $u = kd$ for some positive integer $k$, and in addition, $k \geq 3$ because $u > 2d$. Substituting $u = kd$ into (5), we get

$$k = d^{k-2}. \tag{6}$$

If $k = 3$, then $d = 3$ and $u = kd = 9$. This yields the solution $a = 27$, $b = 3$.

If $k = 4$, then $d = 2$, $u = 8$, $a = 16$, and $b = 2$.

If $k \geq 5$, then $d^{k-2} \geq 2^{k-2} > k$, so (6) is impossible for such $k$.

*Second Solution.* First note that if $b = 1$, then $a = 1$ and vice versa. Hence we may suppose $a, b > 1$. Let $r = \frac{a}{b^2} \in \mathbb{Q}^+$. Then $a = b^r$ and $r = b^{r-2}$. Write $r = p/q$ for relatively prime positive integers $p$ and $q$. Then

$$\frac{p^q}{q^q} = r^q = b^{p-2q}.$$

If $p \geq 2q$, then the right-hand side is an integer and hence $q = 1$, i.e., $r \in \mathbb{Z}$. In this case we get $b = r^{1/(r-2)}$. If $r \geq 5$, then this gives

$1 < b < 2$, a contradiction. Hence $r = 3$ and $(a, b) = (27, 3)$ or $r = 4$ and $(a, b) = (16, 2)$.

If $p < 2q$, then the right-hand side is the reciprocal of an integer and $p = 1$. Hence $b = a^q$ and $a^{2q} = qa$ or $a = q^{1/(2q-1)}$. But this gives $1 < a < 2$ for all $q \geq 2$. Thus we get no solutions in this case.

**11.** *Find all primes $q_1, q_2, \ldots, q_6$ such that*

$$q_1^2 = q_2^2 + \cdots + q_6^2.$$

(Titu Andreescu)

*Solution.* Each square is congruent to 0 or 1 modulo 3 and clearly $q_1 \neq 3$. Suppose that among $q_2, \ldots, q_6$ there are $0 \leq a \leq 5$ primes not equal to 3. Then $a \equiv 1 \pmod 3$, so $a = 1$ or $a = 4$.

If $a = 1$, then $q_1^2 = q_2^2 + 4 \cdot 3^2$, so $(q_1 + q_2)(q_1 - q_2) = 36$. Because $q_1 + q_2 > q_1 - q_2$, $q_1 + q_2$ can be only $9, 12, 18$, or $36$, and we see that there are no solutions.

If $a = 4$, then $q_1^2 = q_2^2 + q_3^2 + q_4^2 + q_5^2 + 9$. Because $q_i$ are primes, their quadratic residues modulo 8 are either 1 (if $q_i$ is odd) or 4 (if $q_i = 2$). Clearly $q_1 \neq 2$, and suppose that among $q_2, \ldots, q_5$ there are $0 \leq b \leq 4$ primes not equal to 2. Then $b + 4(4 - b) + 9 \equiv 1 \pmod 8$, yielding $3b \equiv 0 \pmod 8$. Hence $b = 0$, and the solutions $(q_1, q_2, q_3, q_4, q_5, q_6)$ are $(5, 2, 2, 2, 2, 3)$ and its permutations with 5 fixed.

**12.** *Prove that there are unique positive integers $a$ and $n$ such that*

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

(Putnam Mathematical Competition)

*First Solution.* Suppose $a^{n+1}-(a+1)^n = 2001$. Notice that $a^{n+1}+[(a+1)^n-1]$ is a multiple of $a$. Thus $a$ divides $2002 = 2 \cdot 7 \cdot 11 \cdot 13$.

Since 2001 is divisible by 3, we must have $a \equiv 1 \pmod 3$; otherwise, one of $a^{n+1}$ and $(a+1)^n$ is a multiple of 3 and the other is not, so their difference cannot be divisible by 3. Now $a^{n+1} \equiv 1 \pmod 3$, so we must have $(a+1)^n \equiv 1 \pmod 3$, which forces $n$ to be even, and in particular at least 2.

If $a$ is even, then

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

Since $n$ is even,

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

Since $2001 \equiv 1 \pmod 4$, this is impossible. Thus $a$ is odd, and so must divide $1001 = 7 \cdot 11 \cdot 13$. Moreover,

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

Of the divisors of $7 \cdot 11 \cdot 13$, those congruent to 1 mod 3 are precisely those not divisible by 11 (since 7 and 13 are both congruent to 1 mod 3). Thus $a$ divides $7 \cdot 13$. Now $a \equiv 1 \pmod 4$ is possible only if $a$ divides 13.

We cannot have $a = 1$, since $1 - 2^n \neq 2001$ for any $n$. Thus the only possibility is $a = 13$. One easily checks that $a = 13$, $n = 2$ is a solution. All that remains is to check that no other $n$ works. In fact, if $n > 2$, then

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

But $13^{n+1} \equiv 13 \pmod 8$, since $n$ is even, contradiction. Thus $a = 13$, $n = 2$ is the unique solution.

*Second Solution.* We begin as in the previous solution and get that $a$ divides $2002 = 2 \cdot 7 \cdot 11 \cdot 13$. It follows $a \equiv 1 \pmod 3$. Now $a^{n+1} \equiv 1 \pmod 3$, so we must have $(a+1)^n \equiv 1 \pmod 3$, which forces $n$ to be even, and in particular at least 2.

Notice that $a^{n+1} + 1 - (a+1)^n$ is a multiple of $a+1$ (since $n+1$ is odd). Thus $a+1$ divides 2002. The only pairs of consecutive divisors of 2002 are $(1, 2)$ and $(13, 14)$. Hence $a = 1$ or $a = 13$.

We cannot have $a = 1$, since $a - 2^n \neq 2001$ for every $n$. Thus the only possibility is $a = 13$.

## 1.5 The Method of Mathematical Induction

**1.** *Prove that for all integers $n \geq 2$ there exist odd integers $x, y$ such that $|x^2 - 17y^2| = 4^n$.*

(Titu Andreescu)

*Solution.* For $n = 2$ we have $x_2 = y_2 = 1$. Suppose that for an integer $n \geq 2$, there exist odd integers $x_n, y_n$ such that $|x_n^2 - 17y_n^2| = 4^n$. We will construct a pair of odd integers $(x_{n+1}, y_{n+1})$ such that

$$|x_{n+1}^2 - 17y_{n+1}^2| = 4^{n+1}.$$

Actually,

$$\left(\frac{x_n \pm 17y_n}{2}\right)^2 - 17\left(\frac{x_n \pm y_n}{2}\right)^2 = 4(x_n^2 - 17y_n^2), \tag{1}$$

and precisely one of the numbers

$$\frac{x_n + y_n}{2} \quad \text{and} \quad \frac{x_n - y_n}{2}$$

is odd (since their sum is odd). If, for example, $\frac{x_n+y_n}{2}$ is odd, then

$$\frac{x_n + 17y_n}{2} = 8y_n + \frac{x_n + y_n}{2}$$

is also odd; hence in this case we can choose

$$x_{n+1} = \frac{x_n + 17y_n}{2}, \quad y_{n+1} = \frac{x_n + y_n}{2},$$

and from (1) we have

$$|x_{n+1}^2 - 17y_{n+1}^2| = 4|x_n^2 - 17y_n^2| = 4 \cdot 4^n = 4^{n+1}.$$

If $\frac{x_n - y_n}{2}$ is odd, we will choose

$$x_{n+1} = \frac{x_n - 17y_n}{2}, \quad y_{n+1} = \frac{x_n - y_n}{2}, \quad n \geq 1.$$

**2.** *Prove that for all positive integers $n$, the following equation is solvable in integers:*

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

(Dorin Andrica)

*Solution.* If $n = 1$, we have the solution $x_1 = 2$, $y_1 = 1$. Suppose that there exist positive integers $x_n, y_n$ satisfying

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

and define $x_{n+1} = 2x_n - y_n$, $y_{n+1} = x_n + 3y_n$. Hence

$$x_{n+1}^2 + x_{n+1}y_{n+1} + y_{n+1}^2 = 7(x_n^2 + x_n y_n + y_n^2) = 7 \cdot 7^n = 7^{n+1}.$$

**3.** *Prove that for each positive integer $n$, the equation*

$$(x^2 + y^2)(u^2 + v^2 + w^2) = 2009^n$$

*is solvable in integers.*

(Titu Andreescu)

*Solution.* Because $2009 = 41 \cdot 49$, we seek solutions to the equations

$$x^2 + y^2 = 41^n \quad \text{and} \quad u^2 + v^2 + w^2 = 49^n.$$

The first equation is a special case of Example 2 in Section 1.3 and so it is solvable in integers. For the second equation we find the solution $(2 \cdot 7^{n-1}, 3 \cdot 7^{n-1}, 6 \cdot 7^{n-1})$.

**4.** *The integer* $t_k = \frac{k(k+1)}{2}$ *is called the* $k$*th triangular number,* $k \geq 1$.

*Prove that for all positive integers* $n \geq 3$ *the equation*

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1$$

*is solvable in triangular numbers.*

*Solution.* We easily check that

$$\frac{1}{t_2} + \frac{1}{t_2} + \frac{1}{t_2} = 1, \quad \frac{1}{t_2} + \frac{1}{t_2} + \frac{1}{t_3} + \frac{1}{t_3} = 1.$$

Thus, it suffices to assume that $n \geq 5$. If $n$ is odd, that is, $n = 2k - 1$, where $k \geq 3$, then we have

$$\begin{aligned}\frac{1}{t_2} + \frac{1}{t_3} + \cdots + \frac{1}{t_{k-1}} + \frac{k+1}{t_k} &= \frac{2}{2 \cdot 3} + \frac{2}{3 \cdot 4} + \cdots + \frac{2}{(k-1)k} + \frac{2}{k} \\ &= 2\left[\left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{k-1} - \frac{1}{k}\right)\right] + \frac{2}{k} = 1,\end{aligned}$$

and the left-hand side is the sum of reciprocals of $(k-2)+(k+1) = 2k - 1 = n$ triangular numbers.

If $n$ is even, that is, $n = 2k$, where $k \geq 3$, then we have, in case $k = 3$, $\frac{6}{t_3} = 1$, while in case $k > 3$,

$$\begin{aligned}\frac{2}{t_3} + \frac{1}{t_3} + \frac{1}{t_4} + \cdots + \frac{1}{t_{k-1}} + \frac{k+1}{t_k} &= \frac{1}{3} + \frac{2}{3 \cdot 4} + \frac{2}{4 \cdot 5} + \cdots + \frac{2}{(k-1)k} + \frac{2}{k} \\ &= \frac{1}{3} + 2\left[\left(\frac{1}{3} - \frac{1}{4}\right) + \left(\frac{1}{4} - \frac{1}{5}\right) + \cdots + \left(\frac{1}{k-1} - \frac{1}{k}\right)\right] + \frac{2}{k} = 1,\end{aligned}$$

and the left-hand side is a sum of reciprocals of $(k-1)+(k+1) = 2k = n$ triangular numbers.

**Remark.** One can give an inductive solution with step 3 using the identity

$$\frac{1}{t_k} = \frac{2}{t_{2k}} + \frac{2}{t_{2k+1}}.$$

**5.** *Show that for all $n \geq 6$ the equation*

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = 1$$

*is solvable in integers.*

*Solution.* Note that

$$\frac{1}{a^2} = \frac{1}{(2a)^2} + \frac{1}{(2a)^2} + \frac{1}{(2a)^2} + \frac{1}{(2a)^2}$$

from which it follows that if $(x_1, x_2, \ldots, x_n) = (a_1, a_2, \ldots, a_n)$ is an integer solution to

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

then

$$\begin{aligned}(x_1,&x_2, \ldots, x_{n-1}, x_n, x_{n+1}, x_{n+2}, x_{n+3}) \\ &= (a_1, a_2, \ldots, a_{n-1}, 2a_n, 2a_n, 2a_n, 2a_n)\end{aligned}$$

is an integer solution to

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_{n+3}^2} = 1.$$

Therefore we can construct the solutions inductively if there are solutions for $n = 6, 7$, and 8.

If $n = 6$, we have the solution $(2, 2, 2, 3, 3, 6)$, if $n = 7$, a solution is $(2, 2, 2, 4, 4, 4, 4)$, and if $n = 8$, we have the solution $(2, 2, 2, 3, 4, 4, 12, 12)$.

**6.** *Prove that for all $s \geq 2$ there exist positive integers $x_0, x_1, \ldots, x_s$ such that*

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_s^2} = \frac{1}{x_0^2}$$

*and $x_0 < x_1 < \cdots < x_s$.*

*Solution.* If $s = 2$, then $x_0 = 12$, $x_1 = 15$, $x_2 = 20$ is a solution, since it is easy to verify that

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

We now assume that the assertion holds for some $s \geq 2$, i.e., there exist positive integers $x_0 < x_1 < \cdots < x_s$ such that

$$\frac{1}{x_0^2} = \frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_s^2}.$$

We set $y_0 = 12x_0$, $y_1 = 15x_0$, and $y_i = 20x_{i-1}$ for $i = 2, 3, \ldots, s+1$. It is easy to see that $y_0 < y_1 < \cdots < y_{s+1}$. Furthermore, we have

$$\begin{aligned}\frac{1}{y_0^2} &= \frac{1}{x_0^2} \cdot \frac{1}{12^2} = \frac{1}{x_0^2}\left(\frac{1}{15^2} + \frac{1}{20^2}\right) \\ &= \frac{1}{15^2} \cdot \frac{1}{x_0^2} + \frac{1}{20^2}\left(\frac{1}{x_1^2} + \cdots + \frac{1}{x_s^2}\right) \\ &= \frac{1}{y_1^2} + \frac{1}{y_2^2} + \cdots + \frac{1}{y_s^2} + \frac{1}{y_{s+1}^2}.\end{aligned}$$

This completes the proof by induction.

**7.** *Prove that for every positive integer $m$ and for all sufficiently large $s$, the equation*

$$\frac{1}{x_1^m} + \frac{1}{x_2^m} + \cdots + \frac{1}{x_s^m} = 1$$

*has at least one solution in positive integers* $x_1, x_2, \ldots, x_s$.

*Solution.* Let $m$ be a given positive integer. For $s = 2^m$, our equation has a solution in positive integers $x_1 = x_2 = \cdots = x_s = 2$.

Let now $a$ be a given positive integer, and suppose that our equation is solvable in positive integers for the positive integer $s$. Thus, there exist positive integers $t_1, t_2, \ldots, t_s$ such that

$$\frac{1}{t_1^m} + \frac{1}{t_2^m} + \cdots + \frac{1}{t_s^m} = 1,$$

and since $1/t_s^m = a^m/(at_s)^m$, for $x_1 = t_1$, $x_2 = t_2, \ldots, x_{s-1} = t_{s-1}$, $x_s = x_{s+1} = \cdots = x_{s+a^m-1} = at_s$, we have

$$\frac{1}{x_1^m} + \frac{1}{x_2^m} + \cdots + \frac{1}{x_{s+a^m-1}^m} = 1.$$

Thus, if our equation is solvable in positive integers for a positive integer $s$, then it is also solvable in positive integers for $s + a^m - 1$, and, more generally, for $s+(a^m-1)k$, where $k$ is an arbitrary positive integer. Taking $a = 2$ and $a = 2^m - 1$, we see that (for $s = 2^m$) our equation has a solution in positive integers for every integer of the form $2^m + (2^m - 1)k + [(2^m - 1)^m - 1]l$, where $k$ and $l$ are arbitrary positive integers.

In what follows we will prove and use the following result:

**Lemma.** *If* $a$ *and* $b$ *are two relatively prime positive integers, then all integers* $n \geq ab + 1$ *can be written in the form* $n = ax + by$, *for some positive integers* $x$ *and* $y$.

*Proof.* Applying the result of the lemma in the solution to Example 5 in Section 1.3, it follows that there exist positive integers $u, v$ such that $au - bv = 1$. For $n > ab$ we have $anu - bnv = n > ab$, and

consequently,

$$\frac{nu}{b} - \frac{nv}{a} > 1.$$

Therefore there exists an integer $t$ such that $\frac{nv}{a} < t < \frac{nu}{b}$. Let $x = nu - bt$, $y = at - nv$. We have $x > 0$ and $y > 0$ and also

$$ax + by = a(nu - bt) + b(at - nv) = n. \qquad \square$$

Clearly, the numbers $2^m - 1$ and $(2^m - 1)^m - 1$ are relatively prime. By the lemma above it follows that every integer $\geq (2^m - 1)[(2^m - 1)^m - 1] + 1$ can be written in the form $(2^m - 1)k + [(2^m - 1)^m - 1]l$, where $k$ and $l$ are positive integers. Thus the equation is solvable for all integers $s \geq 2^m + (2^m - 1)[(2^m - 1)^m - 1] + 1$.

**Remark.** The lower bound for $s$ we have found above is not the best possible. For example, if $m = 3$, this bound is

$$2^3 + (2^3 - 1) \cdot [(2^3 - 1)^3 - 1] + 1 = 2403,$$

far larger than 412 obtained in Example 4.

**8.** *Prove that for any nonnegative integer $k$ the equation*

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

*is solvable in positive integers $x, y, z$ with $x < y < z$.*

(Titu Andreescu)

*Solution.* If $k$ is even, say $k = 2n$, consider the identity

$$2n = (3n)^2 + (4n - 1)^2 - (5n - 1)^2.$$

Since $3n < 4n - 1 < 5n - 1$ for $n > 1$ and

$$0 = 3^2 + 4^2 - 5^2, \quad 2 = 5^2 + 11^2 - 12^2,$$

we are done with this case.

If $k$ is odd, say $k = 2n + 3$, we use the identity

$$2n + 3 = (3n + 2)^2 + (4n)^2 - (5n + 1)^2,$$

where for $n > 2$, we have $3n + 2 < 4n < 5n + 1$. Since

$$1 = 4^2 + 7^2 - 8^2, \quad 3 = 4^2 + 6^2 - 7^2,$$
$$5 = 4^2 + 5^2 - 6^2, \quad 7 = 6^2 + 14^2 - 15^2,$$

we have exhausted the case $k$ odd as well.

**9.** *Prove that the equation*

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

*has infinitely many solutions in positive integers* $x, y$.

*Solution.* Note that $x_1 = 3$, $y_1 = 5$ is a solution. Define the sequences $(x_n)_{n\geq 1}$, $(y_n)_{n\geq 1}$ by

$$\begin{cases} x_{n+1} = 3x_n + 2y_n + 1, \\ y_{n+1} = 4x_n + 3y_n + 2, \end{cases}$$

where $x_1 = 3$ and $y_1 = 5$.

Suppose that $(x_n, y_n)$ is a solution to the equation. Then

$$\begin{aligned} x_{n+1}^2 + (x_{n+1} + 1)^2 &= (3x_n + 2y_n + 1)^2 + (3x_n + 2y_n + 2)^2 \\ &= (4x_n + 3y_n + 2)^2, \end{aligned}$$

since $x_n^2 + (x_n + 1)^2 = y_n^2$. Therefore $x_{n+1}^2 + (x_{n+1} + 1)^2 = y_{n+1}^2$, i.e., $(x_{n+1}, y_{n+1})$ is also a solution.

**10.** *Solve in distinct positive integers the equation*

$$x_1^2 + x_2^2 + \cdots + x_{2002}^2 = 1335(x_1 + x_2 + \cdots + x_{2002}).$$

(Titu Andreescu)

*Solution.* We will prove that the only solution up to permutation to the equation in distinct positive integers

$$x_1^2 + \cdots + x_m^2 = \frac{2m+1}{3}(x_1 + \cdots + x_m)$$

is $x_1 = 1, \ldots, x_m = m$.

For this purpose we need the following result.

**Lemma.** *If $a_1, a_2, \ldots$ is a sequence of distinct positive integers, then for all $n \geq 1$ the following inequality holds:*

$$a_1^2 + \cdots + a_n^2 \geq \frac{2n+1}{3}(a_1 + \cdots + a_n).$$

(Romanian Mathematical Olympiad)

*Proof.* Without loss of generality, we may assume that $0 < a_1 < a_2 < \cdots$.

Let us proceed by induction. For $n = 1$, $a_1 \geq 1$ implies

$$a_1^2 \geq \frac{2 \cdot 1 + 1}{3} a_1.$$

It suffices to prove that

$$a_{n+1}^2 \geq \frac{2}{3}(a_1 + \cdots + a_n) + \frac{2n+3}{3} a_{n+1},$$

or

$$3a_{n+1}^2 - (2n+3)a_{n+1} \geq 2(a_1 + \cdots + a_n).$$

Since

$$2(a_1+\cdots+a_n) \le 2(1+2+\cdots+a_n) = a_n(a_n+1) \le (a_{n+1}-1)a_{n+1},$$

it is enough to show that

$$3a_{n+1}^2 - (2n+3)a_{n+1} \ge (a_{n+1}-1)a_{n+1}.$$

The last inequality is equivalent to $a_{n+1} \ge n+1$, which is evident. □

Without loss of generality, suppose that $0 < x_1 < x_2 < \cdots < x_m$. Then

$$x_1 \ge 1,\ \ldots,\ x_m \ge m.$$

We have

$$x_1^2 + \cdots + x_m^2 = \frac{2m+1}{3}(x_1 + \cdots + x_m),$$

and by the lemma,

$$x_1^2 + \cdots + x_{m-1}^2 \ge \frac{2m-1}{3}(x_1 + \cdots + x_{m-1}).$$

It follows that

$$x_m^2 \le \frac{2}{3}(x_1 + \cdots + x_{m-1}) + \frac{2m+1}{3}x_m.$$

Since $x_{m-1} \le x_m - 1$, $x_{m-2} \le x_m - 2, \ldots, x_1 \le x_m - (m-1)$, we also have

$$x_1 + \cdots + x_{m-1} \le (m-1)x_m - \frac{(m-1)m}{2}.$$

Then

$$x_m^2 \le \frac{2(m-1)}{3}x_m - \frac{(m-1)m}{3} + \frac{2m+1}{3}x_m,$$

or

$$x_m^2 - \frac{4m-1}{3}x_m + \frac{(m-1)m}{3} \le 0.$$

That is, $(x_m - m)\left(x_m - \frac{m-1}{3}\right) \le 0$, and since $x_m > \frac{m-1}{3}$, it follows that $x_m \le m$, i.e., $x_m = m$ and $x_1 = 1$, $x_2 = 2, \ldots, x_{m-1} = m-1$.

## 1.6 Fermat's Method of Infinite Descent (FMID)

**1.** *Find all triples $(x, y, z)$ of positive integer solutions to the equation*

$$x^3 + 3y^3 + 9z^3 - 3xyz = 0.$$

(Kürschák Mathematical Competition)

*Solution.* Note that $(0, 0, 0)$ is a solution. Suppose that $(x_1, y_1, z_1)$ is another solution. If one of the components $x_1, y_1, z_1$ equals zero, then from the irrationality of $\sqrt[3]{3}$ or $\sqrt[3]{9}$ it follows that the other two equal zero as well. Hence we may assume that $x_1, y_1, z_1 > 0$.

A similar argument to that in Example 1 shows that $x_1 = 3x_2$, $y_1 = 3y_2$, $z_1 = 3z_2$, where $(x_2, y_2, z_2)$ is also a solution. We obtain in this way a sequence of positive integral solutions $(x_n, y_n, z_n)_{n\geq 1}$ with $x_1 > x_2 > x_3 > \cdots$, in contradiction to FMID Variant 1. Thus the only solution is $(0, 0, 0)$.

**2.** *Find all integers $x, y, z$ satisfying*

$$x^2 + y^2 + z^2 - 2xyz = 0.$$

(Korean Mathematical Olympiad)

*Solution.* The only solution to this equation is $x = y = z = 0$. First, note that $x, y$, and $z$ cannot all be odd, since then $x^2 + y^2 + z^2 - 2xyz$ would be odd and therefore nonzero. Therefore 2 divides $xyz$. But then $x^2 + y^2 + z^2 = 2xyz$ is divisible by 4; since all squares are congruent to 0 or 1 (mod 4), $x, y$, and $z$ must all be even. Write $x = 2x_1$, $y = 2y_1$, $z = 2z_1$; then we have $4x_1^2 + 4y_1^2 + 4z_1^2 = 16x_1y_1z_1$, or $x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1$. Since the

right-hand side is divisible by 4, $x_1, y_1, z_1$ must again be even, so we can write $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$; plugging this in and manipulating, we obtain $x_2^2 + y_2^2 + z_2^2 = 8x_2y_2z_2$. In general, if $n \geq 1$, $x_n^2 + y_n^2 + z_n^2 = 2^{n+1}x_ny_nz_n$ implies that $x_n, y_n, z_n$ are all even, so we can write $x_n = 2x_{n+1}$, $y_n = 2y_{n+1}$, $z_n = 2z_{n+1}$, which satisfy $x_{n+1}^2 + y_{n+1}^2 + z_{n+1}^2 = 2^{n+2}x_{n+1}y_{n+1}z_{n+1}$; repeating this argument gives us an infinite sequence of integers $x_1, x_2, x_3, \ldots$ in which $x_i = 2x_{i+1}$, $i \geq 1$. Therefore $|x_1| > |x_2| > |x_3| > \cdots$, which contradicts FMID Variant 1.

**3.** *Solve the following equation in integers* $x, y, z, u$ :

$$x^4 + y^4 + z^4 = 9u^4.$$

*Solution.* If $u = 0$, then necessarily $x = y = z = 0$, which is a solution of the given equation. We will show that there are no other solutions. Let us assume that the integers $x, y, z, u$ satisfy the given equation and that $u \neq 0$; we set $d = u^4$. If the number $u$ were not divisible by 5, then Fermat's little theorem would give $u^4 \equiv 1 \pmod 5$, and we would have

$$x^4 + y^4 + z^4 \equiv 4 \pmod 5.$$

This, however, is impossible, since by Fermat's little theorem the numbers $x^4, y^4, z^4$ are congruent to 0 or 1 modulo 5. Thus, $u$ is divisible by 5, i.e., $u = 5u_1$ for an appropriate $u_1 \in \mathbb{Z}$, and we get

$$x^4 + y^4 + z^4 \equiv 0 \pmod 5,$$

which implies that $x, y, z$ are divisible by 5, i.e., $x = 5x_1$, $y = 5y_1$, $z = 5z_1$ for appropriate $x_1, y_1, z_1 \in \mathbb{Z}$. Substituting this into the

original equation and dividing by $5^4$, we obtain

$$x_1^4 + y_1^4 + z_1^4 = 9u_1^4,$$

and thus $x_1, y_1, z_1, u_1$ satisfy the given equation, and

$$u_1^4 = \frac{u^4}{5^4} < u^4 = d.$$

Continuing this procedure, we obtain the sequence $u_1^4 > u_2^4 > u_3^4 > \cdots$, in contradiction to FMID Variant 1.

**4.** *Solve the following equation in positive integers:*

$$x^2 - y^2 = 2xyz.$$

*Solution.* We assume that some positive integers $x, y, z$ satisfy the given equation, and set $d = xy$. If we let $d = 1$, then $x = y = 1$ and the equation would give $z = 0$, which is impossible. Hence $d > 1$. Let $p$ be some prime dividing $d$. Since

$$(x + y)(x - y) = x^2 - y^2 = 2xyz \equiv 0 \pmod{p},$$

we have $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. In view of the fact that the prime $p$ divides the product $xy$, either $x$ or $y$ is congruent to 0 modulo $p$, and together $x \equiv y \equiv 0 \pmod{p}$. Hence $x_1 = x/p$ and $y_1 = y/p$ are positive integers, and

$$(px_1)^2 - (py_1)^2 = 2(px_1)(py_1)z,$$

from which, upon dividing by $p^2$, we see that $x_1, y_1, z$ satisfy the given equation, and that

$$x_1 y_1 = \frac{x}{p} \cdot \frac{y}{p} = \frac{d}{p^2} < d.$$

In this way we obtain a decreasing sequence of positive integers $x_1 > x_2 > x_3 > \cdots$, which is not possible.

**5.** *Determine all integral solutions to*

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

(5th USA Mathematical Olympiad)

*Solution.* We show, by considering the equation modulo 4 for all possibilities of $a, b, c$ being even or odd, that it is necessary that they all be even. We can also take them to be all nonnegative. First, note that for even and odd numbers, we have

$$(2n)^2 \equiv 0 \pmod 4 \text{ and } (2n+1)^2 \equiv 1 \pmod 4.$$

*Case 1.* $a, b, c$ all odd. Then

$$a^2 + b^2 + c^2 \equiv 3 \pmod 4, \text{ while } a^2b^2 \equiv 1 \pmod 4.$$

*Case 2.* Two odd and one even. Then

$$a^2 + b^2 + c^2 \equiv 2 \pmod 4, \text{ while } a^2b^2 \equiv 0 \text{ or } 1 \pmod 4.$$

*Case 3.* Two even and one odd. Then

$$a^2 + b^2 + c^2 \equiv 1 \pmod 4, \text{ while } a^2b^2 \equiv 0 \pmod 4.$$

Since the only possible solution is for $a, b, c$ even, let $a = 2a_1$, $b = 2b_1$, and $c = 2c_1$. This leads to the equation

$$a_1^2 + b_1^2 + c_1^2 = 4a_1^2b_1^2, \text{ where } a_1 \le a,\ b_1 \le b,\ c_1 \le c.$$

Now $4a_1^2b_1^2 \equiv 0 \pmod 4$, and each of $a_1^2, b_1^2, c_1^2$ is congruent to 0 or 1 (mod 4). Hence $a_1^2 \equiv b_1^2 \equiv c_1^2 \equiv 0 \pmod 4$ and $a_1, b_1, c_1$ are even,

say $a_1 = 2a_2$, $b_1 = 2b_2$, $c_1 = 2c_2$. This leads to the equation

$$16a_2^2b_2^2 = a_2^2 + b_2^2 + c_2^2.$$

Again, we can conclude that $a_2, b_2, c_2$ are all even, and the process leads to

$$64a_3^2b_3^2 = a_3^2 + b_3^2 + c_3^2,$$

where $a = 8a_3$, $b = 8b_3$, $c = 8c_3$. If we continue the process, we conclude that $a, b$, and $c$ are divisible by as high a power of 2 as we want to specify, and hence the only solution of the equation is $a = b = c = 0$.

**6.** *(a) Prove that if there exists a triple of positive integers* $(x, y, z)$ *such that*

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

*then* $z = 3$.

*(b) Find all such triples.*

*Solution.* (a) Let $(x, y, z)$ be a solution with $z \neq 3$. Then $x \neq y$, for otherwise $x^2(z-2) = 1$, which is impossible, since $z - 2 \neq 1$. We have

$$\begin{aligned} 0 &= x^2 + y^2 + 1 - xyz = (x - yz)^2 + y^2 + 1 + xyz - y^2z^2 \\ &= (yz - x)^2 + y^2 + 1 - (yz - x)yz; \end{aligned}$$

hence $(yz - x, y, z)$ is also a solution, since $x(yz - x) = xyz - x^2 = y^2 + 1 > 0$ implies $yz - x > 0$. Note that if $x > y$, then $x^2 > y^2 + 1 = x(yz - x)$. Hence $x > yz - x$, which shows that the newly obtained solution is smaller than the initial solution in the sense that $x + y > (yz - x) + y$. However, under the assumption that $x \neq y$, this

procedure can be continued indefinitely, which is impossible, since in the process we construct an infinite decreasing sequence of positive integers, violating FMID Variant 1. This contradiction shows that there are no solutions if $z \neq 3$.

(b) Clearly, $(1, 1)$ is a solution to the equation

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

Let $(a, b)$, $a > b$, be another solution. Then $b^2 + (3b - a)^2 + 1 = 3b(3b - a)$, so $(b, 3b - a)$ is also a solution. From

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

it follows that $a > 2b$; hence $3b - a < b$. So the new solution has a smaller $b$. Descending, we reach a solution with $b = 1$, hence with $a^2 + 2 = 3a$, in which case $a = 1$ or $a = 2$. It follows that all solutions are obtained from $(a_1, b_1) = (1, 1)$ by the recurrence

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

Sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ satisfy the same recursion: $x_{n+1} = 3x_n - x_{n-1}$, $x_1 = 1$, $x_2 = 2$, which characterizes the Fibonacci numbers of odd index. Therefore, $(a_n, b_n) = (F_{2n+1}, F_{2n-1})$, $n \geq 1$.

The solutions are $(1, 1)$, $(F_{2n+1}, F_{2n-1})$, $(F_{2n-1}, F_{2n+1})$, $n \geq 1$.

**Remarks.** (1) Some variants of this problem have appeared in various mathematical competitions and training exercises. We will mention here the following:

*Find all pairs $(m, n)$ of positive integers having the property that $mn \mid (m - n)^2 + 1$.*

(USA Mathematical Olympiad Summer Program)

(2) The Diophantine equation

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

is known as *Markov's equation.* The structure of its solutions is quite complicated. Using the result in the problem, it follows that $(F_{2n-1}, F_{2n+1}, 1)$, $n \geq 1$, and its permutations are solutions to this equation, as well as the obvious solution $(1, 1, 1)$.

**7.** *Solve in positive integers $x, y, u, v$ the system*

$$\begin{cases} x^2 + 1 = uy, \\ y^2 + 1 = vx. \end{cases}$$

*Solution.* Clearly $x$ and $y$ are relatively prime. We have

$$x^2 + y^2 + 1 = x(x + v) = y(y + u). \tag{1}$$

It follows that $x \mid x^2 + y^2 + 1$ and $y \mid x^2 + y^2 + 1$; hence there is a positive integer $z$ such that

$$x^2 + y^2 + 1 = xyz. \tag{2}$$

From Problem 6, it follows that $z = 3$ and that $x = F_{2n-1}$ and $y = F_{2n+1}$ in some order. On the other hand, from (1) and from $x^2 + y^2 + 1 = 3xy$ we obtain

$$x + v = 3y, \quad y + u = 3x,$$

hence $u = 3x - y = 3F_{2n-1} - F_{2n+1} = F_{2n-3}$ and $v = 3y - x = 3F_{2n+1} - F_{2n-1} = F_{2n+3}$.

The solutions are

$$(x, y, u, v) = (F_{2n-1}, F_{2n+1}, F_{2n-3}, F_{2n+3}),$$
$$(x, y, u, v) = (F_{2n+1}, F_{2n-1}, F_{2n+3}, F_{2n-3}),$$

where $n \geq 1$ and $F_{-1} = 1$.

**Remark.** Other variants of this problem have appeared in various mathematical competitions and training exercises. We will mention here the following:

*Prove that there are infinitely many pairs $(a, b)$ of positive integers such that $a \mid b^2 + 1$ and $b \mid a^2 + 1$.*

(Tournament of Towns)

**8.** *Find all triples $(x, y, z)$ of positive integers that are solutions to the system of equations*

$$\begin{cases} 2x - 2y + z = 0, \\ 2x^3 - 2y^3 + z^3 + 3z = 0. \end{cases}$$

(Titu Andreescu)

*Solution.* Substituting $z$ from the first equation into the second yields

$$2(x^3 - y^3) - 8(x - y)^3 - 6(x - y) = 0.$$

Because $x \neq y$, this reduces to

$$-(x^2 + xy + y^2) + 4(x - y)^2 + 3 = 0,$$

which is equivalent to $x^2 + y^2 + 1 = 3xy$.

Taking into account that $x < y$, from Problem 6 it follows that all pairs $(x, y) = (x_n, y_n)$ are $(F_{2n-1}, F_{2n+1})$, $n \geq 1$, and

$$z_n = 2(y_n - x_n) = 2F_{2n}.$$

Hence all desired triples are $(F_{2n-1}, F_{2n+1}, 2F_{2n})_{n \geq 1}$.

**9.** *Prove that there are infinitely many triples $(x, y, z)$ of positive integers such that*

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

(College Mathematics Journal)

*Solution.* It suffices to consider $z = 3$. We obtain the equation $x^2 + y^2 + 9 = 3xy$. Taking $x = 3u$ and $y = 3v$, the equation becomes $u^2 + v^2 + 1 = 3uv$. We have seen in Problem 6 that this equation has solutions $(u, v) = (1, 1)$, $(F_{2n-1}, F_{2n+1})$, and $(F_{2n+1}, F_{2n-1})$, $n \geq 1$.

Hence an infinite family of solutions to our equation is given by

$$(x, y, z) = (3F_{2n+1}, 3F_{2n-1}, 3), \quad n \geq 1.$$

**10.** *Find all pairs of positive integers $(a, b)$ such that $ab + a + b$ divides $a^2 + b^2 + 1$.*

(Mathematics Magazine)

*Solution.* Either $a = b = 1$ or $a$ and $b$ are consecutive squares.

The divisibility condition can be written as

$$k(ab + a + b) = a^2 + b^2 + 1, \tag{1}$$

for some positive integer $k$. If $k = 1$, then (1) is equivalent to

$$(a - b)^2 + (a - 1)^2 + (b - 1)^2 = 0,$$

from which $a = b = 1$. If $k = 2$, then (1) can be written as

$$4a = (b - a - 1)^2,$$

forcing $a$ to be a square, say $a = d^2$. Then $b - d^2 - 1 = \pm 2d$, so $b = (d \pm 1)^2$, and $a$ and $b$ are consecutive squares.

Now assume that there is a solution with $k \geq 3$, and let $(a, b)$ be the solution with $a$ minimal and $a \leq b$. Write (1) as a quadratic in $b$:

$$b^2 - k(a+1)b + (a^2 - ka + 1) = 0.$$

Because one root, $b$, is an integer, the other root, call it $r$, is also an integer. Since (1) must be true with $r$ in place of $b$, we conclude that $r > 0$. Because $a \leq b$ and the product of the roots, $a^2 - ka + 1$, is less than $a^2$, we must have $r < a$. But then $(r, a)$ is also a solution to (1), contradicting the minimality of $a$.

**11.** *Let $a$ be a positive integer. The sequence $(x_n)_{n\geq 1}$ is defined by $x_1 = 1$, $x_2 = a$, and $x_{n+2} = ax_{n+1} + x_n$ for all $n \geq 1$. Prove that $(x, y)$ is a solution to the equation*

$$|x^2 + axy - y^2| = 1$$

*if and only if there exists an index $k$ such that $(x, y) = (x_k, x_{k+1})$.*

(Romanian Mathematical Olympiad)

*Solution.* Let $f(x, y) = x^2 + axy - y^2$. We have $f(x_1, x_2) = f(1, a) = 1$. Using mathematical induction, it follows that for any $n \geq 1$, $(x_n, x_{n+1})$ is a solution to the equation.

Consider $(x, y) \in \mathbb{Z}_+^* \times \mathbb{Z}_+^*$ a solution to the equation. From $x^2 + axy - y^2 = \pm 1$ it follows that $y(y - ax) = x^2 \pm 1 \geq 0$, with equality if and only if $x = 1$ and $y = a$. In this case, $(x, y) = (x_1, x_2)$ and we are done. Now assume $y > ax$. The pair $(x^{(1)}, y^{(1)}) = (y - ax, x)$ is also a solution, since $f(x, y) = \pm 1$ implies $f(y - ax, x) = \mp 1$. Moreover, $x + y \geq x^{(1)} + y^{(1)}$ and $y^{(1)} \geq ax^{(1)}$. In this way we obtain a sequence

of solutions $(x^{(n)}, y^{(n)})_{n\geq 1}$ such that $y^{(n)} - ax^{(n)} \geq 0$ and

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

Applying FMID Variant 2, it follows that there exists a positive integer $k$ such that $x^{(n)} + y^{(n)} = x^{(k)} + y^{(k)}$ for all $n \geq k$. In this case, for the solution $(x^{(k)}, y^{(k)})$ we have $y^{(k)} = ax^{(k)}$ and $(x, y) = (x_k, x_{k+1})$.

**12.** *Find all pairs of nonnegative integers $(m, n)$ such that*

$$(m + n - 5)^2 = 9mn.$$

(42nd IMO USA Team Selection Test)

*Solution.* Note that the equation is symmetric in $m$ and $n$. The solutions are the unordered pairs

$$(5F_{2k}^2, 5F_{2k+2}^2), \quad (L_{2k-1}^2, L_{2k+1}^2),$$

where $k$ is a nonnegative integer and $\{F_j\}$, $\{L_j\}$ are the Fibonacci and Lucas sequences, respectively, that is, the sequences defined by $F_1 = F_2 = 1$, $L_1 = 1$, $L_2 = 3$ and the recurrence relations $F_{j+2} = F_{j+1} + F_j$ and $L_{j+2} = L_{j+1} + L_j$ for $j \geq 1$. Note that we amended the Lucas sequence by considering $L_{-1} = -1$ and $L_0 = 2$. Let $g = \gcd(m, n)$ and write $m = gm_1$ and $n = gn_1$. Because $9mn$ is a perfect square, $m_1$ and $n_1$ are perfect squares. Let $m_1 = x^2$ and $n_1 = y^2$. The given condition becomes

$$(gx^2 + gy^2 - 5)^2 = 9g^2x^2y^2.$$

Taking the square root on both sides yields

$$g(x^2 + y^2) - 5 = \pm 3gxy,$$

or

$$g(x^2 + y^2 \pm 3xy) = 5.$$

If $g(x^2 + y^2 + 3xy) = 5$, then $x^2 + y^2 + 3xy \leq 5$, implying that $x = y = g = 1$ and $(m, n) = (1, 1)$. Otherwise, $g(x^2 + y^2 - 3xy) = 5$ and $g = 1$ or 5. Fix $g$ equal to one of these values, so that

$$x^2 - 3xy + y^2 = \frac{5}{g}. \tag{1}$$

We call an unordered pair $(a, b)$ a *g-pair* if $(x, y) = (a, b)$ (or equivalently, $(x, y) = (b, a)$) satisfies (1) and $a$ and $b$ are positive integers. Also, we call an unordered pair $(p, q)$ *smaller* (respectively, *larger*) than another unordered pair $(r, s)$ if $p + q$ is smaller (respectively larger) than $r + s$.

Suppose that $(a, b)$ is a $g$-pair. View (1) as a monic quadratic in $x$ with $y = b$ constant. The coefficient of $x$ in a monic quadratic equation $(x - r_1)(x - r_2)$ equals $-(r_1 + r_2)$, implying that $(3b - a, b)$ should also satisfy (1). Indeed,

$$b^2 - 3b(3b - a) + (3b - a)^2 = a^2 - 3ab + b^2 = \frac{5}{g}.$$

Also, if $b > 2$, note that

$$a^2 - 3ab + b^2 = \frac{5}{g} < b^2.$$

It follows that $a^2 - 3ab < 0$, and so $3b - a > 0$. Thus if $(a, b)$ is a $g$-pair with $b > 2$, then, $(b, 3b - a)$ is a $g$-pair as well. Furthermore, if $a \geq b$, note that $a \neq b$, because otherwise $-a^2 = g > 0$, which is impossible. Thus, $a > b$ and

$$a^2 - 3ab + b^2 = \frac{5}{g} > b^2 - a^2,$$

which implies that $a(2a-3b)>0$ and hence $a+b>b+(3b-a)$ and also $3b-a>b$. Thus, $(b,3b-a)$ is a smaller $g$-pair than $(a,b)$ with $b\geq 3b-a$.

Given any $g$-pair $(a,b)$ with $b\leq a$, if $b\leq 2$, then $a$ must equal $r(g)$, where $r(5)=3$ and $r(1)=4$. Otherwise, according to the above observation, we can repeatedly reduce it to a smaller $g$-pair until $\min(a,b)\leq 2$, that is, to the $g$-pair $(r(g),1)$. Beginning with $(r(g),1)$, we reverse the reducing process so that $(x,y)$ is replaced by the larger $g$-pair $(3x-y,x)$. Moreover, this must generate all $g$-pairs, since all $g$-pairs, can be reduced to $(r(g),1)$. We may express these possible pairs in terms of the Fibonacci and Lucas numbers; for $g=1$, observe that $L_2=1$, $L_4=4=r(1)$, and that

$$\begin{aligned} L_{2k+4} &= L_{2k+3}+L_{2k+2}=(L_{2k+2}+L_{2k+1})+L_{2k+2} \\ &= (L_{2k+2}+(L_{2k+2}-L_{2k}))+L_{2k+2}=3L_{2k+2}-L_{2k} \end{aligned}$$

for $k\geq 0$. For $g=5$, the Fibonacci numbers satisfy an analogous recurrence relation, and $F_2=1$, $F_4=3=r(5)$. Therefore, $(m,n)=(L_{2k}^2,L_{2k+2}^2)$ and $(m,n)=(5F_{2k}^2,5F_{2k+2}^2)$ for $k\geq 0$.

**13.** *Let $x,y,z$ be positive integers such that $xy-z^2=1$. Prove that there exist nonnegative integers $a,b,c,d$ for which*

$$x=a^2+b^2,\quad y=c^2+d^2,\ \textit{and}\ z=ac+bd.$$

(20th IMO Shortlist)

*Solution.* Assume, by way of contradiction, that we have a triple of positive integers $(x_0,y_0,z_0)$ with $x_0y_0-z_0^2=1$ such that there are no integers $a,b,c,d$ satisfying $x_0=a^2+b^2$, $y_0=c^2+d^2$, and

$z_0 = ac + bd$. We may further assume that $2 \le x_0 \le y_0$ and that $z_0$ is minimal (if we had $x_0 = 1$, then $x_0 = 0^2 + 1^2$, $y_0 = 1^2 + k^2$, and $z_0 = 0 \cdot 1 + 1 \cdot k$).

Starting with $(x_0, y_0, z_0)$ we construct another triple satisfying $xy - z^2 = 1$ in the following way: taking $z = x + u$, we obtain $xy - (x^2 + 2xu + u^2) = 1$, or $x(y - x - 2u) - u^2 = 1$. Since $u = z - x$, we have $y - x - 2u = x + y - 2z$; hence $(x_1, y_1, z_1) = (x_0, x_0 + y_0 - 2z_0, z_0 - x_0)$ is that triple. We check now that $x_1, y_1, z_1 \ge 1$. Indeed, the inequalities

$$z_0^2 = x_0 y_0 - 1 < x_0 y_0 \le \left(\frac{x_0 + y_0}{2}\right)^2$$

imply that $z_0 < \frac{x_0+y_0}{2}$, i.e., $y_1 \ge 1$. Also, the inequality $z_0^2 = x_0 y_0 - 1 \ge x_0^2 - 1$ implies $z_0 \ge x_0 - 1$.

If $z_0 = x_0 - 1$, then $x_0(y_0 - x_0 + 2) = 2$, which is impossible, since $x_0 \ge 2$ and $y_0 - x_0 + 2 \ge 2$.

If $z_0 = x_0$, then $x_0(y_0 - x_0) = 1$, which is impossible, since $x_0 \ge 2$. Therefore $z_1 = z_0 - x_0 \ge 1$.

Moreover, if we had $x_1 = m^2 + n^2$, $y_1 = p^2 + q^2$, and $z_1 = mp + nq$, then we would obtain

$$x_0 = m^2 + n^2, \quad x_0 + y_0 - 2z_0 = p^2 + q^2, \text{ and } z_0 - x_0 = mp + nq,$$

and hence

$$y_0 = p^2 + q^2 + 2z_0 - x_0 = p^2 + q^2 + 2mp + 2nq + x_0 = (p+m)^2 + (q+n)^2$$

and $z_0 = m(p+m) + n(q+n)$, which contradicts our initial assumption concerning the triple $(x_0, y_0, z_0)$.

We obtained the positive integers triple $(x_1, y_1, z_1)$ satisfying all properties at the beginning of the proof, with $z_1 < z_0$. This contradicts the minimality of $z_0$.

**Remark.** Choosing $z = (2s)!$, we will prove that each prime $p$ of the form $4s + 1$ is representable as a sum of two perfect squares.

Indeed, from Wilson's theorem it follows that $(p-1)! + 1 \equiv 0 \pmod{p}$, i.e., $(4s)! + 1 = pr$, for some positive integer $r$. But

$$\begin{aligned}(4s)! &= (2s)!(4s+1-1)(4s+1-2)\cdots(4s+1-2s)\\ &\equiv (2s)!(-1)^{2s}(2s)! \equiv ((2s)!)^2 \pmod{p}.\end{aligned}$$

It follows that $((2s)!)^2 = py - 1$. Applying the result in the problem for $p = x$ and $z = (2s)!$, the property follows.

## 1.7 Miscellaneous Diophantine Equations

**1.** *Prove that the equation* $6(6a^2 + 3b^2 + c^2) = 5n^2$ *has no solution in integers except* $a = b = c = n = 0$.

(Asian Pacific Mathematical Olympiad)

*Solution.* Assume that a nontrivial integer solution $(a, b, c, n)$ exists. We may assume that $\gcd(a, b, c, n) = 1$, since any common divisor can be divided out. We have

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

Clearly $6 \mid n$. If $n = 6m$, then

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

and therefore $3 \mid c$. If $c = 3d$, then

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

For any integer $x$, we have $x^2 \equiv 0, 1, 4 \pmod 8$. Therefore

$$\begin{aligned} 2a^2 &\equiv 0, 2 \pmod 8, \\ b^2 &\equiv 0, 1, 4 \pmod 8, \\ 3d^2 &\equiv 0, 3, 4 \pmod 8, \end{aligned}$$

but

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

Hence $b^2$ and $3d^2$, and therefore $b$ and $d$, are even. It follows that $c$ is even. Let $b = 2r$, $c = 2s$. Then from the original equation,

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

and $36a^2$ is therefore divisible by 8. Therefore $a$ is even, along with $b, c$, and $n$, contradicting the coprimality assumption.

**2.** *Determine a positive constant $c$ such that the equation*

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

*has exactly three solutions $(x, y)$ in positive integers.*

(United Kingdom Mathematical Olympiad)

*Solution.* When $y = 1$ the left-hand side is 0; hence we cannot have three solutions. Thus we can rewrite our equation as

$$x = \frac{y(y-1) + c}{(y+1)(y-1)}.$$

The numerator is congruent to $-1(-2)+c$ modulo $(y+1)$, and it is also congruent to $c$ modulo $(y-1)$. Hence we must have $c \equiv -2 \pmod{(y+1)}$ and $c \equiv 0 \pmod{(y-1)}$. Because $c = y-1$ satisfies these congruences, we must have $c \equiv y-1 \pmod{\operatorname{lcm}(y-1, y+1)}$. When $y$ is even, $\operatorname{lcm}(y-1, y+1) = y^2-1$; when $y$ is odd, $\operatorname{lcm}(y-1, y+1) = \frac{1}{2}(y^2-1)$.

Then, for $y = 2, 3, 11$, we have $c \equiv 1 \pmod 3$, $c \equiv 2 \pmod 4$, $c \equiv 10 \pmod{60}$. Hence, we try setting $c = 10$. For $x$ to be an integer, we must have $(y-1) \mid 10 \Rightarrow y = 2, 3, 6$, or 11. These values give $x = 4, 2, \frac{2}{7}$, and 1, respectively. Thus there are exactly three solutions in positive integers, namely $(x, y) = (4, 2), (2, 3)$, and $(1, 11)$.

**3.** *Find all triples $(x, y, z)$ of positive integers such that $y$ is a prime number, $y$ and 3 do not divide $z$, and $x^3 - y^3 = z^2$.*

(Bulgarian Mathematical Olympiad)

*Solution.* Rewrite the equation in the form

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

Any common divisor of $x-y$ and $x^2+xy+y^2$ also divides both $z^2$ and $(x^2+xy+y^2) - (x+2y)(x-y) = 3y^2$. Because $z^2$ and $3y^2$ are relatively prime by assumption, $x-y$ and $x^2+xy+y^2$ must be relatively prime as well. Therefore, both $x-y$ and $x^2+xy+y^2$ are perfect squares.

Now writing $a = \sqrt{x-y}$, we have

$$x^2+xy+y^2 = (a^2+y)^2 + (a^2+y)y + y^2 = a^4 + 3a^2y + 3y^2$$

and $4(x^2+xy+y^2) = (2a^2+3y)^2 + 3y^2$.

Writing $m = 2\sqrt{x^2+xy+y^2}$ and $n = 2a^2+3y$, we have

$$m^2 = n^2 + 3y^2,$$

or $(m-n)(m+n) = 3y^2$, so $(m-n, m+n) = (1, 3y^2), (3, y^2)$, or $(y, 3y)$.

In the first case, $2n = 3y^2 - 1$ and $4a^2 = 2n - 6y = 3y^2 - 6y - 1$ is a square, which is impossible modulo 3.

In the third case, $n = y < 2a^2 + 3y = n$, a contradiction.

In the second case, we have $4a^2 = 2n - 6y = y^2 - 6y - 3 < (y-3)^2$. When $y \geq 10$ we have $y^2 - 6y - 3 > (y-4)^2$; hence we must actually have $y = 2, 3, 5$, or 7. In this case we have $a = \frac{\sqrt{y^2-6y-3}}{2}$, which is real only when $y = 7$, $a = 1$, $x = y + a^2 = 8$, and $z = 13$. This yields the unique solution $(x, y, z) = (8, 7, 13)$.

**4.** *Determine all triples $(x, k, n)$ of positive integers such that*

$$3^k - 1 = x^n.$$

(Italian Mathematical Olympiad)

*Solution.* The solutions are all triples of the form $(3^k - 1, k, 1)$ for positive integers $k$, and $(2, 2, 3)$.

The case of $n = 1$ is obvious. Now, $n$ cannot be even, because then 3 could not divide $3^k = (x^{\frac{n}{2}})^2 + 1$ (because no square is congruent to 2 modulo 3). Also, we must have $x \neq 1$.

Assume that $n > 1$ is odd and $x \geq 2$. Then $3^k = (x+1)\sum_{i=0}^{n-1}(-x)^i$, implying that both $x+1$ and $\sum_{i=0}^{n-1}(-x)^i$ are powers of 3. Because

$$x + 1 \leq x^2 - x + 1 \leq \sum_{i=0}^{n-1}(-x)^i,$$

we must have

$$0 \equiv \sum_{i=0}^{n-1} (-x)^i \equiv n \pmod{(x+1)},$$

so that $(x+1) \mid n$. Specifically, this means that $3 \mid n$.

Writing $x' = x^{\frac{n}{3}}$, we have $3^k = x'^3 + 1 = (x'+1)(x'^2 - x' + 1)$. As before, $x'+1$ must equal some power of 3, say $3^t$. Then $3^k = (3^t - 1)^3 + 1 = 3^{3t} - 3^{2t+1} + 3^{t+1}$, which is strictly between $3^{3t-1}$ and $3^{3t}$ for $t > 1$. Therefore we must have $t = 1$, $x' = 2$, and $k = 2$, giving the solution $(x, k, n) = (2, 2, 3)$.

**5.** *For a positive integer $n$, show that the number of integral solutions $(x, y)$ to the equation $x^2 + xy + y^2 = n$ is finite and a multiple of* 6.

*Solution.* If $(x, y)$ is an integral solution of $x^2 + xy + y^2 = n$, then $(-x, -y)$ is a different solution, so solutions come in pairs. If we can show instead that solutions come in sixes (and that there are only finitely many), we will be done. To see why solutions come in sixes, we can use algebraic manipulation to rewrite $x^2 + xy + y^2$ as $a^2 + ab + b^2$ for suitable $(a, b) \neq (x, y)$.

First note that for any solution $(x, y)$, we have

$$2n = 2x^2 + 2xy + 2y^2 = x^2 + y^2 + (x+y)^2 \geq x^2 + y^2.$$

Therefore, any integral solution is one of the lattice points (points whose coordinates are integers) on or inside a circle of radius $\sqrt{2n}$, and so the number of integral solutions is finite.

Now observe that

$$\begin{aligned} x^2 + xy + y^2 &= (x+y)^2 - xy \\ &= (x+y)^2 - x(x+y) + x^2 \\ &= (x+y)^2 + (x+y)(-x) + (-x)^2. \end{aligned}$$

Thus, if $(x, y)$ is an integral solution of $x^2 + xy + y^2 = n$, then so is $(x+y, -x)$. If we repeat this process with the new solution, we go through a cycle of solutions,

$$(x,y), (x+y,-x), (y,-x-y), (-x,-y), (-x-y,x), (-y,x+y), \quad (1)$$

after which we get back to $(x, y)$. It can be checked directly that since $x$ and $y$ cannot both be zero, all six solution in the cycle (1) are different.

**6.** *Find all positive integers $n$ such that there exist relatively prime positive integers $x$ and $y$ and an integer $k > 1$ satisfying the equation*

$$x^k + y^k = 3^n.$$

(Russian Mathematical Olympiad)

*Solution.* The only solution is $n = 2$. Let $3^n = x^k + y^k$, where $x, y$ are relatively prime integers with $x > y$, $k > 1$, and $n$ a positive integer. Clearly, neither $x$ nor $y$ is a multiple of 3. Therefore, if $k$ is even, $x^k$ and $y^k$ are congruent to 1 mod 3, so their sum is congruent to 2 mod 3, and so is not a power of 3. If $k$ is odd and $k > 1$, then $3^n = (x+y)(x^{k-1} - \cdots + y^{k-1})$. Thus $x + y = 3^m$ for some $m \geq 1$. We will show that $n \geq 2m$. Since $3 \mid k$, by putting $x_1 = x^{k/3}$ and $y_1 = y^{k/3}$, we may assume that $k = 3$. Then $x^3 + y^3 = 3^n$ and

$x + y = 3^m$. To prove the inequality $n \geq 2m$, it suffices to show that $x^3 + y^3 \geq (x + y)^2$, or $x^2 - xy + y^2 \geq x + y$. Since $x \geq y + 1$, $x^2 - x = x(x - 1) \geq xy$, and $(x^2 - x + xy) + (y^2 - y) \geq y(y - 1) \geq 0$, and the inequality $n \geq 2m$ follows.

From the identity $(x+y)^3 - (x^3 + y^3) = 3xy(x+y)$ it follows that

$$3^{2m-1} - 3^{n-m-1} = xy.$$

But $2m - 1 \geq 1$, and $n - m - 1 \geq n - 2m \geq 0$. If strict inequality occurs in either place in the last inequality, then $3^{2m-1} - 3^{n-m-1}$ is divisible by 3, while $xy$ is not. Hence $n - m - 1 = n - 2m = 0$, and so $m = 1$, $n = 2$, and $3^2 = 2^3 + 1^3$.

**Remark.** The inequality $x^2 - xy + y^2 \geq x + y$ can alternatively be shown by noting that

$$x^2 - xy + y^2 - x - y = (x - y)^2 + (x - 1)(y - 1) - 1 \geq 0,$$

since $(x - y)^2 \geq 1$.

**7.** *Prove that for each prime $p$ the equation*

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

*has no integer solutions $(q, n)$ with $q, n > 1$.*

(Italian Mathematical Olympiad)

*Solution.* When $p = 2$, we have $q^n = 13$, which is impossible. Otherwise, $p$ is odd and $5 \mid 2^p + 3^p$. Because $n > 1$, we must have $25 \mid 2^p + 3^p$. Hence

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

so $5 \mid p$. Thus $p = 5$, but the equation $q^n = 2^5 + 3^5 = 5^2 \cdot 11$ has no solutions.

**8.** *Determine all pairs $(a, b)$ of integers for which the numbers $a^2 + 4b$ and $b^2 + 4a$ are both perfect squares.*

(Asian Pacific Mathematical Olympiad)

*Solution.* If $a = 0$, then $b$ must be a perfect square, and vice versa. Now assume that both $a$ and $b$ are nonzero. Also observe that $a^2+4b$ and $a^2$ have the same parity, and similarly $b^2 + 4a$ and $b^2$ have the same parity.

If $b$ is positive, then $a^2+4b \geq (|a|+2)^2 = a^2+4|a|+4$ so $|b| \geq |a|+1$. If $b$ is negative, then $a^2+4b \leq (|a|-2)^2 = a^2-4|a|+4$ so $|b| \geq |a|-1$. Similarly, $a > 0 \;\Rightarrow\; |a| \geq |b| + 1$ and $a < 0 \;\Rightarrow\; |a| \geq |b| - 1$.

Assume without loss of generality that $b > a$. If $a$ and $b$ are positive, then from the inequalities above we have $b \geq a+1$ and $a \geq b+1$, a contradiction.

If $a$ and $b$ are negative, then we have either $a = b$ or $a = b - 1$. For $b \geq -5$, only $(a, b) = (-4, -4)$ and $(-6, -5)$ work. Otherwise, we have $(b + 4)^2 < b^2 + 4a < (b + 2)^2$, a contradiction.

Finally, if $a$ is negative and $b$ is positive, then we have both $|b| \geq |a| + 1$ and $|a| \geq |b| - 1$. Then we must have $|b| = |a| + 1$, and hence $a + b = 1$. Any such pair works, because then $a^2 + 4b = (a - 2)^2$ and $b^2 + 4a = (b - 2)^2$ are both perfect squares.

Therefore the possible pairs $(a, b)$ are

$$(-4, -4), \quad (-6, -5), \quad (-5, -6),$$

and

$$(0, n^2), \quad (n^2, 0), \quad (n, 1-n),$$

where $n$ is any integer.

**9.** *A rectangular parallelepiped has integer dimensions. All of its faces are painted green. The parallelepiped is partitioned into unit cubes by planes parallel to its faces. Find all possible dimensions of the parallelepiped if the number of cubes without a green face is one-third of the total number of cubes.*

(Bulgarian Mathematical Olympiad)

*Solution.* Let the parallelepiped's dimensions be $a, b, c$. These lengths must all be at least 3, or else every cube has a green face. The given condition is equivalent to

$$3(a-2)(b-2)(c-2) = abc,$$

or

$$3 = \frac{a}{a-2} \cdot \frac{b}{b-2} \cdot \frac{c}{c-2}.$$

If all the dimensions are at least 7, then $\frac{a}{a-2} \cdot \frac{b}{b-2} \cdot \frac{c}{c-2} \leq \left(\frac{7}{5}\right)^3 = \frac{343}{125} < 3$, a contradiction. Thus one of the dimensions, say $a$, equals $3, 4, 5$, or 6. Assume without loss of generality that $b \leq c$.

When $a = 3$, we have $bc = (b-2)(c-2)$, which is impossible.

When $a = 4$, rearranging the equation yields $(b-6)(c-6) = 24$. Thus $(b, c) = (7, 30), (8, 18), (9, 14)$, or $(10, 12)$.

When $a = 5$, rearranging the equation yields $(2b-9)(2c-9) = 45$. Thus $(b, c) = (5, 27), (6, 12)$, or $(7, 9)$.

Finally, when $a = 6$, rearranging the equation yields $(b-4)(c-4) = 8$. Thus $(b, c) = (5, 12)$ or $(6, 8)$.

Therefore the parallelepiped may measure $4 \times 7 \times 30$, $4 \times 8 \times 18$, $4 \times 9 \times 14$, $4 \times 10 \times 12$, $5 \times 5 \times 27$, $5 \times 6 \times 12$, $5 \times 7 \times 9$, or $6 \times 6 \times 8$.

**10.** *Find all positive integer solutions* $(x, y, z, t)$ *of the equation*

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

*such that* $\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$.

(Romanian Mathematical Olympiad)

*First Solution.* It is clear that $\gcd(x, x + y) = \gcd(x, x + z) = 1$, so $x$ divides $y + z$, $y$ divides $z + x$, and $z$ divides $x + y$. Let $a, b$, and $c$ be integers such that

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

If we consider a system of linear equations having a nonzero solution, we get $\Delta = abc - 2 - a - b = 0$, which is the determinant of

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

The Diophantine equation $abc - 2 = a + b + c$ can be solved by consider the following cases:

(1) $a = b = c$. Then $a = 2$ and it follows that $x = y = z$. Because $\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$, we get $x = y = z = 1$ and $t = 8$, hence the solution $(1, 1, 1, 8)$.

(2) $a = b,\ a \neq c$. The equation becomes

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

If $c = 2$, it follows that $x = y = z$ (which is case (1)). So $c = 1$ and, immediately, $x = y = 1$ and $z = 2$. So the solution is $(1, 1, 2, 9)$.

(3) $a > b > c$. In this case, $abc - 2 = a + b + c < 3a$. Therefore $a(bc - 3) < 2$. It follows that $bc - 3 < 2 \Rightarrow bc < 5$. We have the following cases:

(i) $b = 2,\ c = 1 \Rightarrow a = 3$ and we return to case (2).

(ii) $b = 3,\ c = 1 \Rightarrow a = 5$. We obtain the solution $(1, 2, 3, 10)$.

(iii) $b = 4,\ c = 1 \Rightarrow 3a = 7$, impossible.

Finally, the solutions are $(1, 1, 1, 8)$, $(1, 1, 2, 9)$, $(1, 2, 3, 10)$ and those obtained by permutations of $x, y, z$.

*Second Solution.* Without loss of generality we may assume $x \leq y \leq z$. If $x = y$, then since $\gcd(x, y) = 1$, we must have $x = y = 1$. Hence $z \mid 2$ and we get solutions $(1, 1, 1, 8)$ and $(1, 1, 2, 4)$. If $x < y$, then $y \geq 2$, and since $\gcd(y, z) = 1$, we must have $x < y < z$. In this case $\gcd(z, y + z) = \gcd(z, x + z) = 1$, so $z \mid x + y$ and $x + y < 2z$. Thus $x + y = z$. Since similarly $y \mid x + z$, this gives $y \mid 2x + y$ and $y \mid 2x$. Since $\gcd(x, y) = 1$, we must have $y \mid 2$. Since $x < y$ this forces $x = 1$ and $y = 2$ and hence $z \mid 3$. Since this gives $z = 3$, we have the solution $(1, 2, 3, 10)$.

# II.2

# Solutions to Some Classical Diophantine Equations

## 2.1 Linear Diophantine Equations

**1.** *Solve the equation*

$$6x + 10y - 15z = 1.$$

*Solution.* Working modulo 3, we have $y \equiv 1 \pmod 3$; hence $y = 1 + 3s$, $s \in \mathbb{Z}$. The equation becomes

$$6x - 15z = -9 - 30s,$$

or equivalently, $2x - 5z = -3 - 10s$. Passing to modulo 2 yields $z \equiv 1 \pmod 2$, i.e., $z = 1 + 2t$, $t \in \mathbb{Z}$ and $x = 1 - 5s + 5t$. Hence the solutions are

$$(x, y, z) = (1 - 5s + 5t, 1 + 3s, 1 + 2t), \quad s, t \in \mathbb{Z}.$$

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, 265
DOI 10.1007/978-0-8176-4549-6_6, © Springer Science+Business Media, LLC 2010

**2.** *Let $a, b, c$ be pairwise relatively prime positive integers. Show that $2abc - ab - bc - ca$ is the largest integer that cannot be expressed in the form $xbc + yca + zab$, where $x, y, z$ are nonnegative integers.*

(24th IMO)

*Solution. Step 1.* The number $2abc-ab-bc-ca$ cannot be expressed in the required form. Assume, for the sake of contradiction, that

$$2abc - ab - bc - ca = xbc + ycz + zab,$$

where $x, y, z \geq 0$. Then

$$2abc = bc(x + 1) + ca(y + 1) + ab(z + 1),$$

where $x + 1 > 0$, $y + 1 > 0$, $z + 1 > 0$. It follows that $a \mid bc(x + 1)$.

Since $a$ is relatively prime to $b$ and $c$, $a$ divides $x + 1$; hence $a \leq x + 1$. Using similar arguments, we obtain $b \leq y + 1$ and $c \leq z + 1$. Thus $2abc = bc(x + 1) + ca(y + 1) + ab(z + 1) \geq 3abc$. This is a contradiction.

*Step 2.* Every number $N$, $N > 2abc-ab-bc-ca$, can be expressed in the form $N = xbc + yca + zab$.

First, observe that $2abc - ab - bc - ca + 1 > 0$. Indeed,

$$\begin{aligned}\frac{1}{abc}(2abc - ab - bc - ca + 1) &= 2 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c} + \frac{1}{abc} \\ &> 2 - \frac{1}{1} - \frac{1}{2} - \frac{1}{3} + \frac{1}{abc} > 0.\end{aligned}$$

Going further, we have two situations. When $N \equiv 0 \pmod{abc}$, $N = abcq$, we may consider the combination $N = (ab)cq+bc\cdot 0+ca\cdot 0$, which is of the required form.

Suppose now that $N \not\equiv 0 \pmod{abc}$. Since $\gcd(bc, a) = 1$, the congruence

$$xbc \equiv N \pmod{a}$$

has a solution $x_0,\ 0 < x_0 < a$. Similarly, the congruences

$$ycz \equiv N \pmod{b},$$
$$zab \equiv N \pmod{c},$$

have solutions $y_0, z_0$, respectively, $0 < y_0 < b,\ 0 < z_0 < c$.

Let $A = x_0bc + y_0ca + z_0ab$. Then

$$A \equiv x_0bc \equiv N \pmod{a}, \quad A \equiv N \pmod{b}, \quad A \equiv N \pmod{c}.$$

Since $a, b, c$ are pairwise relatively prime, we obtain $A \equiv N \pmod{abc}$.

The number $A$ is a combination of the required form. Since $x_0 \leq a-1$, $y_0 \leq b-1$, and $z_0 \leq c-1$, it follows that $A \leq 3abc-bc-ca-ab$. Also, since $A \equiv N \pmod{abc}$, we may write $N = A+kabc$. We have $k \geq 0$, because $N > 2abc - bc - ca - ab$. Therefore

$$N = (x_0 + ka)bc + y_0ca + z_0ab,$$

where $x_0 + ka \geq 0,\ y_0 \geq 0,\ z_0 \geq 0$.

**Remark.** This is in fact the Frobenius coin problem with $n = 3$ and coefficients $bc, ca, ab$.

**3.** *Find the number of triples $(x, y, z)$ of nonnegative integers such that*

$$x + y + 2z = n.$$

*Solution.* From Theorem 2.1.3 we obtain that the desired number is

$$A_n = \frac{1}{n!} f^{(n)}(0),$$

where the generating function $f$ is given by

$$f(t) = \frac{1}{(1-t)(1-t)(1-t^2)}.$$

We have

$$f(t) = -\frac{1}{2} \cdot \frac{1}{(t-1)^3} + \frac{1}{4} \cdot \frac{1}{(t-1)^2} - \frac{1}{8} \cdot \frac{1}{t-1} + \frac{1}{8} \cdot \frac{1}{t+1}$$

hence

$$f^{(n)}(t) = -\frac{1}{4} \cdot \frac{(-1)^n (n+2)!}{(t-1)^{n+3}} + \frac{1}{4} \cdot \frac{(-1)^n (n+1)!}{(t-1)^{n+2}} - \frac{1}{8} \cdot \frac{(-1)^n n!}{(t-1)^{n+1}} + \frac{1}{8} \cdot \frac{(-1)^n n!}{(t+1)^{n+1}}.$$

Thus

$$f^{(n)}(0) = \frac{(n+2)!}{4} + \frac{(n+1)!}{4} + \frac{n!}{8} + \frac{(-1)^n n!}{8}$$

and

$$A_n = \frac{1}{n!} f^{(n)}(0) = \frac{2(n+1)(n+3) + 1 + (-1)^n}{8}.$$

**4.** *Determine the positive integer $n$ such that the equation*

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

*has exactly* 100 *solutions* $(x, y, z)$ *in nonnegative integers.*

*Solution.* Using the result in Problem 3, we obtain that the number of triples $(x, y, z)$ of nonnegative integers satisfying the equation $x + 2y + z = n$ is

$$A_n = \frac{2(n+1)(n+3) + 1 + (-1)^n}{8}.$$

If $n = 2k$, then $A_n = (k+1)^2$. It follows that $k = 9$ and that $n = 18$.

If $n = 2k+1$, then $A_n = (k+1)(k+2)$ and note that the equation $(k+1)(k+2) = 100$ has no integral solutions.

**5.** *Let $a, b, c, d$ be integers such that for all integers $m$ and $n$ there exist integers $x$ and $y$ for which $ax+by = m$ and $cx+dy = n$. Prove that $ad - bc = \pm 1$.*

(Eötvös Mathematics Competition)

*First Solution.* First, suppose that $a = 0$. Then we can express any integer $m$ in the form $by$, so that $b = \pm 1$, $cx = n - dy$, and $c$ divides $n \mp dm$ for all $m$ and $n$, and so $c = \pm 1$ and $ad - bc = \pm 1$. The argument is similar if any of $b, c$, and $d$ are 0.

If $abcd \neq 0$, let $\Delta = ad - bc$. Suppose that $\Delta = 0$. Then $\frac{c}{a} = \frac{d}{b}$. Let their common value be $\lambda$. Then $n = cx+dy = \lambda(ax+by) = \lambda m$. This means that $\frac{n}{m} = \lambda$ for any integers $m$ and $n$. This is of course absurd. Hence $\Delta \neq 0$. We now solve $ax + by = m$ and $cx + dy = n$ for $x$ and $y$. We have $x = \frac{dm-bn}{\Delta}$ and $y = \frac{an-cm}{\Delta}$. We are given that for any integers $m$ and $n$, $x$ and $y$ are also integers. In particular, for $(m, n) = (1, 0)$, $x_1 = \frac{d}{\Delta}$ and $y_1 = -\frac{c}{\Delta}$ are integers, and for $(m, n) = (0, 1)$, $x_2 = -\frac{b}{\Delta}$ and $y_2 = \frac{a}{\Delta}$ are integers. It follows that $x_1y_2 - x_2y_1 = \frac{ad-bc}{\Delta^2} = \frac{1}{\Delta}$ is also an integer. The only integers whose reciprocals are also integers are $\pm 1$. Since $\Delta$ is clearly an integer, we must have $\Delta = \pm 1$.

*Second Solution.* Taking $m = 1$ and $n = 0$ gives integers $x_1$ and $y_1$ with $ax_1 + by_1 = 1$ and $cx_1 + dy_1 = 0$. Similarly, taking $m = 0$ and $n = 1$ gives $x_2$ and $y_2$ with $ax_2 + by_2 = 0$ and $cx_2 + dy_2 = 1$. Then

we compute

$$\begin{aligned}(ad-bc)&(x_1y_2-x_2y_1)\\&=(ax_1+by_1)(cx_2+dy_2)-(cx_1+dy_1)(ax_2+by_2)\\&=1\cdot 1-0\cdot 0=1.\end{aligned}$$

Since these are integers, we must have $ad-bc=\pm 1$.

**6.** *Let $n$ be an integer greater than 3 and let $X$ be a $3n^2$-element subset of $\{1,2,\ldots,n^3\}$. Prove that there exist nine distinct numbers $a_1,a_2,\ldots,a_9$ in $X$ such that the system*

$$\begin{cases} a_1x+a_2y+a_3z=0,\\ a_4x+a_5y+a_6z=0,\\ a_7x+a_8y+a_9z=0,\end{cases}$$

*is solvable in nonzero integers.*

(Romanian Mathematical Olympiad)

*Solution.* Label the elements of $X$ in increasing order $x_1<\cdots<x_{3n^2}$, and put

$$X_1=\{x_1,\ldots,x_{n^2}\},\ X_2=\{x_{n^2+1},\ldots,x_{2n^2}\},$$
$$X_3=\{x_{2n^2+1},\ldots,x_{3n^2}\}.$$

Define the function $f:X_1\times X_2\times X_3\to X\times X$ as follows:

$$f(a,b,c)=(b-a,c-b).$$

The domain of $f$ contains $n^6$ elements. The range of $f$, on the other hand, is contained in the subset of $X\times X$ of pairs whose sum is at most $n^3$, a set of cardinality

$$\sum_{k=1}^{n^3-1}k=\frac{n^3(n^3-1)}{2}<\frac{n^6}{2}.$$

By the pigeonhole principle, some three triples $(a_i, b_i, c_i)$ $(i = 1, 2, 3)$ map to the same pair, in which case $x = b_1 - c_1$, $y = c_1 - a_1$, $z = a_1 - b_1$ is a solution in nonzero integers. Note that $a_i$ cannot equal $b_j$, since $X_1$ and $X_2$ are disjoint and so on, and that $a_1 = a_2$ implies that the triples $(a_1, b_1, c_1)$ and $(a_2, b_2, c_2)$ are identical, a contradiction. Hence the nine numbers chosen are indeed distinct.

**7.** *Let*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1q}x_q = 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2q}x_q = 0, \\ \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pq}x_q =, 0 \end{cases}$$

*be a system of linear equations, where* $q = 2p$ *and* $a_{ij} \in \{-1, 0, 1\}$. *Prove that there exists a solution* $(x_1, x_2, \ldots, x_q)$ *of the system with the following properties:*

*(a)* $x_j$ *is an integer, for any* $j = 1, 2, \ldots, q$*;*

*(b) there exists* $j$ *such that* $x_j \neq 0$*;*

*(c)* $|x_j| \leq q$ *for any* $j = 1, 2, \ldots, q$.

(18th IMO)

*Solution.* Let $(y_1, y_2, \ldots, y_q)$ be a $q$-tuple of integers such that $|y_j| \leq p$, $j = 1, 2, \ldots, q$. Then the value of the left-hand side of the $r$th equation is some integer between $-pq$ and $pq$, since the coefficients are $-1$, 0, or 1. Thus

$$\sum_{i=1}^{q} a_{ri}y_i$$

can have at most $2pq+1$ values, $pq$ positive integer values, $pq$ negative integer values and the value 0. Now consider the $p$-tuple of all $p$ left

sides in our system. Since each can take at most $2pq + 1$ values, at most $(2pq + 1)^p$ distinct $p$-tuples can result. Each $y_j$ is an integer between $-p$ and $p$, so there are $2p + 1$ choices for each $y_j$, and since there are $q$ $y$'s in a $q$-tuple, we can make up a total $(2p+1)^q$ different ordered $q$-tuples.

Now $q = 2p$, so the number of $q$-tuples $(y_1, \ldots, y_q)$ with $|y_j| \leq p$ is

$$(2p + 1)^q = (2p + 1)^{2p} = [(2p + 1)^2]^p = [4p^2 + 4p + 1]^p,$$

while the number of $p$-tuples

$$\left( \sum_{j=1}^{q} a_{1j} y_j, \sum_{j=1}^{q} a_{2j} y_j, \ldots, \sum_{j=1}^{q} a_{pj} y_j \right)$$

they can generate is at most

$$(2pq + 1)^p = (4p^2 + 1)^p.$$

Therefore there are more $q$-tuples $(y_1, \ldots, y_q)$ than there are value sets, and by the pigeonhole principle, there are at least two distinct $q$-tuples producing the same values of the left sides. Denote these $q$-tuples by

$$(y_1, y_2, \ldots, y_q) \text{ and } (z_1, z_2, \ldots, z_q). \tag{1}$$

We claim that the $q$-tuple $(x_1, x_2, \ldots, x_q)$ of differences $y_j - z_j = x_j$, $j = 1, 2, \ldots, q$, is a solution of the problem satisfying properties (a), (b), (c). To verify this claim, we first observe that

$$\sum_{j=1}^{q} a_{rj} y_j = \sum_{j=1}^{q} a_{rj} z_j, \quad r = 1, 2, \ldots, p,$$

implies

$$\sum_{j=1}^{q} a_{rj} x_j = \sum_{j=1}^{q} a_{rj} (y_j - z_j) = \sum_{j=1}^{q} a_{rj} y_j - \sum_{j=1}^{q} a_{rj} z_j = 0.$$

So the $x_i$ satisfy all $p$ equations. Moreover, since $y_i$ and $z_i$ are integers, so are their differences, and (a) is satisfied. The $q$-tuples (1) are distinct, so not all $x_j$ are zero; thus (b) is satisfied. Finally, since $|y_j| \le p$ and $|z_j| \le p$, we see by the triangle inequality that $|x_j| = |y_j - z_j| \le |y_j| + |z_j| \le 2p$, so $|x_j| \le q$; (c) also is satisfied.

## 2.2 Pythagorean Triples and Related Problems

**1.** *Prove that the system of equations*

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

*is not solvable in positive integers.*

*Solution.* Assume, for the sake of contradiction, that the system is solvable and let $(x, y, u, v)$ be a solution. Then

$$u^2 - y^2 = x^2 \text{ and } u^2 + y^2 = v^2.$$

But this contradicts the result in Example 2.

**2.** *Let $m$ and $n$ be distinct positive integers. Show that none of the numbers*

$$2(m^4 + n^4), \quad m^4 + 6m^2n^2 + n^4$$

*is a perfect square.*

*Solution.* Suppose that $2(m^4 + n^4) = v^2$, for some $v \in \mathbb{Z}_+$. Then

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

and

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

in contradiction to the result in Problem 1.

Similarly, assuming that $m^4 + 6m^2n^2 + n^4 = v^2$, for some $v \in \mathbb{Z}_+$, we obtain

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

and

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

which also contradicts the result in Problem 1.

**3.** *Prove that the equation*

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

*has no solution in positive integers.*

(Bulgarian Mathematical Olympiad)

*Solution.* Solving the given equation for $z^2$, we find that the discriminant of the resulting equation is $x^4 + 6x^2y^2 + y^4$. By the second result in Problem 2, this cannot be a perfect square, and we are done.

**4.** *Prove that the equation*

$$x^2 + y^2 = (a^2 + b^2)z^2,$$

*where $a$ and $b$ are nonzero given integers, has infinitely many solutions.*

*Solution.* Let $x = au + bv$ and $y = bu - av$. Then

$$x^2 + y^2 = (a^2 + b^2)(u^2 + v^2)$$

and the equation becomes $u^2 + v^2 = z^2$. We obtain

$$u = k(m^2 - n^2), \quad v = 2kmn, \quad z = k(m^2 + n^2),$$

for some integers $m$ and $n$, hence the solution

$$x = k(am^2 + 2bmn - an^2), \quad y = k(bm^2 - 2amn - bn^2),$$
$$z = k(m^2 + n^2).$$

**5.** *Find all quadruples $(x, y, z, w)$ of positive integers such that*

$$xy + yz + zx = w^2.$$

*Solution.* The equation is equivalent to

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

From Theorem 2.2.3 it follows that

$$y - z = \frac{l^2 + m^2 - n^2}{n}, \quad 2x = 2l, \quad 2w = 2m,$$
$$2x + y + z = \frac{l^2 + m^2 + n^2}{n},$$

for some positive integers $l, m, n$, with $n$ a divisor of $l^2 + m^2$.

Hence all solutions to the given equation are

$$x = l, \quad y = \frac{l^2 - ln + m^2}{n}, \quad z = n - l, \quad w = m,$$

where $l, m, n$ are positive integers such that $n$ is a divisor of $l^2 + m^2$ with $l < n < l + \frac{m^2}{2}$.

**6.** *Prove that there is no Pythagorean triangle whose area is a perfect square.*

*Solution.* Suppose, to the contrary, that such a triangle $(a, b, c)$ exists. Then

$$a^2 + b^2 = c^2 \text{ and } ab = 2d^2,$$

for some positive integer $d$. Without loss of generality we may assume that $a > b$, since the case $a = b$ cannot possibly occur because $2a^2 = c^2$ is impossible. Hence

$$c^2 + (2d)^2 = (a+b)^2 \text{ and } c^2 - (2d)^2 = (a-b)^2,$$

contrary to Example 2.

**7.** *Prove that the number of primitive Pythagorean triangles with a given inradius $r$ is a power of 2, if $r$ is integer.*

*Solution.* Let $a, b, c$ be the side lengths of a Pythagorean triangle with inradius $r$, $r \in \mathbb{Z}_+$. Simple geometric considerations lead to the relation

$$\frac{a+b-c}{2} = r.$$

On the other hand, there exist positive integers $m, n$ such that $m > n$, $\gcd(m,n) = 1$, $m+n$ is odd, and

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

We obtain $n(m-n) = r$. Then the formula $n(m-n) = r$ says that $m-n$ is an odd factor of $r$ relatively prime to $r/(m-n)$. Thus $m-n$ is determined by the set of odd prime divisors of $r$ that divide $m-n$. Any such set determines $m-n$ and $n$, hence the primitive Pythagorean triple. Thus the number of solutions is $2^t$, where $t$ is the number of odd primes dividing $r$, as claimed.

**8.** *(a) Solve the equation*

$$x^2 + y^2 + z^2 - xy - yz - zx = t^2.$$

*(b) Prove that the equation*

$$u^2 + v^2 + w^2 = 2t^2$$

*has infinitely many solutions in positive integers.*

(Titu Andreescu and Dorin Andrica)

*Solution.* (a) The equation is equivalent to

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

Let $x-z=u$ and $y-z=v$. Then

$$(u-v)^2+uv=t^2,$$

that is,

$$(t+u-v)(t-u+v)=uv.$$

Set

$$\frac{t+u-v}{u}=\frac{v}{t-u+v}=\frac{m}{n},$$

with $\gcd(m,n)=1$ and get the system of equations

$$\begin{cases}(m-n)u+nv=nt,\\ mu-(m-n)v=mt.\end{cases}$$

For $t=k(m^2-mn+n^2)$, we obtain

$$u=k(2mn-n^2) \text{ and } v=k(2mn-m^2),$$

for some rational number $k$ such that $u,v,t$ are integers.

All quadruples $(x,y,z,t)$ satisfying the equations are given by

$$x=l+k(2mn-n^2),\quad y=l+k(2mn-m^2),$$
$$z=l,\quad t=k(m^2-mn+n^2).$$

(b) Seeking quadruples $(u,v,w,s)$ with $u+v+w=0$, we perform the substitutions $u=x-y$, $v=y-z$, $w=z-x$. The equation

reduces to the previous one; hence an infinite family of solutions in nonzero integers is

$$u = k(m^2 - n^2), \quad v = k(2mn - m^2),$$
$$w = k(n^2 - 2mn), \quad t = k(m^2 - mn + n^2),$$

where $k, m, n$ are chosen so that $uvwt \neq 0$.

Passing to absolute values yields infinitely many solutions in positive integers.

## 2.3 Other Remarkable Equations

**1.** *Let $p$ be a prime. Find all solutions to the equation*

$$a + b - c - d = p,$$

*where $a, b, c, d$ are positive integers such that $ab = cd$.*

(Mathematical Reflections)

*Solution.* Substitute $a = xy$, $b = zk$, $c = xz$, $d = yk$, and without loss of generality $a \geq b$. Then

$$a + b - c - d = (x - k)(y - z) = p$$

yields $x - k = 1$, $y - z = p$ or $x - k = p$, $y - z = 1$. So solutions for quadruples $(a, b, c, d)$ are quadruples

$$(xy, (y - p)(x - 1), x(y - p), y(x - 1)),$$

where $x, y \in \mathbb{Z}$.

**2.** *Let $a, b, c$ be integers such that*

$$\gcd(a, b, c) = 1 \text{ and } ab + bc + ca = 0.$$

*Prove that $|a+b+c|$ can be expressed in the form $x^2+xy+y^2$, where $x, y$ are integers.*

(Mathematical Reflections)

*Solution.* Note that if $a, b, c$ are integers such that $ab = c^2$, then there exist integers $k, m, n$ with $(m, n) = 1$ such that $a = km^2$, $b = kn^2$, $c = kmn$. Now $ab+bc+ca = 0$ is equivalent to $(a+b)(a+c) = a^2$. Therefore we have

$$\begin{aligned} a+b &= km^2, \\ a+c &= \pm kn^2, \\ a &= kmn, \end{aligned}$$

where $k \in \mathbb{Z}$. Since $\gcd(a, b, c) = 1$, we get $k = \pm 1$. So

$$a+b+c = k(m^2 - mn + n^2),$$

or

$$|a+b+c| = (-m)^2 + (-m)n + n^2.$$

**3.** *Prove that the equation*

$$x^2 + xy + y^2 = 36^2$$

*is not solvable in positive integers.*

*Solution.* Assume that the equation $x^2+xy+y^2 = 36^2$ is solvable. Using formulas (2.3.9), we obtain

$$k(m^2 + mn + n^2) = 36;$$

hence $m^2 + mn + n^2$ is one of the numbers $1, 2, 3, 4, 6, 9, 12, 18, 36$. None of these numbers appear in the third column of the table in Example 1.

**4.** *Find all pairs of positive integers such that*

$$x^2 - xy + y^2 = 727.$$

(Turkish Mathematical Olympiad)

*Solution.* Given any solution to $x^2 - xy + y^2 = 727$, we can apply the transformations $(x, y) \mapsto (y, y-x)$, then possibly $(x, y) \mapsto (y, x)$, to obtain another solution $(x, y)$ with $y \leq 0 \leq x \leq |y|$.

We now find all such solutions with $y \leq 0 \leq x \leq |y|$. Rearranging the required equation gives

$$y^2 - xy + x^2 - 727 = 0.$$

Viewing this as a quadratic in $y$, we can apply the quadratic formula to find that

$$y = \frac{x \pm \sqrt{2908 - 3x^2}}{2}.$$

Hence $2908 - 3x^2$ must be a perfect square, and it is not divisible by 3. Because $3x^2 \leq y^2 - xy + x^2 = 727$, we further know that $2181 \leq 2908 - 3x^2 \leq 2908$, giving $46 < \sqrt{2908 - 3x^2} < 54$. Testing these possibilities, we find that only $\sqrt{2908 - 3x^2} = 49$ has an integer solution $x$, yielding the unique solution $(13, -18)$ of the desired form.

Thus, every solution can be transformed into $(13, -18)$ by applying the two maps described earlier. Hence, any solution is in the orbit of $(13, -18)$ or $(-18, 13)$ under $(x, y) \mapsto (y, y - x)$, implying that all the solutions to $x^2 - xy + y^2 = 727$ are

$$(18, 31),\ (31, 13),\ (13, 31),\ (31, 18).$$

**5.** *We say that the positive integer $z$ satisfies property (P) if*

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

*for some positive integers $x$ and $y$. Prove that:*

*(a) if $z$ satisfies property (P), then so does $z^2$;*

*(b) if $z^2$ satisfies property (P) and $\gcd(x, y) = 1$, then so does $z$.*

(Dorin Andrica)

*Solution.* (a) Since $z = m^2+mn+n^2$, for some positive integers $m$ and $n, m > n$, it follows that $z^2 = q^2 + qr + r^2$, where $q = 2mn + n^2$ and $r = m^2 - n^2$.

(b) If $z^2 = x^2 + xy + y^2$, with $\gcd(x, y) = 1$, then from (2.3.9) we deduce that $x = 2mn + n^2$, $y = m^2 - n^2$, $m > n$, and $z = m^2 + mn + n^2$, for some positive integers $m$ and $n$.

**6.** *Solve in integers the equation*

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

*Solution.* Without loss of generality we may assume that

$$\gcd(x, y) = 1.$$

Also, note that $x$ and $y$ cannot have different parity. It follows that $x$ and $y$ are both odd. Setting $x + y = 2a$, $x - y = 2b$, $a, b \in \mathbb{Z}$, the equation becomes

$$a^2 - ab + b^2 = z^2.$$

From (2.3.11) it follows that

$$\begin{cases} a = 2mn - n^2, \\ b = m^2 - n^2, \\ z = m^2 - mn + n^2, \end{cases} \quad \text{or} \quad \begin{cases} a = m^2 - n^2, \\ b = 2mn - n^2, \\ z = m^2 - mn + n^2, \end{cases}$$

for some integers $m, n$.

The general solutions are

$$\Big(k(m^2+2mn-2n^2), k(2mn-m^2), k(m^2-mn+n^2)\Big)$$

and

$$\Big(k(m^2+2mn-2n^2), k(m^2-2mn), k(m^2-mn+n^2)\Big)$$

where $k, m, n \in \mathbb{Z}$.

**7.** *Find all triples $(x, y, z)$ of nonnegative integers satisfying the equation $x^4 + 14x^2y^2 + y^4 = z^2$.*

(Ion Cucurezeanu)

*Solution.* Let $(x, y, z)$ be a solution to the equation. Then

$$(2x)^4 + 14(2x)^2(2y)^2 + (2y)^4 = (4z)^2.$$

Setting $2x = a + b$, $2y = a - b$, $a, b \in \mathbb{Z}_+$, $a \geq b$, yields the equivalent equation

$$(a+b)^4 + 14(a^2-b^2)^2 + (a-b)^4 = 16z^2,$$

which reduces to

$$a^4 - a^2b^2 + b^4 = z^2.$$

From Theorem 2.3.3 we obtain

$$(a, b, z) = (k, k, k^2) \text{ and } (a, b, z) = (k, 0, k^2),$$

where $k \in \mathbb{Z}_+$. The solutions to the equation are

$$(x, y, z) = (k, 0, k^2), (0, k, k^2) \text{ and } (x, y, z) = (l, l, 4l^2),$$

where $k, l \in \mathbb{Z}_+$.

**8.** *Solve in positive integers the equation*

$$3x^4 + 10x^2y^2 + 3y^4 = z^2.$$

*Solution.* Write the equation in the form

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

It is not difficult to see that $x$ and $y$ have the same parity, for otherwise $z^2 \equiv 3 \pmod 4$, which is not possible. We may assume that $\gcd(x, y) = 1$. Then $\gcd(3x^2 + y^2, x^2 + 3y^2) = 1$, and so

$$3x^2 + y^2 = 4s^2 \text{ and } x^2 + 3y^2 = 4t^2$$

for some positive integers $s$ and $t$. Using the result in Example 2, we obtain $x = y = s = t = 1$.

The general solution is

$$(x, y, z) = (k, k, 4k^2), \quad k \in \mathbb{Z}_+.$$

*Solution 2.* Since $x$ and $y$ have the same parity, set $x = a + b$, $y = a - b$, $z = 4c$, where $a, b, c \in \mathbb{Z}_+$, $a > b$. Then

$$3(a + b)^4 + 10(a^2 - b^2)^2 + 3(a - b)^4 = 16c^2,$$

which reduces to

$$a^4 + a^2b^2 + b^4 = c^2.$$

From Theorem 2.3.2, it follows that $(a, b, c) = (k, 0, k^2)$ or $(a, b, c) = (0, k, k^2)$, $k \in \mathbb{Z}_+$.

The solutions are

$$(x, y, z) = (k, k, 4k^2), \quad k \in \mathbb{Z}_+.$$

**9.** *Find all distinct squares $a^2, b^2, c^2$ that form an arithmetic sequence.*

*Solution.* We have $a^2 + c^2 = 2b^2$, so we may assume without loss of generality that $a$ and $c$ are both odd.

Setting $a = u + v$, $c = u - v$, where $u, v \in \mathbb{Z}_+$, $u > v$ yields $u^2 + v^2 = b^2$. Then

$$\begin{cases} u = 2mn, \\ v = m^2 - n^2, \\ b = m^2 + n^2, \end{cases} \quad \text{or} \quad \begin{cases} u = m^2 - n^2, \\ v = 2mn, \\ b = m^2 + n^2, \end{cases}$$

for some positive integers $m, n$, with $m > n$. The desired triples are $((m^2 + 2mn - n^2)^2, (m^2 + n^2)^2, (m^2 - 2mn - n^2)^2)$ where $m, n \in \mathbb{Z}_+$, $m > n$.

**10.** *Solve in integers the equation*

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

(Titu Andreescu)

*Solution.* Multiply both sides by 8 and write the equation in the equivalent form

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

From Example 6 it follows that $x - y = 0$, so the solutions are $(x, y, z) = (k, k, k^2)$, $k \in \mathbb{Z}$.

*Solution 2.* We may assume that $x, y, z > 0$ and $\gcd(x, y) = 1$. Write the equation as

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

The condition $\gcd(x, y) = 1$ implies

$$\gcd(2xy, x^2 + y^2) = 1 \text{ or } \gcd(2xy, x^2 + y^2) = 2.$$

In the first case, it follows that $2xy = u^2$ and $x^2 + y^2 = v^2$, for some positive integers $u, v$. We obtain the system

$$\begin{cases} v^2 + u^2 = (x + y)^2, \\ v^2 - u^2 = (x - y)^2, \end{cases}$$

which is solvable only if $x - y = 0$ (see Example 2 in Section 2.2).

In the second case, we obtain the system

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

which can be written in the equivalent form

$$\begin{cases} (x + y)^2 + (x - y)^2 = (2v)^2, \\ (x + y)^2 - (x - y)^2 = (2u)^2, \end{cases}$$

and the same argument shows that $x - y = 0$.

**11.** *Find all integral triples $(x, y, z)$ satisfying the equation*

$$x^4 - 6x^2y^2 + y^4 = z^2.$$

*Solution.* We may assume that $x, y, z > 0$, $x > y$, and $\gcd(x, y) = 1$. Write the equation as

$$(x^2 - y^2)^2 - 4x^2y^2 = z^2.$$

Then

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

We will show that $\gcd(x^2-y^2+z, x^2-y^2-z) = 2$. We cannot have both $x$ and $y$ odd, for then $z^2 \equiv -4 \pmod{16}$. Let $x$ be odd and $y$ even. Then $z$ is odd and $\gcd(x^2-y^2+z, x^2-y^2-z)$ divides $2z$, so it is 2. It follows that

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

for some positive integers $a, b$, with $xy = ab$ and $\gcd(a,b) = 1$. Then $x^2-y^2 = a^2+b^2$, and so

$$(x^2+y^2)^2 = (a^2+b^2)^2 + 4a^2b^2.$$

We obtain

$$a^4+6a^2b^2+b^4 = (x^2+y^2)^2,$$

and from Example 6, $(a,b) = (k,0)$ or $(a,b) = (0,k)$, $k \in \mathbb{Z}$.

The solutions are $(x,y,z) = (k,0,k^2)$, $(x,y,z) = (0,k,k^2)$, $k \in \mathbb{Z}$.

**12.** *If $a$ and $b$ are distinct positive integers, then $2a(a^2+3b^2)$ is not a cube.*

*Solution.* Note that

$$2a(a^2+3b^2) = (a+b)^3 + (a-b)^3.$$

Hence if $2a(a^2+3b^2) = c^3$, then we obtain

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

By Theorem 2.3.8 it follows that the above relation is not possible.

**13.** *Prove that equation $x^6 - y^6 = 4z^3$ is not solvable in positive integers.*

(Titu Andreescu)

*Solution.* Assume that the equation is solvable in positive integers and let $(x, y, z)$ be a solution. Then $2(x^6 - y^6)$ is a perfect cube; hence

$$2(x^2 - y^2)\Big[(x^2 - y^2)^2 + 3(xy)^2\Big]$$

is a perfect cube. But this contradicts the result in Problem 10.

**14.** *Prove that the system of equations*

$$\begin{cases} x + y = z^2, \\ xy = \dfrac{z^4 - z}{3}, \end{cases}$$

*is not solvable in nonzero integers.*

(Titu Andreescu)

*First Solution.* Assuming that $(x, y, z)$ is a positive integral solution to the given system, we have

$$x^2 - xy + y^2 = (x + y)^2 - 3xy = z^4 - (z^4 - z) = z;$$

hence $x^3 + y^3 = (x + y)(x^2 - xy + y^2) = z^2 \cdot z = z^3$, in contradiction to the result in Theorem 2.3.8.

*Second Solution.* We have $z^4 = (x + y)^2 \geq 4xy = 4(z^4 - z)/3$, or on rearranging, $4z \geq z^4$. This means that $z > 0$ and $4 \geq z^3$. Hence $z = 1$, and we get $xy = 0$, a contradiction.

# II.3

# Solutions to Pell-Type Equations

## 3.1 Solving Pell's Equation by Elementary Methods

**1.** *Find all positive integers $n$ such that $\frac{n(n+1)}{3}$ is a perfect square.*

(Dorin Andrica)

*Solution.* Let $\frac{n(n+1)}{3} = y^2$, which is equivalent to

$$(2n+1)^2 - 12y^2 = 1.$$

The Pell's equation $x^2 - 12y^2 = 1$ has $(7, 2)$ as fundamental solution, and all its solutions are given by

$$x_m = \frac{1}{2}\Big[(7+2\sqrt{12})^m + (7-2\sqrt{12})^m\Big],$$
$$y_m = \frac{1}{2\sqrt{12}}\Big[(7+2\sqrt{12})^m - (7-2\sqrt{12})^m\Big].$$

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, DOI 10.1007/978-0-8176-4549-6_7, © Springer Science+Business Media, LLC 2010

It follows that

$$2n_m + 1 = x_m = \frac{1}{2}\Big[(2+\sqrt{3})^{2m} + (2-\sqrt{3})^{2m}\Big], \quad m \geq 1;$$

hence the desired numbers are

$$n_m = \left[\frac{(2+\sqrt{3})^m - (2-\sqrt{3})^m}{2}\right]^2 = 3\left[\frac{(2+\sqrt{3})^m - (2-\sqrt{3})^m}{2\sqrt{3}}\right]^2,$$

$m \geq 0$.

**Remark.** Note that all $n$ with this property are of the form $3k^2$.

**2.** *Find all triangles having side lengths consecutive integers and area also an integer.*

*Solution.* Let the sides be $z-1, z, z+1$. The semiperimeter $s$ and the area $A$ are $\frac{3z}{2}$ and $A = \frac{z\sqrt{3(z^2-4)}}{4}$, respectively. If $A$ is an integer, then $z$ cannot be odd, say $z = 2x$, and $z^2 - 4 = 3u^2$. So $4x^2 - 4 = 3u^2$, which implies that $u$ is even, say $u = 2y$. Then $x^2 - 3y^2 = 1$, which has $(2,1)$ as fundamental solution. Therefore all positive integral solutions are $(x_n, y_n)$, where

$$x_n = \frac{1}{2}\Big[(2+\sqrt{3})^n + (2-\sqrt{3})^n\Big],$$
$$y_n = \frac{1}{2\sqrt{3}}\Big[(2+\sqrt{3})^n - (2-\sqrt{3})^n\Big], \ n \geq 1.$$

The sides of the triangles are $2x_n - 1, 2x_n, 2x_n + 1$, and the areas are $A = 3x_n y_n$.

**3.** *Prove that there are infinitely many triples $(a,b,c)$ of positive integers such that the greatest common divisor of $a$, $b$, and $c$ is 1, and $a^2b^2 + b^2c^2 + c^2a^2$ is the square of an integer.*

*Solution.* Suppose $a^2b^2 + b^2c^2 + c^2a^2 = d^2$, and rewrite the equation as

$$d^2 - (a^2+b^2)c^2 = a^2b^2.$$

With $a = 1$, this reduces to

$$d^2 - (b^2 + 1)c^2 = b^2.$$

Now let $b = 1$ to obtain $d^2 - 2c^2 = 1$. This is a Pell's equation, having the fundamental solution $(d_1, c_1) = (3, 2)$. The general solution of this Pell's equation is

$$d_n = \frac{1}{2}\Big[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n\Big], \quad c_n = \frac{1}{2\sqrt{2}}\Big[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n\Big],$$

generating infinitely many triples $(1, 1, c_n)$.

**4.** *Prove that there are infinitely many positive integers $n$ such that $\lceil\sqrt{2}n\rceil$ is a perfect square.*

*Solution.* We consider the equation

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

with the fundamental solution $(x, y) = (3, 2)$. By Theorem 3.2.1, it has infinitely many positive integer solutions. For each of these solutions, we have

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

implying that

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

or

$$x^2 - 1 < xy\sqrt{2} < x^2.$$

Setting $n = xy$ shows that $\lceil n\sqrt{2}\rceil = x^2$ is a perfect square.

**5.** *Prove that there are infinitely many triples $(a, b, c)$ of integers such that*

$$a^4 + b^3 = c^2,$$

*and* $\gcd(a, c) = 1$.

*Solution.* To prove this, factor the equation

$$b^3 = c^2 - a^4$$

as

$$b^3 = (c + a^2)(c - a^2).$$

If $a$ and $c$ have opposite parity, the two factors on the right are relatively prime, so there are integers $m$ and $n$ such that

$$m^3 = c + a^2, \quad n^3 = c - a^2.$$

It follows that we have a solution if we can find integers $a$ and $c$ of the form

$$c = \frac{m^3 + n^3}{2}, \quad a^2 = \frac{m^3 - n^3}{2}.$$

These values of $a^2$ and $c$ are clearly integers (since $m$ and $n$ are both odd), so the only constraint on $m$ and $n$ is that they make $a$ an integer. There are several ways of constructing an infinite family with this property. For example, if we restrict ourselves to "twin" values of $m$ and $n$, meaning that $m = k+1$ and $n = k-1$, the above equation for $a^2$ becomes

$$a^2 - 3k^2 = 1,$$

which is a Pell equation. By the usual method we have the fundamental solution $(a_1, k_1) = (2, 1)$. All solutions $(a_j, k_j)$ are given by

$$a_j + k_j\sqrt{3} = (2 + \sqrt{3})^j, \quad j = 1, 2, \ldots;$$

hence

$$a_j = \frac{1}{2}\Big[(2+\sqrt{3})^j + (2-\sqrt{3})^j\Big],$$
$$k_j = \frac{1}{2\sqrt{3}}\Big[(2+\sqrt{3})^j - (2-\sqrt{3})^j\Big],\ j = 1, 2, \ldots.$$

We obtain the triples $(a_j, (k_j^2 - 1), k_j^3 + 3k_j)$, $j = 1, 2, \ldots$.

**6.** *Solve in positive integers the equation*

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

*Solution.* Substituting $u = y - 2x$, the equation becomes

$$u^2 - 3x^2 = 1.$$

The general solution $(u_n, x_n)$ is given by

$$u_n + x_n\sqrt{3} = (2+\sqrt{3})^n.$$

We obtain

$$x_n = \frac{1}{2\sqrt{3}}\Big[(2+\sqrt{3})^n - (2-\sqrt{3})^n\Big], \quad u_n = \frac{1}{2}\Big[(2+\sqrt{3})^n + (2-\sqrt{3})^n\Big];$$

hence

$$y_n = u_n + 2x_n = \frac{1}{2\sqrt{3}}\Big[(2+\sqrt{3})^{n+1} - (2-\sqrt{3})^{n+1}\Big].$$

Because of the symmetry, the equation also has the solution $(y_n, x_n)$.

**7.** *Let* $a_0 = 0$, $a_1 = 4$, *and* $a_{n+1} = 18a_n - a_{n-1}$, $n \geq 1$. *Prove that* $5a_n^2 + 1$ *is a perfect square for all* $n$.

*Solution.* Consider the Pell's equation

$$x^2 - 5y^2 = 1,$$

with the fundamental solution $(9, 4)$. Its general solution is given by

$$x_n + y_n\sqrt{5} = (9 + 4\sqrt{5})^n, \quad n \geq 0.$$

According to Theorem 3.2.1, sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ satisfy the recurrence relations

$$x_{n+1} = 9x_n + 20y_n, \quad y_{n+1} = 4x_n + 9y_n, \quad n \geq 0,$$

with $x_0 = 1$ and $y_0 = 0$. Moreover, $y_1 = 4$, and substituting $4x_n = y_{n+1} - 9y_n$ into the first relation yields

$$\frac{1}{4}(y_{n+2} - 9y_{n+1}) = 9 \cdot \frac{1}{4}(y_{n+1} - 9y_n) + 20y_n,$$

that is, $y_{n+2} = 18y_{n+1} - y_n$, $n \geq 0$.

Because sequences $(a_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ satisfy the same recurrence relation and $a_0 = y_0$, $a_1 = y_1$, it follows that $a_n = y_n$ for all $n$.

On the other hand, $5a_n^2 + 1 = 5y_n^2 + 1 = x_n^2$, for all $n \geq 0$.

**8.** *Prove that if the difference of two consecutive cubes is $n^2$, then $2n - 1$ is a square.*

*Solution.* Let

$$(m + 1)^3 - m^3 = 3m^2 + 3m + 1 = n^2.$$

Then

$$(2n)^2 = 3(2m + 1)^2 + 1,$$

so $(2n, 2m + 1)$ is a solution of Pell's equation

$$x^2 - 3y^2 = 1.$$

As shown already, we obtain

$$2n + (2m + 1)\sqrt{3} = (2 + \sqrt{3})^l.$$

In order for $n$ to be integral, $l$ must be odd. It follows that

$$4n = (2+\sqrt{3})^{2k+1} + (2-\sqrt{3})^{2k+1}.$$

Finally,

$$2n - 1 = \frac{(1+\sqrt{3})^2(2+\sqrt{3})^{2k} + (1-\sqrt{3})^2(2-\sqrt{3})^{2k} - 4}{4} = N^2,$$

where

$$N = \frac{1}{2}((1+\sqrt{3})(2+\sqrt{3})^k + (1-\sqrt{3})(2-\sqrt{3})^k)$$

is an integer.

**9.** *Consider the system of equations*

$$\begin{cases} x + y = z + u, \\ 2xy = zu. \end{cases}$$

*Find the largest value of the real constant $m$ such that $m \le \frac{x}{y}$ for any positive integral solution $(x, y, z, u)$ of the system, with $x \ge y$.*

(42nd IMO Shortlist)

*Solution.* Squaring the first equation and then subtracting four times the second, we obtain

$$x^2 - 6xy + y^2 = (z-u)^2,$$

from which

$$\left(\frac{x}{y}\right)^2 - 6\left(\frac{x}{y}\right) + 1 = \left(\frac{z-u}{y}\right)^2. \tag{1}$$

The quadratic $\omega^2 - 6\omega + 1$ takes the value 0 for $\omega = 3 \pm 2\sqrt{2}$, and is positive for $\omega > 3 + 2\sqrt{2}$. Because $x/y \ge 1$ and the right side of (1) is a square, the left side of (1) is positive, and we must have

$x/y > 3 + 2\sqrt{2}$. We now show that $x/y$ can be made as close to $3 + 2\sqrt{2}$ as we like, so the desired valued of $m$ is $3 + 2\sqrt{2}$. We prove this by showing that the term $((z - u)/y)^2$ in (1) can be made as small as we like.

To this end, we first find a way to generate solutions of the system. If $p$ is a prime divisor of $z$ and $u$, then $p$ is a divisor of both $x$ and $y$. Thus we may assume, without loss of generality, that $z$ and $u$ are relatively prime. If we square both sides of the first equation and then subtract twice the second equation, we have

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

Thus $(z, u, x - y)$ is a primitive Pythagorean triple, and we may assume that $u$ is even. Hence there are relatively prime positive integers $a$ and $b$, one of them even and the other odd, such that

$$z = a^2 - b^2, \quad u = 2ab, \quad \text{and} \quad x - y = a^2 + b^2.$$

Combining these equations with $x + y = z + u$, we find that

$$x = a^2 + ab \text{ and } y = ab - b^2.$$

Observe that $z - u = a^2 - b^2 - 2ab = (a - b)^2 - 2b^2$. When $z - u = 1$, we get the Pell equation

$$(a - b)^2 - 2b^2 = 1,$$

whose fundamental solution is $a - b = 3$, $b = 2$.

This equation has infinitely many positive integer solutions $a - b$ and $b$, and both of these quantities can be made arbitrarily large. It follows that $y = ab - b^2$ can be made arbitrarily large. Hence the right

side of (1) can be made as small as we like, and the corresponding value of $x/y$ can be made as close to $3 + 2\sqrt{2}$ as we like.

**10.** *Prove that the equation* $x^2 - Dy^4 = 1$ *has no positive integer solution if* $D \not\equiv 0, 3, 8, 15 \pmod{16}$ *and there is no factorization* $D = pq$, *where* $p > 1$ *is odd,* $\gcd(p, q) = 1$, *and either* $p \equiv \pm 1 \pmod{16}$, $p \equiv q \pm 1 \pmod{16}$, *or* $p \equiv 4q \pm 1 \pmod{16}$.

*Solution.* Let $x, y > 0$ be a nontrivial solution with minimal $y$. If $y$ is odd, then

$$Dy^4 + 1 \not\equiv 0, 1, 4, 9 \pmod{16},$$

and thus it is not a quadratic residue modulo 16. Thus $y$ should be even and $x$ odd. Further, we have

$$x + 1 = 2pa^4, \quad x - 1 = 8qb^4, \quad y = 2ab,$$

or

$$x - 1 = 2pa^4, \quad x + 1 = 8qb^4, \quad y = 2ab,$$

where $D = pq$, $\gcd(p, q) = 1$, and $a$ is odd.

If $p > 1$, then

$$pa^4 - 4qb^4 = \pm 1.$$

If $b$ is even, then $p \equiv \pm 1 \pmod{16}$, contradiction. If $b$ is odd, then $p \equiv 4q \pm 1 \pmod{16}$, again false.

Thus $p = 1$ and

$$a^4 - 4Db^4 = \pm 1.$$

The equation $a^4 - 4Db^4 = -1$ has no solution modulo 4; thus $a^4 - 1 = 4Db^4$. Then $D = rs$, $b = cd$, $\gcd(r, s) = 1$, and

$$a^2 + 1 = 2rc^4, \quad a^2 - 1 = 2sd^4.$$

Thus $c$, $r$ are odd, and we have

$$rc^4 - sd^4 = 1.$$

If $r = 1$, then $c^4 - Dd^4 = 1$ and $y = 2acd$, so there exists a solution of our equation with $d \leq y/2$, contradicting the minimality of $y$.

If $r > 1$, then $d$ cannot be even because $r \not\equiv \pm 1 \pmod{16}$. But if $d$ is odd, then $r \equiv s + 1 \pmod{16}$, contradicting our assumptions.

**Remark.** In 1942, W. Ljunggren proved that the equation $x^2 - Dy^4 = 1$ has at most two positive integer solutions if $D > 0$ is not a perfect square. He also gave an algorithm that computes the nontrivial solution when it exists.

## 3.2 The Equation $ax^2 - by^2 = 1$

**1.** *Prove that there are infinitely many quadruples $(x, y, u, v)$ of positive integers such that $x^2 + y^2 = 6(z^2 + w^2) + 1$ with $3 \mid x$ and $2 \mid y$.*

(Dorin Andrica)

*Solution.* The equation $3r^2 - 2s^2 = 1$ has minimal solution $(x_0, y_0) = (1, 1)$, and from Theorem 3.3.2 all its solutions are given by

$$r_n = u_n + 2v_n, \quad s_n = u_n + 3v_n, \quad n \geq 0,$$

where $(u_n, v_n)_{n \geq 0}$ is the general solution to Pell's resolvent $u^2 - 6v^2 = 1$.

The quadruples $(x, y, z, w) = (3r_k r_l, 2s_k s_l, r_k s_l, r_l s_k)$, $k, l \geq 0$ have the desired property. Indeed,

$$x^2 + y^2 - 6(z^2 + w^2) = 8r_k^2 r_l^2 + 4s_k^2 s_l^2 - 6r_k^2 s_l^2 - 6r_l^2 s_k^2$$
$$= (3r_k^2 - 2s_k^2)(3r_l^2 - 2s_l^2) = 1 \cdot 1 = 1,$$

and $3 \mid x$, $2 \mid y$.

**Remark.** The solution $(3r_k, 2s_l, s_k, r_l)$ also works and it is easier to check:

$$(3r_k)^2 + (2s_l) - 6s_k^2 - 6r_l^2 = 3(3r_k^2 - 2s_k^2) - 2(3r_l^2 - 2s_l^2) = 3 - 2 = 1.$$

**2.** *(a) Find all positive integers $n$ such that $n + 1$ and $3n + 1$ are simultaneously perfect squares.*

*(b) If $n_1 < n_2 < \cdots < n_k < \cdots$ are all positive integers satisfying the above property, then $n_k n_{k+1} + 1$ is also a perfect square, $k = 1, 2, \ldots$.*

(American Mathematical Monthly)

*Solution.* (a) If $n + 1 = x^2$ and $3n + 1 = y^2$, then $3x^2 - y^2 = 2$, which is equivalent to the Pell's equation

$$u^2 - 3v^2 = 1,$$

where $u = \frac{1}{2}(3x - y)$ and $v = \frac{1}{2}(y - x)$. The general solution is $(u_k, v_k)_{k \geq 0}$, where

$$u_k = \frac{1}{2}\left[(2+\sqrt{3})^k + (2-\sqrt{3})^k\right],\ v_k = \frac{1}{2\sqrt{3}}\left[(2+\sqrt{3})^k - (2-\sqrt{3})^k\right],\ k \geq 0;$$

hence

$$n_k = x_k^2 - 1 = (u_k + v_k)^2 - 1 = \frac{1}{6}\left[(2+\sqrt{3})^{2k+1} + (2-\sqrt{3})^{2k+1} - 4\right],\ k \geq 0.$$

(b) We have

$$n_k n_{k+1} + 1 = \left\{ \frac{1}{6}[(2+\sqrt{3})^{2k+2} + (2-\sqrt{3})^{2k+2} - 8] \right\}^2, \quad k \geq 0.$$

**3.** *Prove that there exist two strictly increasing sequences* $(a_n)$ *and* $(b_n)$ *of positive integers such that* $a_n(a_n+1)$ *divides* $b_n^2+1$ *for all* $n \geq 1$.

(40th IMO Shortlist)

*Solution.* It suffices to find increasing sequences $(a_n), (b_n)$ of positive integers and a positive integer $k$ such that $b_n^2 + 1 = k(a_n^2 + a_n)$, for all $n \geq 1$. The last relation is equivalent to

$$k(2a_n+1)^2 - (2b_n)^2 = k + 4.$$

For $k = 5$, the equation

$$5x^2 - y^2 = 9$$

has infinitely many solutions. Indeed, $(3, 6)$ is a solution and the pairs $(x_n, y_n)$, where

$$x_n = 3u_n + 6v_n, \quad y_n = 6u_n + 15v_n, \quad n \geq 1;$$

and $(u_n, v_n)$ is the general solution to Pell's equation $u^2 - 5v^2 = 1$, satisfy the equation. Indeed,

$$\begin{aligned} 5x_n^2 - y_n^2 &= 5(3u_n + 6v_n)^2 - (6u_n + 15v_n)^2 \\ &= 9u_n^2 - 45v_n^2 = 9(u_n^2 - 5v_n^2) = 9 \cdot 1 = 9 \end{aligned}$$

for all $n \geq 0$.

It is clear that $u_n^2 - 5v_n^2 = 1$ implies $u_n$ odd and $v_n$ even for all $n \geq 0$.

It follows that the sequences $(a_n), (b_n)$, where

$$a_n = \frac{x_n - 1}{2} = \frac{3u_n - 1}{2} + 3v_n, \quad b_n = \frac{y_n}{2} = 3u_n + 15\frac{v_n}{2}, \quad n \geq 0,$$

contain only positive integers, are increasing, and $a_n(a_n + 1)$ divides $b_n^2 + 1$ for all $n \geq 0$.

**4.** *Let $x$ and $y$ be positive integers such that $x(y+1)$ and $y(x+1)$ are perfect squares. Prove that either $x$ or $y$ is a perfect square.*

(Titu Andreescu, Iurie Boreico)

*Solution.* Suppose $x = an^2$ and $y = bv^2$ for some positive integers $a, b, u, v$, where $a$ and $b$ are square-free. Then $au^2(bv^2 + 1)$ and $bv^2(au^2 + 1)$ are perfect squares, so there are positive integers $s$ and $t$ such that

$$a(bv^2 + 1) = (as)^2 \text{ and } b(au^2 + 1) = (bt)^2.$$

Then

$$as^2 - bv^2 = 1 \text{ and } au^2 - bt^2 = -1.$$

From Example 3, $a = 1$ or $b = 1$ and the conclusion follows.

## 3.3 The Negative Pell's Equation

**1.** *Find all pairs $(x, y)$ of positive integers satisfying the equation*

$$x^2 - 6xy + y^2 = 1.$$

(Titu Andreescu)

*Solution.* The equation is equivalent to

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

Without loss of generality we may assume $x \geq y$.

Performing the substitutions $X=x+y$, $Y=x-y$, we obtain the negative Pell's equation

$$X^2-2Y^2=-1.$$

By Theorem 3.4.1, its general solution $(X_n,Y_n)_{n\geq 1}$ is given by

$$X_n=u_n+2v_n, \quad Y_n=u_n+v_n,$$

where $(u_n,v_n)_{n\geq 1}$ is the general solution to the Pell's resolvent $u^2-2v^2=1$, that is,

$$\begin{aligned} u_n &= \frac{1}{2}\Big[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n\Big], \\ v_n &= \frac{1}{2\sqrt{2}}\Big[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n\Big]. \end{aligned}$$

We obtain

$$\begin{aligned} X_n &= u_n+2v_n=\frac{1}{2}\Big[(1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}\Big], \\ Y_n &= u_n+v_n=\frac{1}{2\sqrt{2}}\Big[(1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}\Big]; \end{aligned}$$

hence

$$\begin{aligned} x_n &= \frac{1}{2}(X_n+Y_n)=\frac{1}{4\sqrt{2}}\Big[(1+\sqrt{2})^{2n+2}-(1-\sqrt{2})^{2n+2}\Big], \\ y_n &= \frac{1}{2}(X_n-Y_n)=\frac{1}{4\sqrt{2}}\Big[(1+\sqrt{2})^{2n}-(1-\sqrt{2})^{2n}\Big]. \end{aligned}$$

The sequence $(P_m)_{m\geq 1}$ given by

$$P_m=\frac{1}{2\sqrt{2}}\Big[(1+\sqrt{2})^m-(1-\sqrt{2})^m\Big]$$

is known as *Pell's sequence*. It satisfies the recurrence relation $P_{m+1} = 2P_m + P_{m-1}$, $P_1 = 1$, $P_2 = 2$. Hence the solutions to our equation can be written in the form

$$(x_n, y_n) = \left(\frac{1}{2}P_{2n+2}, \frac{1}{2}P_{2n}\right), \quad (x_n, y_n) = \left(\frac{1}{2}P_{2n}, \frac{1}{2}P_{2n+2}\right), \ n \geq 1,$$

where the second solution follows by the symmetry in $x$ and $y$.

**2.** *Prove that there are infinitely many positive integers $n$ such that $n^2 + 1$ divides $n!$.*

(Kvant)

*Solution.* The equation $x^2 - 5y^2 = -1$ has $(2, 1)$ as its least positive solution. So it has infinitely many positive solutions. Consider those solutions with $y > 5$. Then $5 < y < 2y \leq x$, since $4y^2 \leq 5y^2 - 1 = x^2$. Therefore $2(x^2 + 1) = 5y \cdot 2y$ divides $x!$.

**3.** *Let $a_n = \left[\sqrt{n^2 + (n+1)^2}\right]$, $n \geq 1$. Prove that there are infinitely many $n$'s such that $a_n - a_{n-1} > 1$ and $a_{n+1} - a_n = 1$.*

*First Solution.* First, consider $n^2 + (n+1)^2 = y^2$, which can be rewritten as $(2n+1)^2 - 2y^2 = -1$. This negative Pell's equation has infinitely many solutions $(x, y)$ and each $x$ is odd, say $x = 2n + 1$, for some $n$. For these $n$'s, $a_n = y$ and

$$a_{n-1} = \left[\sqrt{(n-1)^2 + n^2}\right] = \left[\sqrt{y^2 - 4n}\right]$$

implies $n > 2$ and

$$a_{n-1} \leq \sqrt{y^2 - 4n} < y - 1 = a_n - 1,$$

i.e., $a_n - a_{n-1} > 1$.

Also, for these $n$'s,

$$a_{n+1} = \left[\sqrt{(n+1)^2 + (n+2)^2}\right] = \left[\sqrt{y^2 + 4n + 4}\right].$$

Since $n < y < 2n + 1$, we easily get

$$y + 1 < \sqrt{y^2 + 4n + 4} < y + 2, \text{ so } a_{n+1} - a_n = (y + 1) - y = 1.$$

*Second Solution.* If $a_n = k \geq 1$ so that $k^2 \leq n^2 + (n+1)^2 < (k+1)^2$, then $16(n + 1)^2 \geq 8k^2 \geq (2k + 1)^2$ so $4(n + 1) \geq 2k + 1$. Hence $(k + 1)^2 \leq n^2 + (n + 1)^2 + 4(n + 1) = (n + 1)^2 + (n + 2)^2$. Thus $a_{n+1} - a_n \geq 1$. Also one easily computes that $\lim_{n\to\infty} a_n/n = \sqrt{2}$. Therefore there must be arbitrarily large $n$ with $a_n - a_{n-1} > 1$, but this cannot hold for all large $n$, so there must be infinitely many transitions back to difference 1.

**4.** *Let $k$ be an integer greater than 2. Prove that*

$$x^2 - (k^2 - 4)y^2 = -1$$

*is solvable if and only if $k = 3$.*

*Solution.* We will show that

$$u^2 - (k^2 - 4)v^2 = -4 \tag{1}$$

is not solvable if $k \neq 3$. Assume the contrary and let $(u, v)$ be a solution. Then $u$ and $kv$ have the same parity. Consider $x = \frac{u+kv}{2}$. Then $u = 2x - kv$, and (1) becomes

$$x^2 + v^2 + 1 = xvk.$$

Since $k \neq 3$, this contradicts the result in Problem 6(a) in Section 1.6.

Assume now that for $k \neq 3$, (1) has a solution $(x, y)$. Multiplying both sides by 4 yields

$$(2x)^2 - (k^2 - 4)(2y)^2 = -4,$$

contradicting the above result concerning (1).

When $k = 3$, (1) becomes

$$x^2 - 5y^2 = -1. \tag{2}$$

The minimal solution to (2) is $(2, 1)$. From the general theory of Pell-type equations it follows that all solutions to (2) are given by $(x_n, y_n)$, $n \geq 0$, where

$$\begin{aligned} x_n &= \frac{1}{2}\left[(1 + 2\sqrt{5})(2 + \sqrt{5})^{2n} + (1 - 2\sqrt{5})(2 - \sqrt{5})^{2n}\right], \\ y_n &= \frac{1}{2}\left[\left(2 + \frac{1}{\sqrt{5}}\right)(2 + \sqrt{5})^{2n} + \left(2 - \frac{1}{\sqrt{5}}\right)(2 - \sqrt{5})^{2n}\right]. \end{aligned} \tag{3}$$

**Remark.** The equation $x^2 + y^2 + 1 = kxy$ is solvable in integers if and only if the quadratic equation

$$x^2 - (ky)x + y^2 + 1 = 0$$

in $x$ has integral solutions. This means that if its discriminant

$$\Delta = (ky)^2 - 4y^2 - 4 = (k^2 - 4)y^2 - 4$$

is a perfect square, then (1) is solvable. From Problem 6(a) in Section 1.6 it follows that the first equation is solvable only if $k = 3$, so (1) is solvable only if $k = 3$. The same argument as in the previous proof shows that if (1) is solvable only for $k = 3$, then the same is true for the equation $u^2 - (k^2 - 4)v^2 = -4$.

**5.** *Prove that if* $\frac{a^2+1}{b^2}+4$ *is a perfect square, then this square is* 9.

*Solution.* Let

$$\frac{a^2+1}{b^2}+4=k^2$$

for some positive integer $k$. Then $a^2+1=(k^2-4)b^2$, that is, $a^2-(k^2-4)b^2=-1$. From the previous problem it follows that $k=3$.

**Remark.** There are infinitely many pairs $(a,b)$ with this property. All of them are $(a,b)=(x_n,y_n)$, where $x_n$ and $y_n$ are given by (3) in the previous problem.

**6.** *Find all pairs* $(m,n)$ *of integers such that* $mn+m$ *and* $mn+n$ *are both squares.*

(Titu Andreescu, Iurie Boreico)

*Solution.* The pairs $(0,k^2)$ and $(k^2,0)$ are trivial solutions. For $mn\neq 0$, $m=\pm aq^2$ and $n=\pm br^2$, for some positive integers $q,r,a$, and $b$, where the signs + and − correspond. Then, as in the solution to Problem 4 in Section 3.3, there are positive integers $s$ and $t$ such that $as^2-bt^2=\pm 1$ and $as^2-bt^2=\mp 1$, and from Example 3 in the same section, it follows that $a=1$ or $b=1$. The problem reduces to finding all pairs $(x,y)$ of positive integers with $x>1$ such that $(x^2-1)(y^2+1)$ is a perfect square. Such pairs exist if and only if there are a square-free positive integer $d$ and positive integers $w$ and $z$ such that $x^2-1=dw^2$ and $y^2+1=dz^2$. Because the Pell's equation $x^2-dw^2=1$ is solvable for each square-free positive integer $d$, this boils down to the solvability in positive integers of the negative Pell's equation $y^2-dz^2=-1$.

Hence let $D$ be the set of all square-free positive integers $d$ for which the equation $y^2-dz^2=-1$ is solvable in positive integers.

Then for each such $d$ let $(y_0(d), z_0(d))$ be its minimal solution. From Theorem 3.4.1, the general solution to $y^2 - dz^2 = -1$ is $(y_k(d), z_k(d))$,

$$y_k(d) = y_0(d)u_k(d) + dz_0(d)v_k(d),\ \ z_k(d) = z_0(d)u_n kd) + y_0(d)v_k(d),$$

where $(u_k(d), v_k(d))$ is the general solution to the Pell's equation

$$u^2 - dv^2 = 1.$$

It follows that all pairs $(m, n) = (m_k, n_k)$ are

$$(dv_k(d)^2, y_k(d)^2),\ \ (-dz_k(d)^2, -u_k(d)^2),$$

and the other two symmetric pairs.

# II.4

# Solutions to Some Advanced Methods in Solving Diophantine Equations

## 4.1 The Ring $\mathbb{Z}[i]$ of Gaussian Integers

**1.** *Solve the equation*

$$x^2 + 4 = y^n,$$

*where $n$ is an integer greater than* 1.

*Solution.* For $n = 2$, the only solutions are $(0, 2)$ and $(0, -2)$. For $n = 3$, we have seen in Example 4 that the solutions are $(2, 2)$, $(-2, 2)$, $(11, 5)$, and $(-11, 5)$. Let now $n \geq 4$. Clearly, for $n$ even, the equation is not solvable, since no other squares differ by 4. For $n$ odd, we may assume without loss of generality that $n$ is a prime $p \geq 5$. Indeed, if $n = qk$, where $q$ is an odd prime, we obtain an equation of the same type: $x^2 + 4 = (y^k)^q$.

For $x$ odd we have $(2+ix)(2-ix) = y^p$ and $\gcd(2+ix, 2-ix) = 1$ in $\mathbb{Z}[i]$. Using the uniqueness of the prime factorization in $\mathbb{Z}[i]$, it follows

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*, 309
DOI 10.1007/978-0-8176-4549-6_8, © Springer Science+Business Media, LLC 2010

that $2+ix=(a+ib)^p$ for some integers $a$ and $b$ having different parities. Identifying the real and imaginary parts, we obtain

$$2=2^p-\binom{p}{2}a^{p-2}b^2+\cdots+(-1)^{\frac{p-1}{2}}pab^{p-1}. \tag{1}$$

It is clear that all terms in the above relation are even and $a \mid 2$. Hence $a=\pm 2$, and from Fermat's little theorem, it follows that $a=2$ and $b$ is odd. Relation (1) becomes

$$1=2^{p-1}-\binom{p}{2}2^{p-3}b^2+\cdots+(-1)^{\frac{p-1}{2}}pb^{p-1}. \tag{2}$$

We will prove that $b^2=1$. Indeed, if $q \mid b$ for some odd prime, from (2) it follows that $2^{p-1}\equiv 1 \pmod{q^2}$. Using again Fermat's little theorem, we obtain $q \mid p-1$. Indeed, since $2^{q-1}\equiv 1 \pmod{q}$, there is a divisor $s$ of $q-1$ such that $2^s\equiv 1 \pmod{q}$. Let $s$ be the least such divisor. We have $s \mid q-1$ and $s \mid p-1$. Moreover, $2^{sq}\equiv 1 \pmod{q^2}$; hence $sq \mid p-1$, i.e., $q \mid p-1$. If $b^2\neq 1$, then the exponent of $q$ in each term $(-1)^k\binom{p}{2k}2^{p-1-2k}b^{2k}$, $k=1,2,\ldots,\frac{p-1}{2}$, of (2) is greater than the exponent of (2) in $2^{p-1}-1$, a contradiction. Hence $b^2=1$. Then $2+ix=(2\pm i)^p$ and $|2+ix|=|2\pm i|^p$, yielding $4+x^2=5^p$.

The relation (2) becomes

$$1=2^{p-1}-\binom{p}{2}2^{p-3}+\cdots+(-1)^{p-1}p. \tag{3}$$

If $p=4m+1$, let $p=2^\alpha q+1$ with $q$ odd. From (3) it follows that $1\equiv p \pmod{2^{\alpha+1}}$, a contradiction. Hence in this case the equation is not solvable.

Let $p = 4m + 3$, $m \geq 1$. Assume $p = 2^\beta q + 3$, with $q$ odd. Using again relation (3), we obtain

$$1 \equiv -p + \binom{p}{p-3} 4 \pmod{2^{\beta+2}};$$

hence $p \equiv 3 \pmod{2^{\beta+1}}$, a contradiction.

Hence there are no solutions for $p \geq 5$ and $x$ odd.

If $x$ is even, say $x = 2u$, then $y$ is even, $y = 2v$. The equation becomes $u^2 + 1 = 2^{p-2}v^p$. Because $p - 2 > 2$, this equation is not solvable, because 4 does not divide $u^2 + 1$, so there are no solutions for $p \geq 5$ and $x$ even as well.

**Remark.** The perfect squares in the sequence $5^n - 2^m$, $m, n \geq 0$ are $0, 1, 4, 9$, and 121. Indeed, if $n = 2k$, $k \geq 1$, the relation $5^n - 2^m = x^2$ is equivalent to $(5^k - x)(5^k + x) = 2^m$, yielding $5^k - x = 2^{\alpha+1}$ and $5^k + x = 2^{\beta+1}$ with $\alpha + \beta = m - 2$, $\alpha < \beta$. It follows that $5^k = 2^\alpha + 2^\beta$ and $\alpha$ must be 0. We obtain $5^k = 1 + 2^\beta$. For $k$ even, we get $(5^{\frac{k}{2}} - 1)(5^{\frac{k}{2}} + 1) = 2^\beta$, which is not possible. For $k$ odd, we have $(1 + 4)^k = 1 + 4\binom{k}{1} + 4^2\binom{k}{2} + \cdots = 1 + 2^\beta$; hence $k + 4\binom{k}{2} + \cdots = 2^\beta$, yielding a contradiction for $k \geq 3$. Hence $k = 1$, $\beta = 2$, and $x^2 = 5^2 - 2^4 = 9$.

Assume $n$ odd. Then $5^n \equiv 5 \pmod 8$. But for $m \geq 3$, $5^5 - x^2 = 2^m \equiv 0 \pmod 8$, which is impossible. Hence $m \in \{0, 1, 2\}$. For $m = 0$ we get $x^2 + 1 = 5^n$, which, according to Example 1, is not solvable for $n \geq 2$. It follows that $n = 1$ and $x^2 = 4$. For $m = 1$, we have $x^2 + 2 = 5^n$, which is impossible, as we tell by looking modulo 4. For $m = 2$, $x^2 + 4 = 5^n$. If $n = 1$, then $x^2 = 1$. If $n$ has a prime divisor $p$, then $n = pq$, and so $x^2 + 4 = (5^q)^p$. From the solution of the problem

it follows that $5^q = 5$; hence $q = 1$ and $n$ is a prime. We have seen that $n$ must be 3, so $x^2 = 121$.

**2.** *Solve the equation*

$$x^2 + 9 = y^n,$$

*where $n$ is an integer greater than* 1.

*Solution.* For $n = 2$, the only solutions are $(0, 3)$, $(0, -3)$, $(4, 5)$, $(4, -5)$, $(-4, 5)$, and $(-4, -5)$. For $n$ even, $n \geq 4$, the equation is not solvable. For $n$ odd, we may assume without loss of generality that $n$ is a prime $p \geq 3$. The argument is the same as in the previous problem. We will prove that the equation is not solvable in this case.

Clearly, 3 does not divide $x$, for otherwise, 3 would divide $\left(\frac{x}{3}\right)^2 + 1$, a contradiction. We will use again the uniqueness of prime factorization in $\mathbb{Z}[i]$. The equation can be written as $(3 + ix)(3 - ix) = y^p$, and since $\gcd(3 + ix, 3 - ix) = 1$, it follows that $3 + ix = (a + bi)^p$ and $y = a^2 + b^2$, where $a$ and $b$ have different parities. Identifying the real parts, we get

$$3 = a^p - \binom{p}{2} a^{p-2}b^2 + \cdots + (-1)^{\frac{p-1}{2}} \binom{p}{p-1} ab^{p-1}. \qquad (1)$$

From (1) it follows that $3 \equiv a^p \pmod{p}$. Then Fermat's little theorem gives $a^p \equiv a \pmod{p}$; hence we get that $a \mid 3$, so clearly $a = 3$. Therefore, relation (1) becomes

$$1 = 3^{p-1} - \binom{p}{2} 3^{p-3}b^2 + \cdots + (-1)^{\frac{p-1}{2}} \binom{p}{p-1} b^{p-1}. \qquad (2)$$

That is,

$$3^{p-1} - 1 = \binom{p}{2} 3^{p-3}b^2 - \binom{p}{4} 3^{p-5}b^4 + \cdots - (-1)^{\frac{p-1}{2}} \binom{p}{p-1} b^{p-1}. \quad (3)$$

If $p = 4m + 3$, then from (3) it follows that $b$ must be even. But in this case, $3^{p-1} - 1$ is divisible by $2^3$ and not by $2^4$, while $b^2$ is divisible by an even power of 2, a contradiction.

If $p = 4m + 1$, then from (3) we get again that $b$ must be even. Assume that $p = 2^\mu k + 1$, where $\mu \geq 1$ and $k$ is odd.

But $3^{p-1} - 1 = 3^{2^\mu k} - 1 = (-1 + 4)^{2^\mu k} - 1 = 2^{\mu+2}k - \ldots$, which shows that $2^{\mu+2}$ is the greatest power of 2 dividing $3^{p-1} - 1$. Because $b$ is even, $b = 2^\sigma q$, where $\alpha \geq 1$ and $q$ is odd. Then

$$\binom{p}{2} b^2 = \frac{p(p-1)}{2} b^2 = (2^\mu k + 1) 2^{\mu-1} k \cdot 2^{2\alpha} q^2;$$

hence the greatest power of 2 dividing $\binom{p}{2} b^2$ is $2^{\mu-1+2\alpha}$. The parities of the exponents $\mu + 2$ and $\mu - 1 + 2\alpha$ are different, a contradiction.

In all cases, we have shown the insolvability of the equation.

**3.** *Let $p = 4m - 1$ be a prime and let $x$ and $y$ be relatively prime integers such that*

$$x^2 + y^2 = z^{2m}$$

*for some integer $z$. Prove that $p \mid xy$.*

(American Mathematical Monthly)

*Solution.* Because $\gcd(x, y) = 1$, $x$ and $y$ have different parities. Indeed, they cannot both be odd, since in this case $x^2 + y^2 \equiv 2 \pmod 4$, so $x^2 + y^2$ is not a perfect square. Hence $z$ is odd. We will use the uniqueness of prime factorization in $\mathbb{Z}[i]$. The equation is equivalent to $(x + iy)(x - iy) = z^{2m}$. Let $d = \gcd(x + iy, x - iy)$. Then $d \mid (x+iy)+(x-iy) = 2x$ and $d \mid (x+iy)-(x-iy) = 2iy$; thus $d \mid 2x$ and $d \mid 2y$. From $\gcd(x, y) = 1$ it follows that $d \mid 2$. On the other hand, from $(x+iy)(x-iy) = z^{2m}$, we see that $d \mid z^{2m}$. But $z$ is

odd; hence $d$ must be a unit in $\mathbb{Z}[i]$, implying that $x+iy$ and $x-iy$ are relatively prime. From the uniqueness of prime factorization we get

$$x+iy = i^k(a+ib)^{2m},$$

for some integers $a$ and $b$ and some $k \in \{0,1,2,3\}$.

We have

$$\begin{aligned}(a+ib)^{4m} &= (a+ib)^{p+1} = (a+ib)^p(a+ib)\\ &\equiv (a^p+(ib)^p)(a+ib) \pmod p\\ &= (a^p - ib^p)(a+ib) \pmod p,\end{aligned}$$

and by Fermat's little theorem we obtain

$$(a+ib)^{4m} \equiv (a-ib)(a+ib) \pmod p = (a^2+b^2) \pmod p.$$

On the other hand, from $x+iy = i^k(a+ib)^{2m}$, it follows that

$$x^2 - y^2 + 2ixy = (-1)^k(a+ib)^{4m};$$

hence

$$x^2 - y^2 + 2ixy \equiv (-1)^k(a^2+b^2) \pmod p.$$

But $p \mid u+iv$ if and only if $p \mid u$ and $p \mid v$. Thus $p \mid 2xy$, and since $p$ is odd, $p \mid xy$.

## 4.2 The Ring of Integers of $\mathbb{Q}[\sqrt{d}]$

**1.** *Find all pairs $(x,y)$ of positive integers such that*

$$13^x + 3 = y^2.$$

(Mathematical Reflections)

*Solution.* We have

$$(4-\sqrt{3})^x(4+\sqrt{3})^x = 13^x = (y-\sqrt{3})(y+\sqrt{3}).$$

It is easy to see that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain with the norm $N$ given by

$$N(a+b\sqrt{3}) = |a^2-3b^2|.$$

Hence $\mathbb{Z}[\sqrt{3}]$ is a PID and so a UFD.

Suppose there exists a prime $p \in \mathbb{Z}[\sqrt{3}]$ that divides both $y-\sqrt{3}$ and $y+\sqrt{3}$. Then

$$N(p) \mid N(y+\sqrt{3}) = |y^2-3| = 13^x.$$

On the other hand, since $p \mid 2\sqrt{3}$, we have $N(p) \mid N(2\sqrt{3}) = 12$. Then $N(p) \mid (12, 13^x) = 1$, and so $N(p) = 1$, contradiction.

Hence $(y-\sqrt{3}, y+\sqrt{3}) = 1$, and so $y+\sqrt{3}$ is an $x$th power. In particular, since both $4-\sqrt{3}$ and $4+\sqrt{3}$ are primes, then $(4+\sqrt{3})^x = y+\sqrt{3}$, which after comparing coefficients of $\sqrt{3}$ in both sides yields

$$1 = \sum \binom{x}{2k+1} 3^k 4^{x-(2k+1)} = x4^{x-1} + (\text{terms} \geq 1).$$

Therefore $x = 1$.

**2.** *Solve the equation*

$$x^2 + 3 = y^n,$$

*where $n$ is an integer greater* 1.

*Solution.* For $n = 2$ the solutions are $(1,2)$, $(1,-2)$, $(-1,2)$, and $(-1,-2)$. For $n$ even, $n \geq 4$, the equation is not solvable, since no other squares differ by 3. For $n$ odd, $n \geq 3$, we may assume that $n$

is a prime $p$. Indeed, if $n = qk$, where $q$ is an odd prime, we obtain an equation of the same type:

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

We will use the uniqueness of prime factorization in the ring of integers of $\mathbb{Q}[\sqrt{-3}]$. According to Theorem 4.2.3, the integers in $\mathbb{Q}[\sqrt{-3}]$ are $\frac{\alpha+\beta\sqrt{-3}}{2}$, where $\alpha$ and $\beta$ are integers of the same parity. Write the equation as

$$(x + \sqrt{-3})(x - \sqrt{-3}) = y^p,$$

where $y = \frac{\alpha^2+3\beta^2}{4}$.

Clearly, $x$ must be even, for otherwise, $x^2 + 3 \equiv 4 \pmod 8$, while $y^p \equiv 0 \pmod 8$.

The equation $x^2 - x + 1 = y^3$ is equivalent to

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

that is,

$$\frac{(2x-1)+\sqrt{-3}}{2} \cdot \frac{(2x-1)-\sqrt{-3}}{2} = y^3. \tag{2}$$

Let

$$d = \gcd\left(\frac{2x-1+\sqrt{-3}}{2}, \frac{2x-1-\sqrt{-3}}{2}\right).$$

Then

$$d \mid \left(\frac{2x-1+\sqrt{-3}}{2} - \frac{2x-1-\sqrt{-3}}{2}\right) = \sqrt{-3}.$$

Hence $N(d) \mid N(\sqrt{-3})$, that is, $d^2 \mid 3$. It follows that $d = 1$ or $d = \sqrt{-3}$. The second case requires $x \equiv 2 \pmod 3$, which gives $3 \mid y^3$, but $9 \nmid y^3$, a contradiction. Hence the only possibility is $d = 1$, so the integers $\frac{2x-1+\sqrt{-3}}{2}$ and $\frac{2x-1-\sqrt{-3}}{2}$ are relatively prime in $R$.

Using the uniqueness of prime factorization in $R$, we get

$$\frac{2x-1+\sqrt{-3}}{2} = w^k \left(\frac{\alpha+\beta\sqrt{-3}}{2}\right)^3 \tag{3}$$

and

$$\frac{2x-1-\sqrt{-3}}{2} = w^{6-k} \left(\frac{\alpha-\beta\sqrt{-3}}{2}\right)^3,$$

where $w = \frac{-1+\sqrt{-3}}{2}$ and $\frac{\alpha^2+3\beta^2}{4} = y$.

Then $\gcd(x+\sqrt{-3}, x-\sqrt{-3}) = 1$ and

$$x+\sqrt{-3} = w^k \left(\frac{\alpha+\beta\sqrt{-3}}{2}\right)^p, \quad x-\sqrt{-3} = w^{6-k} \left(\frac{\alpha-\beta\sqrt{-3}}{2}\right)^p,$$

where $w = \frac{-1+\sqrt{-3}}{2}$. The first relation can be written as

$$x+\sqrt{-3} = \left(\frac{m+n\sqrt{-3}}{2}\right)^p, \tag{1}$$

for some integers $m$ and $n$ of the same parity.

Indeed, for each $k \in \{0, 1, \ldots, 5\}$, there is a positive integer $s$ such that $w^k = w^{sp}$. The choice of $s$ depends on the residue of $p$ modulo 6. If $p \equiv 1 \pmod 6$, we take $s = k$, while for $p \equiv 5 \pmod 6$ we take $s = 6 - k$.

Taking the conjugate in (1), we obtain

$$x-\sqrt{-3} = \left(\frac{m-n\sqrt{-3}}{2}\right)^p;$$

hence

$$2\sqrt{-3} = \left(\frac{m+n\sqrt{-3}}{2}\right)^p - \left(\frac{m-n\sqrt{-3}}{2}\right)^p.$$

Factoring the expression in the right-hand side as

$$A^p - B^p = (A-B)(A^{p-1} + A^{p-2}B + \cdots + AB^{p-2} + B^{p-1}),$$

we get $2\sqrt{-3} = n\sqrt{-3}\cdot u$, where $u$ is an integer in $\mathbb{Q}[\sqrt{-3}]$. It follows that $2 = n\cdot u$, and so $N(2) = N(n\cdot u) = N(n)\cdot N(u)$, i.e., $4 = n^2 N(u)$. Hence $n \mid 2$.

For $n = \pm 1$, from (1) we obtain

$$\pm 2^p = \binom{p}{1} m^{p-1} - 3\binom{p}{3} m^{p-3} + \cdots + (-3)^{\frac{p-1}{2}}. \tag{2}$$

Looking modulo $p$, from Fermat's little theorem we get

$$\pm 2 \equiv (-3)^{\frac{p-1}{2}} \pmod{p};$$

hence $4 \equiv (-3)^{p-1} \equiv 1 \pmod{p}$, so $p = 3$.

The equation becomes $x^2 + 3 = y^3$. This equation is not solvable for $y \equiv 1 \pmod 4$. Hence $y \equiv 3 \pmod 4$ and $x^2 + 4 = y^3 + 1 = (y+1)(y^2 - y + 1)$, which is again impossible, since $y^2 - y + 1$ is of the form $4m + 3$ and it cannot divide the sum of squares $x^2 + 4$.

For $n = \pm 2$, $m = 2a$ and (1) becomes

$$x + \sqrt{-3} = (a + \sqrt{-3})^p,$$

so

$$1 = \binom{p}{1} a^{p-1} - 3\binom{p}{3} a^{p-3} + 9\binom{p}{5} a^{p-5} - \cdots + (-3)^{\frac{p-1}{2}}. \tag{3}$$

Clearly, $3 \nmid a$, so $a^2 \equiv 1 \pmod 3$. From (3), we get $1 \equiv pa^{p-1} \pmod 3$; hence $p \equiv 1 \pmod 3$. Let $p = 3^u \cdot 2q + 1$, where $3 \nmid q$. Looking at (3) modulo $3^{\mu+2}$, we get

$$1 \equiv pa^{p-1} + \frac{p-1}{2} a^{p-3} \pmod{3^{\mu+2}}. \tag{4}$$

Indeed, $3^{\mu+2} \mid 9\binom{p}{5}$ and

$$\begin{aligned} 3\binom{p}{3} &= \frac{p-1}{2} p(p-2) = \frac{p-1}{2}[(p-1)^2 - 1] \\ &\equiv -\frac{p-1}{2} \pmod{3^{\mu+2}}. \end{aligned}$$

We have

$$a^{p-1} = (a^2)^{\frac{p-1}{2}} = (1+3k)^{3^\mu q} \equiv 1 + 3^{\mu+1}kq \pmod{3^{\mu+2}}.$$

Multiplying (4) by $\frac{p-1}{2} = 3^\mu q$ and looking mod $3^{\mu+2}$, we obtain

$$\frac{p-1}{2}a^{p-1} \equiv 3^\mu q(1+3^{\mu+1}kq) \equiv 3^\mu q \pmod{3^{\mu+2}}. \tag{5}$$

On the other hand,

$$a^2(pa^{p-1}-1) \equiv -\frac{p-1}{2}a^{p-1} \pmod{3^{\mu+2}}$$

and

$$\begin{aligned} a^2(pa^{p-1}-1) &= (1+3k)[p(1+3k)^{\frac{p-1}{2}} - 1] = (1+3k)[p(1+3k)^{3^\mu q} - 1] \\ &\equiv (1+3k)p + (1+3k)p \cdot 3^{\mu+1}kq - (1+3k) \pmod{3^{\mu+2}} \\ &\equiv (1+3k)(p-1) + pkq \cdot 3^{\mu+1} \pmod{3^{\mu+2}} \\ &\equiv 3^\mu \cdot 2q + 3^{\mu+1} \cdot 2kq + (3^\mu \cdot 2q + 1)kq3^{\mu+1} \pmod{3^{\mu+2}} \\ &\equiv 3^\mu \cdot 2q + 3^{\mu+1}(2kq + kq) \pmod{3^{\mu+2}} \\ &\equiv 3^\mu \cdot 2q \pmod{3^{\mu+2}}. \end{aligned}$$

Using (5) we obtain

$$-3^\mu q \equiv 3^\mu \cdot 2q \pmod{3^{\mu+2}};$$

hence $3^{\mu+2} \mid 3^{\mu+1}q$, i.e., $3 \mid q$, a contradiction.

In conclusion, the equation is not solvable for $n \geq 3$.

**3.** *Solve the equation*

$$x^2 + 11 = 3^n,$$

*where $n$ is an integer greater than* 1.

*Solution.* Looking modulo 13 we have the following table:

| $x$ | $0$ | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ | $\pm5$ | $\pm6$ |
|---|---|---|---|---|---|---|---|
| $x^2$ | $0$ | $1$ | $4$ | $9$ | $3$ | $12$ | $10$ |
| $x^2+11$ | $11$ | $12$ | $2$ | $7$ | $1$ | $10$ | $8$ |

while $3^n \equiv 1, 3$, or $9 \pmod{13}$, as $n \equiv 0, 1$, or $2 \pmod 3$, respectively. It follows that $n = 3k$, for some positive integer $k$. Let $y = 3^k$ and the equation becomes $x^2 + 11 = y^3$. It is clear that $x$ is even. Using the uniqueness of prime factorization in the ring of integers of $\mathbb{Q}[\sqrt{-11}]$, we get

$$x \pm \sqrt{-11} = \left(\frac{a + b\sqrt{-11}}{2}\right)^3,$$

where $a$ and $b$ are integers of the same parity.

Identifying the imaginary parts, we obtain $\pm 2^3 = 3a^2b - 11b^3$; hence $b \mid 2^3$.

A short case analysis shows that the only solutions are $b = \pm 1$ and $a^2 = 1$. Because $y = \frac{a^2+11b^2}{4}$, it follows that $y = 3$, i.e., $n = 3$ and $x = \pm 4$. The solutions $(x, n)$ are $(4, 3)$ and $(-4, 3)$.

**4.** *Solve the equation*

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

*Solution.* The equation is equivalent to

$$\frac{(2x+1) + \sqrt{-7}}{2} \cdot \frac{(2x+1) - \sqrt{-7}}{2} = y^3.$$

But

$$\gcd\left(\frac{2x + 1 + \sqrt{-7}}{2}, \frac{2x + 1 - \sqrt{-7}}{2}\right) = 1.$$

Indeed, if $d$ is this gcd, then

$$d \mid \frac{2x+1+\sqrt{-7}}{2} - \frac{2x+1-\sqrt{-7}}{2} = \sqrt{-7};$$

hence $N(d) \mid N(\sqrt{-7})$, that is, $d^2 \mid 7$. Using the uniqueness of the prime factorization in the ring of integers of $\mathbb{Q}[\sqrt{-7}]$, we obtain

$$\frac{2x+1+\sqrt{-7}}{2} = \left(\frac{a+b\sqrt{-7}}{2}\right)^3,$$

where $a$ and $b$ are integers of the same parity and $\frac{a^2+7b^2}{4} = y$.

It follows that $3a^2b - 7b^3 = 4$; hence $b \mid 4$.

Analyzing all possibilities ($b = \pm 1, \pm 2, \pm 4$), we get $b = \pm 1$ and $a^2 = 1$, yielding the solution $y = 2$, and so $x = 2$ or $x = -3$. The solutions are $(2, 2)$ and $(-3, 2)$.

**5.** *Let $a$ and $b$ be positive integers such that $b = x^2 - dy^2$ for some integers $x, y, d$ with $d = a^2 - 1$. Prove that if $b < 2(a+1)$, then $b$ is a perfect square.*

*Solution.* Everything is clear for $a = 1$. For $a \geq 2$, the fundamental solution to Pell's equation $x^2 - (a^2-1)y^2 = 1$ is $z_1 = a + \sqrt{d}$. From the hypothesis, the equation $N(z) = b$ has solution $(x, y)$; hence, according to Theorem 4.2.7, it also has a solution $z' = x' + y'\sqrt{d}$ with

$$\begin{aligned} |x'| &\leq \frac{z_1+1}{2\sqrt{z_1}}\sqrt{b} = \frac{a+1+\sqrt{d}}{2\sqrt{a+\sqrt{d}}}\sqrt{b} \\ &= \sqrt{\frac{(a+1+\sqrt{d})^2}{4(a+\sqrt{d})}b} = \sqrt{\frac{(a+1)b}{2}} < a+1; \end{aligned}$$

hence $x' \leq a$.

On the other hand,

$$y' = \sqrt{\frac{(x')^2 - b}{d}} \leq \sqrt{\frac{a^2-b}{d}} = \sqrt{\frac{a^2-b}{a^2-1}} < 1.$$

It follows that $y' = 0$ and $b = (x')^2$.

## 4.3 Quadratic Reciprocity and Diophantine Equations

**1.** *For a prime $p$, the equation $x^2 - 3y^2 = p$ has solutions in integers if and only if $p \equiv 1 \pmod{12}$.*

*Solution.* From the previous problem, it suffices to take $p \geq 5$. A necessary condition for solvability is $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$. The second relation means that $p \equiv 1 \pmod 3$. Moreover, since $3 \equiv -1 \pmod 4$, quadratic reciprocity tells us that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if and only if $p \equiv 1 \pmod 4$. Thus $p \equiv 1 \pmod{12}$.

Because 3 is a quadratic residue modulo $p$, we have $3 + np = x^2$ for some integers $n$ and $p$. This is equivalent to $np = (x + \sqrt{3})(x - \sqrt{3})$. It follows that $p \mid x + \sqrt{3}$ or $p \mid x - \sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$. But this is clearly impossible; hence $p$ factors nontrivially in $\mathbb{Z}[\sqrt{3}]$, the nontriviality meaning that neither factor is a unit, so neither has norm $\pm 1$. Then

$$p = (s + t\sqrt{3})(u + v\sqrt{3}),$$

and taking norms yields $p^2 = (s^2 - 3t^2)(u^2 - 3v^2)$. This implies $s^2 - 3t^2 = u^2 - 3v^2 = p$ or $s^2 - 3t^2 = u^2 - 3v^2 = -p$. The latter is not possible, since looking mod 3, we get $-p \equiv u^2 \pmod p$. But quadratic residues tell us that $\left(\frac{-p}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{p}{3}\right) = (-1) \cdot 1$, because $p \equiv 1 \pmod 3$, a contradiction.

**2.** *Let $p$ be a prime of the form $4k + 3$. Prove that exactly one of the equations $x^2 - py^2 = \pm 2$ is solvable.*

*Solution.* Suppose the equations

$$x^2 - py^2 = 2 \quad \text{and} \quad u^2 - pv^2 = -2$$

are both solvable. Then $p \mid x^2-2$ and $p \mid u^2+2$, implying $p \mid x^2+u^2$. From Theorem 4.4.2 it follows that $p \mid x$ and $p \mid u$, implying $p \mid 2$, a contradiction. Hence at most one equation is solvable. Let $(x_1, y_1)$ be the fundamental solution to Pell's equation $u^2 - pv^2 = 1$. If $x_1 - 1$ and $x_1 + 1$ are not relatively prime, then from $(x_1-1)(x_1+1) = py_1^2$ we get $x_1 \pm 1 = ax^2$ and $x_1 \mp 1 = pay^2$. Hence $a(x^2 - py^2) = 2$, implying $a = 2$. It follows that $x_1 \pm 1 = 2x^2$ and $x_1 \mp 1 = 2py^2$, which yields $x^2 - py^2 = \pm 1$. The situation $x^2 - py^2 = 1$ contradicts the minimality of $(x_1, y_1)$, while $x^2 = py^2 - 1$ is in contradiction to the result in Theorem 3.4.2.

Hence $x_1 - 1$ and $x_1 + 1$ are relatively prime, so $x_1 \pm 1 = x^2$ and $x_1 \mp 1 = py^2$ for some positive integers $x$ and $y$. It follows that $x^2 - py^2 = \pm 2$.

**3.** *Let $p$ be a prime of the form $8k + 7$. Prove that the equation $x^2 - py^2 = 2$ is solvable.*

*First Solution.* Let $(u, v)$ be the fundamental solution to Pell's equation $x^2 - py^2 = 1$. We will prove that $u$ is even and $v$ is odd. Indeed, if $u$ is odd, then $v$ is even, and from

$$\frac{u-1}{2} \cdot \frac{u+1}{2} = p\left(\frac{v}{2}\right)^2 \text{ and } \gcd\left(\frac{u-1}{2}, \frac{u+1}{2}\right) = 1$$

it follows that

$$\frac{u-1}{2} = p\alpha^2 \text{ and } \frac{u+1}{2} = \beta^2 \text{ or } \frac{u-1}{2} = \alpha^2 \text{ and } \frac{u+1}{2} = p\beta^2$$

for some positive integers $\alpha$ and $\beta$. In the first case we get $\beta^2 - p\alpha^2 = 1$, contradicting the minimality of $(u, v)$, while in the second we obtain $\alpha^2 - p\beta^2 = -1$, contradicting the result in Theorem 3.4.2.

Hence $u$ is even and $v$ is odd, so $\gcd(u-1, u+1) = 1$. From $(u-1)(u+1) = pv^2$, we get $u-1 = a^2$ and $u+1 = pb^2$ or $u-1 = pa^2$ and $u+1 = b^2$, for some integers $a$ and $b$. In the first case, $pb^2 - a^2 = 2$; hence $a^2 \equiv -2 \pmod{p}$. But

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

since $p \equiv 7 \pmod{8}$, a contradiction. In the second case, $b^2 - pa^2 = 2$, and we are done.

*Second Solution.* It is clear that $p$ is of the form $4m+3$. Using the result in Problem 2, it suffices to show that the equation $x^2 - py^2 = -2$ is not solvable. If this equation were solvable and $(x, y)$ were a solution, then we would have $x^2 \equiv -2 \pmod{p}$. But

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

since $p \equiv 7 \pmod{8}$, a contradiction.

**Remark.** In a similar way we can prove that if $p$ is a prime of the form $8k+3$, then the equation $x^2 - py = -2$ is solvable.

## 4.4 Divisors of Certain Forms

**1.** *Let $p$ be a prime of the form $4k+3$. Prove that the system of equations*

$$\begin{cases} (p-1)x^2 + y^2 = u^2, \\ x^2 + (p-1)y^2 = v^2, \end{cases}$$

*is not solvable in nonzero integers.*

*Solution.* Without loss of generality we may assume that

$$\gcd(x, y) = 1.$$

We have $u^2+v^2 = p(x^2+y^2)$; hence $p \mid u^2+v^2$. By Theorem 4.4.2 it follows that $p \mid u$ and $p \mid v$. Then one gets $p \mid x^2+y^2$, contradicting Theorem 4.4.2.

**2.** *Prove that the equation* $x^2 + y^2 = z^n + 2^n$ *is not solvable if* $\gcd(x, y) = 1$ *and* $n$ *is an odd integer greater than* 1.

*Solution.* Because $\gcd(x, y) = 1$, it follows that $z$ is odd, for otherwise, $2^n \mid x^2 + y^2$, in contradiction to $x^2 + y^2 \equiv 2 \pmod 8$.

The right-hand side of the equation has a prime factor of the form $4k + 3$. Indeed, if $z = 4m - 1$, then $z^n + 2^n$ is of the same form. If $z = 4m + 1$, then $z + 2 = 4m + 3$ and it divides $z^n + 2^n$. In both cases, $x^2 + y^2$ has a prime factor of the form $4k+3$, a contradiction.

(Ion Cucurezeanu)

**3.** *Prove that for any integer* $n$ *greater than 1, the equation*

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

*is not solvable.*

(Ion Cucurezeanu)

*Solution.* Clearly, $x$ is odd, for otherwise, $y$ would also be even and so we would have $0 \equiv 2 \pmod 4$, a contradiction.

If $n$ is even, then

$$(y - x^{\frac{n}{2}})(y + x^{\frac{n}{2}}) = 2^n - 2.$$

Because $x$ and $y$ are both odd, the left-hand side is congruent to 0 (mod 4), while the right-hand side is congruent to 2 (mod 4). Hence $n$ is odd.

If $x = 4k+1$, then working modulo 4 we get another contradiction. If $x = 4k - 1$, then $x = 8m - 1$ or $x = 8m + 3$. In the first case, working modulo 8 we obtain again a contradiction. In the second case, $x + 2 = 8k + 5$ has a prime divisor of the form $8m - 3$ or $8m - 1$, contradicting the result in Remark 2.

**Remark.** A short way to get a contradiction is the following. After we have proved that $x$ and $y$ are both odd, we reduce the equation mod 4 and obtain $1 \equiv 3 \pmod 4$, which is not possible.

# References


[Ac] Acu, D., *Aritmetică şi teoria numerelor* (Romanian), Universitatea "Lucian Blaga" din Sibiu, Colecţia Facultăţii de Ştiinţe, Seria Matematică, Sibiu, 1999.

[AndreAndri1] Andreescu, T., Andrica, D., *360 Problems for Mathematical Contests*, GIL Publishing House, 2003.

[AndreAndri2] Andreescu, T., Andrica, D., *Asupra rezolvării în numere naturale a ecuaţiei* $ax^2 - by^2 = 1$ (Romanian), G.M. **4**(1980), 146–148.

[AndreAndri3] Andreescu, T., Andrica, D., *Existenţa unei soluţii de bază pentru ecuaţia* $ax^2 - by^2 = 1$ (Romanian), G.M. **2**(1981), 52–54.

[AndreAndri4] Andreescu, T., Andrica, D., *Condiţii în care numerele* $an + b$ *şi* $cn + d$ *sunt simultan pătrate perfecte*, (Romanian) G.M. **7**(1983), 265–266.

[AndreAndri5] Andreescu, T., Andrica, D., *Asupra unor clase de ecuaţii de forma* $Ax^2 - By^2 = C$ *care nu admit soluţie de bază* (Romanian), G.M. **12**(1983), 446–447.

[AndreAndri6] Andreescu, T., Andrica, D., *Ecuaţia lui Pell. Aplicaţii* (Romanian), Caiete metodico-ştiinţifice, Matematică, Universitatea din Timişoara, **15**, 1984.

[AndreAndri7] Andreescu, T., Andrica, D., *Ecuaţia lui Pell şi aplicaţii* (Romanian), în "Teme şi probleme pentru pregătirea olimpiadelor de matematică" (T. Albu, col.), pp.33–42, Piatra Neamţ, 1984.

[AndreAndri8] Andreescu, T., Andrica, D., *Number Theory. Structures, Examples, and Problems*, Birkhäuser, Boston–Basel–Berlin, 2009.

[AndreAndri9] Andreescu, T., Andrica, D., *An Introduction to Diophantine Equations*, GIL Publishing House, 2002.

[AndreAndri10] Andreescu, T., Andrica, D., *On a Diophantine Equation and Its Ramifications*, The College Mathematics Journal, 1(2004).

[AndreAndriFe] Andreescu, T., Andrica, D., Feng, Z., *104 Number Theory Problems: From the Training of the USA IMO Team*, Birkhäuser, Boston, 2007.

[AndreFe1] Andreescu, T., Feng, Z., *101 Problems in Algebra: From the Training of the USA IMO Team*, AMT Publishing, 2001.

[AndreFe2] Andreescu, T., Feng, Z., *Mathematical Olympiads 1999–2000, Problems and Solutions From Around the World*, Mathematical Association of America, 2001.

[AndreGe1] Andreescu, T., Gelca, R., *Putnam and Beyond*, Springer, 2007.

[AndreGe2] Andreescu, T., Gelca, R., *Mathematical Olympiad Challenges*, Birkhäuser, Boston–Basel–Berlin, 2009, Second Edition.

[AndreKe] Andreescu, T., Kedlaya, K., *Mathematical Contests 1995–1996*, Mathematical Association of America, 1997.

[Andri] Andrica, D., *Asupra unei ecuaţii diofantiene* (Romanian), Arhimede, Nr.3-4(2001), 1–2.

[AndriTu1] Andrica, D., Tudor, Gh. M., *Parametric solutions for some Diophantine equations*, General Mathematics Vol. 12, No. 1(2004), 23–34.

[AndriTu2] Andrica, D., Tudor, Gh. M., *Some Diophantine Equations of the Form* $ax^2+pxy+by^2=z^{k^n}$, General Mathematics Vol. 13, No. 2(2005), 121–130.

[Ba] Barbeau, E.J., *Pell's Equation*, Springer, 2003.

[BoFu] Boju, V., Funar, L., *The Math Problems Notebook*, Birkhäuser, Boston–Basel–Berlin, 2007.

[BuBoPi] Buşneag, D., Boboc, F., Piciu, D., *Aritmetică şi teoria numerelor* (Romanian), Editura Universitaria, Craiova, 1999.

[Car] Carmichael, R.D., *The Theory of Numbers and Diophantine Analysis*, Dover Publications, Inc., New York, 1959.

[Ch] Chrystal, G., *Algebra. An Elementary Text-Book*, Part II, Dover, New York, 1961.

[Co] Cohen, E., *Théorie des Nombres*, Tome II, Paris, 1924.

[Co] Cohen, H., *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[Cu] Cucurezeanu, I., *Ecuaţii în Numere ˆIm ntregi* (Romanian), Aramis, Bucureşti, 2006.

[Dic] Dickson, L.E., *Introduction to the Theory of Numbers*, Dover Publications, Inc., New York, 1957.

[Dö] Dörrie, H., *100 Great Problems of Elementary Mathematics. Their History and Solution*, New York, Dover Publications, Inc., 1965.

[Ghe] Ghelfond, A.O., *Rezolvarea Ecuaţiilor ˆIm n Numere ˆIm ntregi* (Romanian), Editura Tehnică, Bucureşti, 1954.

[JaWi] Jacobson, M.J., Jr., Williams, *Solving the Pell Equation*, Canadian Mathematical Society, Springer, 2009.

[HaWr] Hardy, G.H., Wright, E.M., *Theory of Numbers*, 3rd edition, 1954.

[Hu] Hurwitz, A., *Lectures on Number Theory*, Springer-Verlag, 1986.

[Len] Lenstra, H.W., *Solving the Pell equation*, Notices of the American Mathematical Society, **29**(2002), 182–192.

[Lev] Leveque, W.J., *Topics in Number Theory*, Volume 1, Addison–Wesley, New York, 1956.

[Ma] Mattews, K., *Number Theory*, Chelsea, New York, 1961.

[Mol1] Mollin, R.A., *Quadratics*, CRC Press, Boca Raton, 1996.

[Mol2] Mollin, R.A., *Fundamental Number Theory and Applications*, CRC Press, New York, 1998.

[Mor] Mordell, L.J., *Diophantine Equations*, Academic Press, London and New York, 1969.

[Na] Nagell, I., *Introduction to Number Theory*, John Wiley & Sons, Inc., New York, Stockholm, 1951.

[PaGi1] Panaitopol, L., Gica, A., *Probleme Celebre de Teoria Numerelor* (Romanian), Editura Universităţii din Bucureşti, 1998.

[PaGi2] Panaitopol, L., Gica, A., *O Introducere în Aritmetică şi Teoria Numerelor* (Romanian), Editura Universităţii din Bucureşti, 2001.

[Si1] Sierpiński, W., *Elementary Theory of Numbers*, Polski Academic Nauk, Warsaw, 1964.

[Sie2] Sierpiński, W., *Ce Ştim şi ce nu Ştim despre Numerele Prime* (Romanian), Editura Ştiinţifică, Bucureşti, 1966.

[Sie3] Sierpiński, W., *250 Problems in Elementary Number Theory*, American Elsevier Publishing Company, Inc., New York, PWN, Warszawa, 1970.

[Tat] Tattersall, J.J., *Elementary Number Theory in Nine Chapters*, Cambridge University Press, 1999.

# Glossary

*Arithmetic function*

A function defined on the positive integers that is complex-valued.

*Arithmetic–Geometric Means Inequality*

If $n$ is a positive integer and $a_1, a_2, \ldots, a_n$ are nonnegative real numbers, then

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geq (a_1 a_2 \cdots a_n)^{1/n},$$

with equality if and only if $a_1 = a_2 = \cdots = a_n$. This inequality is a special case of the **power mean inequality**.

*Associated elements*

Two elements $a$ and $b$ of a ring $R$ such that $a = ub$ for some unit $u \in R$.

*Base-b representation*

Let $b$ be an integer greater than 1. For any integer $n \geq 1$ there is a unique system $(k, a_0, a_1, \ldots, a_k)$ of integers such that $0 \leq a_i < b$, $i = 0, 1, \ldots, k$, $a_k \neq 0$ and,

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

*Beatty's theorem*

Let $\alpha$ and $\beta$ be two positive irrational real numbers such that

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1.$$

The sets $\{\lfloor \alpha \rfloor, \lfloor 2\alpha \rfloor, \lfloor 3\alpha \rfloor, \ldots\}$, $\{\lfloor \beta \rfloor, \lfloor 2\beta \rfloor, \lfloor 3\beta \rfloor, \ldots\}$ form a partition of the set of positive integers.

*Bernoulli's inequality*

For $x > -1$ and $a > 1$,

$$(1 + x)^a \geq 1 + ax,$$

with equality when $x = 0$.

*Bezout's identity*

For positive integers $m$ and $n$, there exist integers $x$ and $y$ such that $mx + ny = gcd(m, n)$.

*Binomial coefficient*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

the coefficient of $x^k$ in the expansion of $(x + 1)^n$.

*Binomial theorem*
The expansion

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

*Canonical factorization*

Any integer $n > 1$ can be written uniquely in the form

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ and } p_1 < p_2 < \cdots < p_k,$$

where $p_1, \ldots, p_k$ are distinct primes and $\alpha_1, \ldots, \alpha_k$ are positive integers.

*Carmichael's integers*

The composite integers $n$ satisfying $a^n \equiv a \pmod{n}$ for any integer $a$.

*Ceiling function*

The least integer that is greater than or equal to $x$ is called the ceiling of $x$ and is denoted by $\lceil x \rceil$.

*Commutative ring*

A set $R$ equipped with two commutative binary operations, addition and multiplication, such that $(R, +)$ is an abelian group, $0_R \neq 1_R$, and the distributive law holds ($(a+b)c = ac + bc$, for all $a, b, c \in R$).

*Complete set of residue classes modulo n*

A set $S$ of integers such that for each $0 \leq i < n$ there is a unique element $s \in S$ with $i \equiv s \pmod{n}$.

*Congruence relation*

Let $a, b$, and $m$ be integers. We say that $a$ and $b$ are congruent modulo $m$ if $m \mid a - b$. We denote this by $a \equiv b \pmod{m}$. The relation "$\equiv$" on the set $\mathbb{Z}$ of integers is called the congruence relation.

*Division algorithm*

For any positive integers $a$ and $b$ there exists a unique pair $(q, r)$ of nonnegative integers such that $b = aq + r$ and $r < a$.

*Euclidean algorithm*

Repeated application of the division algorithm:

$$\begin{aligned} m &= nq_1 + r_1,\ 1 \le r_1 < n, \\ n &= r_1 q_2 + r_2,\ 1 \le r_2 < r_1, \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k,\ 1 \le r_k < r_{k-1}, \\ r_{k-1} &= r_k q_{k+1} + r_{k+1},\ r_{k+1} = 0. \end{aligned}$$

This chain of equalities is finite because $n > r_1 > r_2 > \cdots > r_k > 0$.

*Euclidean domain*

A ring $R$ with the property that there exists a function $\lambda : R \setminus \{0\} \to \mathbb{N}^0$ such that for any two $a, b \in R$, $b \neq 0$, one can find some $c, d \in R$ satisfying $a = cb + d$, where either $d = 0$ or $\lambda(d) < \lambda(b)$.

*Euler's theorem*

Let $a$ and $m$ be relatively prime positive integers. Then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

*Euler's totient function*

The function $\varphi$ defined by $\varphi(m) =$ the number of all positive integers $n$ less than or equal to $m$ that are relatively prime to $m$.

*Fermat's little theorem*

Let $a$ be any integer and let $p$ be a prime. Then

$$a^p \equiv a \pmod{p}.$$

*Fibonacci sequence*

The sequence defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for every positive integer $n$.

*Field*

A set $k$ equipped with two commutative binary operations, addition and multiplication, such that:

1. $(k, +)$ is an abelian group under addition;
2. every nonzero element of $k$ has a multiplicative inverse, and $(k^*, \cdot)$ is an abelian group under multiplication, where $k^* = k \setminus \{0_k\}$;
3. $0_k \neq 1_k$;
4. the distributive law holds: $(a + b)c = ac + bc$ for all $a, b, c \in k$.

*Floor function*

For a real number $x$ there is a unique integer $n$ such that $n \leq x < n + 1$. We say that $n$ is the greatest integer less than or equal to $x$ or the floor of $x$ and we write $n = \lfloor x \rfloor$.

*Ideal*

A subset of a ring $R$ closed under addition and subtraction and under multiplication by elements of $R$.

*Integral domain*

A commutative ring without zero-divisors.

*Irreducible element*

An element $p$ of a ring $R$ such that $a \mid p$ implies that $a$ is a unit or $a$ is associated with $p$.

*Gaussian integer*

A complex number whose real part and imaginary part are both integers.

*Legendre symbol*

Let $p$ be an odd prime and let $a$ be a positive integer not divisible by $p$. The Legendre symbol of $a$ with respect to $p$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

*Linear Diophantine equation*

An equation of the form

$$a_1x_1 + \cdots + a_nx_n = b,$$

where $a_1, a_2, \ldots, a_n, b$ are fixed integers.

*Linear recurrence of order k*

A sequence $x_0, x_1, \ldots, x_n, \ldots$ of complex numbers defined by

$$x_n = a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_k x_{n-k}, \quad n \geq k,$$

where $a_1, a_2, \ldots, a_k$ are given complex numbers and $x_0 = \alpha_0$, $x_1 = \alpha_1, \ldots, x_{k-1} = \alpha_{k-1}$ are also given.

*Lucas sequence*

The sequence defined by $L_0 = 2$, $L_1 = 1$, $L_{n+1} = L_n + L_{n-1}$ for every positive integer $n$.

*Number of divisors*

For a positive integer $n$ denote by $\tau(n)$ the number of its divisors. It is clear that

$$\tau(n) = \sum_{d|n} 1.$$

*Order modulo m*

We say that $a$ has order $d$ modulo $m$, denoted by $o_m(a) = d$, if $d$ is the smallest positive integer such that $a^d \equiv 1 \pmod{m}$. We have $o_n(1) = 1$.

*Pell's equation*

The quadratic equation $u^2 - Dv^2 = 1$, where $D$ is a positive integer that is not a perfect square.

*Principal ideal*

An ideal of a ring $R$ generated by one element.

*Principal ideal domain (PID)*

A ring $R$ with the property that every ideal in it is principal.

*Prime element*

A nonunit element $p$ of a ring $R$, $p \neq 0$, such that $p \mid ab$ implies $p \mid a$ or $p \mid b$.

*Pythagorean equation*

The Diophantine equation $x^2 + y^2 = z^2$.

*Pythagorean triple*

A triple of the form $(a, b, c)$ where $a^2 + b^2 = c^2$. All Pythagorean triples are $(m^2 - n^2, 2mn, m^2 + n^2)$, where $m$ and $n$ are positive integers such that $m > n$ and $m + n$ is odd.

*Quadratic residue mod m*

Let $a$ and $m$ be positive integers such that $\gcd(a, m) = 1$. We say that $a$ is a quadratic residue mod $m$ if the congruence $x^2 \equiv a \pmod{m}$ has a solution.

*Quadratic reciprocity law of Gauss*

If $p$ and $q$ are distinct odd primes, then

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

*Unit*

An element of a ring $R$ with a multiplicative inverse.

*Wilson's theorem*

For any prime $p$, $(p-1)! \equiv -1 \pmod{p}$. So $n$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

*Zero-divisor*

A nonzero element $r$ of a ring $R$ such that $rs = 0$ for some nonzero $s \in R$.

# Index


5th USA Math Olympiad, 57, 242

8th USA Math Olympiad, 34, 220

16th USA Math Olympiad, 12, 196

18th IMO, 76, 271

20th IMO Shortlist, 58, 251

21st IMO Shortlist, 61

22nd IMO, 50

23rd IMO, 31

24th IMO, 75, 266

29th IMO, 19, 211

33rd IMO, 12, 197

37th IMO, 35, 225

40th IMO Shortlist, 140, 300

42nd IMO Shortlist, 135, 295

42nd IMO USA Team Selection Test, 58, 249

AM–GM inequality, 204

American Math Monthly, 138, 140, 299

Andrew Wiles, 110

APMO, 64, 253, 260

arithmetic progression, 99, 115

arithmetic sequence, 284

Asian Pacific Mathematical Olympiad, 65

Australian Math Olympiad, 18, 204

Balkan Math Olympiad, 30
Baudhayana, 118
Berkeley Math. Circle, 120
Beyer, 72
Bhaskara, 118
Brauer, 72
Bulgarian Math Olympiad, 34, 37, 64, 65, 223, 255, 261, 274

canonical form, 120
Cartesian plane, 120
College Mathematics Journal, 57, 143, 247
conic, 120
cuboid, 81

Diophantine quadratic equation, 119
Diophantus, 118
Dirichlet, 110
discriminant of the equation, 120
Dorin Andrica, 9, 18, 23, 27, 38, 45, 115, 134, 140, 204, 214, 230, 281, 289, 298

Eötvös Competition, 75, 269
eigenvalues, 124
ellipse, 120
Erdős, 72
Euler, 102, 110, 111, 119

Fermat, 109, 111, 119
Fermat's equation, 109
Fermat's last theorem, 109
Fermat's little theorem, 50, 240
Fermat's method of infinite descent (FMID), 48
Fibonacci, 53, 249
Fibonacci numbers, 51, 244, 251
FMID Variant 1, 48, 239–241, 244
FMID Variant 2, 49, 249
Frobenius coin problem, 71, 267
fundamental solution, 121, 138, 143

g-pair, 250
G.M. Bucharest, 34, 221
general equation of the conic, 120
general Pell's equation, 117
general solution, 136, 139, 141
generating function, 73
Gerd Faltings, 110
German Math Olympiad, 30
Graham, 72
Greenberg, 72

homogeneous polynomial, 117
Hungarian Math Olympiad, 15, 33, 219
hyperbola, 120

Indian Math Olympiad, 6, 11, 193
Ion Cucuruzeanu, 115
irreducible polynomial, 117
Italian Math Olympiad, 64, 65, 256, 259

John Pell, 118

KöMaL, 11, 194
Korean Math Olympiad, 56, 239
Kummer, 110
Kürschák Competition, 56
Kürschák Math Competition, 239
Kvant, 145, 303

Lagrange, 119, 121
Lagrange identity, 213
Lamé, 110
Legendre symbol, 102
linear Diophantine equation, 67
Liouville, 110
Lucas sequence, 53, 249

Markov's equation, 245
mathematical induction, 36
Mathematics Magazine, 58, 247
matrix form, 124
minimal solution, 24
MOSP, 244

negative Pell's equation, 141, 144, 302
negative Pythagorean equation, 82
Noam Elkies, 111

order linear recurrences, 53

parabola, 120
Pell's equation, 118, 122, 124, 126, 128, 289, 300
Pell's resolvent, 136, 298, 302
Pell's sequence, 303
Polish Math Olympiad, 7, 18, 205
primitive Pythagorean triangles, 88, 276
primitive Pythagorean triple, 112, 296
primitive solution, 77
Putnam Math Competition, 49, 126
Pythagorean equation, 76, 90, 93
Pythagorean theorem, 198
Pythagorean triple, 78

quadratic residue, 220
quadratic residue modulo m, 102

rectangular parallelepiped, 65, 261
Roger Frye, 111
Romanian Math Olympiad, 12, 14, 17, 58, 65, 75, 196, 203, 237, 248, 262, 270
Russian Math Olympiad, 11, 18, 29, 65, 194, 205, 258

second order linear recurrence, 56
Selmer, 72
Sophie Germain, 110
Sylvester, 71

Thue, 117
Titu Andreescu, 4, 9, 12, 14, 19, 27, 28, 34, 45–47, 59, 115, 116, 144, 199, 208, 215, 217, 219, 229, 235, 237, 284, 286, 287, 301
Tournament of Towns, 20, 246
triangular number, 46, 126, 231
Turkish Math Olympiad, 115, 280

UK Math Olympiad, 16, 27, 64, 213, 254
USA Proposal for the 38th IMO, 62

Vietnamese Math Olympiad,
52

Wallis, 118
William Brouncker, 119
Wilson's theorem, 253