TITU ANDREESCU DORIN ANDRICA

AN INTRODUCTION TO DIOPHANTINE EQUATIONS

GIL PUBLISHING HOUSE

To the memory of Emma Andreescu

AN INTRODUCTION TO DIOPHANTINE EQUATIONS

Authors: Titu Andreescu, Dorin Andrica

ISBN 973-9238-88-2

National Library of Romania CIP Description
ANDREESCU, TITU
An Introduction to Diophantine Equations/ Titu Andreescu, Dorin Andrica. – Zalau: GIL, 2002
p. ; cm.
Bibliogr.
ISBN 973-9238-88-2

I. Andrica, Dorin

511.5

GIL Publishing House
P.O. Box 44, Post Office 3, 4700, Zalau, Romania,
tel. (+40) 60/616314
fax.: (+40) 60/616414
email: gil773@xnet.ro
www.gil.ro

Lucrarea executată
la Imprimeria „ARDEALUL" Cluj
B-dul 21 Decembrie nr. 146 Cluj-Napoca
Tel.: 413871; Fax: 413883
Comanda nr. 20032

Motto:

"Nothing is as easy as it looks"

(Murphy's 2^{nd} law)

TITU ANDREESCU DORIN ANDRICA

AN INTRODUCTION
TO

DIOPHANTINE EQUATIONS

GIL Publishing House

Contents

Preface

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

Diophantus did his work in the great city of Alexandria. At this time Alexandria was the center of mathematical learning. During the time span from 250 BC to 350 AD, Alexandria was know to be in the "Silver Age" or also known as the Later Alexandrian Age. This was a time when mathematicians were discovering many ideas that lead to our concept of today's mathematics. This time was considered "Silver" because it came after what was known as the "Golden Age". The "Golden Age" was a time of great development in the field of mathematics. This "Golden Age" is considered to be around the time of Euclid. The quality that came out of this time period inspired much of the mathematics, which we use today.

While it is known that Diophantus lived in the "Silver Age", it is remarkably hard to pinpoint the exact years in which he lived. While many references to the work of Diophantus have been made, Diophantus himself, made very few references towards other mathematicians' work, thus making the process of pinpointing his dates harder.

Diophantus did quote the definition of a polygonal number from the work of Hypsicles. Hypsicles worked before 150 BC, so we can determine that Diophantus lives after this date. Looking in the other direction, Theon, a mathematician also from Alexandria, quoted the work of Diophantus in 350 AD. The fact that most historians believe is that Diophantus did most of his work around 250 AD. The greatest amount of information that is available about Diophantus's life comes from the possibly fictitious collection of riddles written by Metrodorus in approximately 500 AD. The riddle is as follows:

"*...his boyhood lasted* $1/6^{th}$ *of his life; he married after* $1/7^{th}$ *more; his beard grew after* $1/12^{th}$ *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.*"

While not much more is known about the person Diophantus, much has been on his work, *Arithmetica*. Diophantus used abbreviations for powers of numbers and for relationships and operations. This clearly defines *Arithmetica* to be a work from the syncopated or second stage, in the levels of algebra development. Before the time of Diophantus, abbreviations for powers of numbers or for relationships and operations were not used. By using these abbreviations, Diophantus set his work above the standard quality of work that was coming out of Alexandria at the time.

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

While there are 150 problems that are written by Diophantus, ther were, at one point it history, more books to *Arithmetica.* There are 6 books from which these 150 problems originate. It is believed that there were originally 13 books in *Arithmetica.* The other 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 will 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, (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. In case of solvability is the number of its solutions finite or infinite?

Problem 3. In case of solvability, determine all of its solutions.

Diophantus' work on equations of type (1) was continued by Chinese mathematicians (3^{rd} century), Arabs (8-12 centuries) and taken to a deeper level by Fermat, Euler, Lagrange, Gauss, and many others. This topic remains an important domain of contemporary mathematics.

As one can see from the title, this book is an introduction to the study of diophantine equations. The material is organized in two parts. The first part contains three chapters. Chapter 1 introduces the reader to the main elementary methods in solving diophantine equations such as decomposition, modular arithmetic, mathematical induction, Fermat's

infinite descent. Chapter 2 presents some classical diophantine equations, including linear, pythagorean and some higher degree equations. Chapter 3 focuses on Pell's-type equations, serving again as an introduction to this special class of quadratic diophantine equations. Throughout Part I, each of the sections contains representative examples that illustrate the theoretical part.

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

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

This book was finalized during the period October 2001 – January 2002, when the second author was a visiting mathematician with the MAA American Mathematics Competitions at the University of Nebraska-Lincoln.

The authors wish to express their gratitude for all the support they have received while preparing the manuscript.

Lincoln, Nebraska, USA — The authors

January, 2002

Part 1

Diophantine Equations

CHAPTER 1

Elementary Methods for Solving Diophantine Equations

1.1. The Decomposition Method

This method consists of writing the equation $f(x_1, x_2, \ldots, x_n) = 0$ in the form

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

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 decomposition yields a system of equation

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

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

We will 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

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

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

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

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

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

All of the eight pairs we 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

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

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

Indeed, the equation is equivalent to

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

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

Example 3. *Determine all non-negative 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

$$\begin{cases} xy-6-(x+y)=-1 \\ xy-6+(x+y)=13 \end{cases} ; \quad \begin{cases} xy-6-(x+y)=-13 \\ xy-6+(x+y)=1 \end{cases}$$

These systems are equivalent to

$$\begin{cases} x+y=7 \\ xy=6 \end{cases} ; \quad \begin{cases} x+y=7 \\ xy=0 \end{cases}$$

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

$$\begin{cases} u+v=1 \\ uv=0 \end{cases}; \quad \begin{cases} u+v=-9 \\ uv=-2 \end{cases}; \quad \begin{cases} u+v=-3 \\ uv=4 \end{cases}; \quad \begin{cases} u+v=-5 \\ uv=-6 \end{cases}$$

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 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.

Exercises and Problems

1. Solve the following equation in integers x, y

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

2. For any 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 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 of integers (x, y) such that

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

(Romanian Mathematical Olympiad)

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

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

(16^{th} 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 $abc - 1$.

(33^{rd} IMO)

9. Find all right triangles with integer sidelengths such that their area and perimeter are equal.

10. Solve the 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)

1.2. Solving Diophantine Equations Using Inequalities

This method consists of restricting the intervals in which the variables lie by 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 of integers (x, y) 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 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 equation in positive integers* x, y, z

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

(Romanian Mathematical Olympiad)

Solution. Taking into account the symmetry, we may assume that $2 \leq x \leq y \leq z$. This implies the inequality $\frac{3}{x} \geq \frac{3}{5}$, 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 $(y - 10) | 100$. We obtain the solutions $(2, 11, 110)$, $(2, 12, 60)$, $(2, 14, 35)$, $(2, 15, 30)$, $(2, 20, 20)$.

If $x = 3$, we have $\frac{1}{y} + \frac{1}{z} = \frac{1}{15}$ 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 of positive integers* (x, y, z, w) *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

$$P(x) - (2x+8)^3 = -12x^2 + 36x + 272 = 0$$

$$P(x) - (2x+9)^3 = -24x^2 - 66x + 55 = 0$$

have 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 $-6 \leq x \leq -1$. For $-3 \leq x \leq -1$, 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 $-3 \leq x \leq -1$. Therefore $(-4, -4)$ and $(-5, -6)$ are the only solutions with $-6 \leq x \leq -4$. So the only solutions are $(-2, 6), (-3, 4), (-4, -4)$, and $(-5, -6)$.

Example 5. *Find all triples of positive integers (x, y, z) 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 $x \geq y \geq z$. Note that we must have $2 \leq (1 + 1/z)^3$ which implies that $z \leq 3$.

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 $\frac{4}{3} \leq \left(1 + \frac{1}{y}\right)^2$, which forces $y < 7$. Since $1 + \frac{1}{x} > 1$, 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 $y \geq z = 3$. These values yield the solutions $(8, 3, 3)$ and $(5, 4, 3)$.

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

Exercises and Problems

1. Solve in positive integers the equation

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

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

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

3. Determine all triples of positive integers (x, y, z) solutions to the equation

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

(Romanian Mathematical Olympiad)

4. Determine all pairs of integers (x, y) 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.

(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 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. Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that $\dfrac{a^2+b^2}{ab+1}$ is the square of an integer.

(29^{th} IMO)

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 integral-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. In many such cases the parametric method provides a proof of the existence of infinitely many solutions.

Example 1. *Prove that there exists an infinite set of triples of integers (x, y, z) 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 following 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 of positive integers (x, y, z) 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

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

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 by using 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

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

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

Example 3. *Find all triples of positive integers (x, y, z) 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 $(m + n)|d$, 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 $k, m, n \in \mathbb{Z}_+$.

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 integral solutions (x, y, z).

(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

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

and their remainders when dividing by B. All these remainders are distinct. Indeed, if

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

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 when dividing 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 the equation (1), i.e. u_0 (and v_0) is minimal. Then all solutions in positive integers to the equation (1) are given by

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

Coming back 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 exist 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 $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$ contain strictly increasing subsequences $(u_{n_j})_{j\geq 1}$, $(v_{n_j})_{j\geq 1}$. An infinite family of solutions is given by $(v_{n_j}, u_{n_j}, z_{n_j})$, $j \geq 1$.

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 relatively prime integral solutions.

(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 system of equations

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

has infinitely many solutions in positive integers.

(Titu Andreescu)

6. Find all triples of integers (x, y, z) 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 there are infinitely many quadruples of positive integers (x, y, z, w) such that

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

(Titu Andreescu)

9. Prove that each of the following equations has infinitely many solutions in integers (x, y, z, u):

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

10. 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.

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. *Show 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), hence it cannot be a perfect square.

Example 2. *Find all pairs of prime numbers (p, q) 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 (mod 3) and $q \equiv 1$ or 2 (mod 3). If $p \equiv q$ (mod 3), then the left hand side is divisible by 3, while the right hand side is not. If $p \not\equiv q$ (mod 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 not possible.

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 (mod 11) for all x, we have $x^5 \equiv -1$, 0 or 1 (mod 11). So $x^5 - 4$ is either 6, 7 or 8 modulo 11. However, the square residues modulo 11 are 0, 1, 3, 4, 5, or 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 is has at least three such solutions. Show that the equation has no integer solution when $n = 2891$.

(23^{rd} IMO)

Solution. Completing the cube, we obtain

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

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 of x and y give the same residue modulo 3 (different from 0), or exactly one of x and y is divisible by 3. Any of the two situations implies that one of the numbers $-x, y, x-y$ is divisible by 3, and by 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 the residue 2, and the only cubic residues modulo 9 are 0, 1, and 8.

Exercises and Problems

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)

2. Find all pairs of positive integers (x, y) 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 of positive integers (x, y) 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

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

(8^{th} USA Mathematical Olympiad)

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

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

(G.M. - Bucharest)

7. Find all triples of nonnegative integers (x, y, z) solutions to the equation

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

(Bulgarian Mathematical Olympiad)

8. Prove that the equation

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

has no solution in positive integers.

(25^{th} IMO Shortlist)

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

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

(37^{th} IMO)

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 (as 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

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

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

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

Example 2. *Prove that for all positive integers n, the following equation is solvable in positive integers*

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

(Dorin Andrica)

Solution. We use mathematical induction with step $s = 2$ 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

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

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

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

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 $x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^{k+2}$.

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 pairwise 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 the equation (1) and all its components are pairwise distinct.

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

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

Indeed,

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

$$= 1 - \frac{1}{2^{n-2}} + \frac{2^{n-2}}{2^{n-2}(2^{n-2}+1)} + \frac{1}{2^{n-2}(2^{n-2}+1)} = 1 - \frac{1}{2^{n-2}} + \frac{1}{2^{n-2}} = 1.$$

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

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

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 recursive 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) It is not known if there are infinitely many positive integers n for which equation (1) admits of 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 $n=15$,

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

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 for all $n \geq 412$ there exist 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 step 7, it suffices to prove the solvability of the equation (1) for $n = 412, 413, \ldots, 418$. The key idea is to construct solution in each of the above cases from smaller ones modulo 7.

Observe that $\dfrac{27}{3^3}=1$ and $27 \equiv 412 \pmod 7$,

$$\frac{4}{2^3}+\frac{9}{3^3}+\frac{36}{6^3}=1 \text{ and } 4+9+36=49 \equiv 413 \pmod 7,$$

$$\frac{4}{2^3}+\frac{32}{4^3}=1 \text{ and } 4+32=36 \equiv 414 \pmod 7,$$

$$\frac{18}{3^3}+\frac{243}{9^3}=1 \text{ and } 18+243=261 \equiv 415 \pmod 7,$$

$$\frac{18}{3^3}+\frac{16}{4^3}+\frac{144}{12^3}=1 \text{ and } 18+16+144=178 \equiv 416 \pmod 7,$$

$$\frac{4}{2^3}+\frac{16}{4^3}+\frac{36}{6^3}+\frac{144}{12^3}=1 \text{ and } 4+16+36+144=200=417 \pmod 7.$$

Finally,

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

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

$$x_1^3 + x_2^3 + \cdots + x_m^3 = (x_1 + x_2 + \cdots + x_m)^2.$$

(Titu Andreescu)

Solution. We will prove first the following auxiliary result:

Lemma. *If $a_1, a_2, \ldots$ is a sequence of distinct positive integers, then for all integers $n \geq 1$ the following inequality holds*

$$a_1^3 + \cdots + a_n^3 \geq (a_1 + \cdots + a_n)^2 \tag{1}$$

Proof. One may assume, without loss of generality, that $a_1 < a_2 < \cdots < a_n$, is this can be considered part of the hypothesis. For $n = 1$, $a_1 \geq 1$ implies $a_1^3 \geq a_1^2$. Suppose the claim is true for some $n = k$, and let $a_1 < a_2 < \cdots < a_k < a_{k+1}$ be $k+1$ distinct positive integers. Then $a_{k+1} \geq a_k + 1$. A short computation then gives

$$\frac{(a_{k+1} - 1)a_{k+1}}{2} \geq \frac{a_k(a_k + 1)}{2} = 1 + 2 + \cdots + a_k.$$

Note that the sum $1 + 2 + \cdots + a_k$ contains all positive integers not exceeding a_k, so it is greater than or equal to $a_1 + a_2 + \cdots + a_k$, a sum of distinct integers among $1, 2, \ldots, a_k$. So

$$\frac{(a_{k+1} - 1)a_{k+1}}{2} \geq a_1 + a_2 + \cdots + a_k$$

which, multiplied by $2a_{k+1}$, gives

$$(a_{k+1}^2 - a_{k+1})a_{k+1} \geq 2(a_1 + a_2 + \cdots + a_k)a_{k+1},$$

that is

$$a_{k+1}^3 \geq 2(a_1 + a_2 + \cdots + a_k)a_{k+1} + a_{k+1}^2.$$

On the other hand, by the induction hypothesis,

$$a_1^3 + a_2^3 + \cdots + a_k^3 \geq (a_1 + a_2 + \cdots + a_k)^2.$$

Adding up the last two inequalities yields

$$a_1^3 + a_2^3 + \cdots + a_k^3 + a_{k+1}^3 \geq (a_1 + a_2 + \cdots + a_k + a_{k+1})^2,$$

hence the inequality is true for $n = k + 1$. □

Without loss of generality, we may assume that $x_1 < x_2 < \cdots < x_m$. This means $x_1 \geq 1$, $x_2 \geq 2, \ldots$, $x_m \geq m$. We will prove that $x_1 = 1$, $x_2 = 2, \ldots$, $x_m = m$.

We have $x_{m-1} \leq x_m - 1$, $x_{m-2} \leq x_m - 2, \ldots$, $x_1 \leq x_m - (m-1)$, hence

$$x_1 + x_2 + \cdots + x_{m-1} \leq (m-1)x_m - \frac{(m-1)m}{2} \tag{2}$$

From the Lemma,

$$x_1^3 + x_2^3 + \cdots + x_{m-1}^3 \geq (x_1 + x_2 + \cdots + x_{m-1})^2 \tag{3}$$

On the other hand, from the given equation,

$$x_1^3 + x_2^3 + \cdots + x_{m-1}^3 + x_m^3 = (x_1 + x_2 + \cdots + x_{m-1})^2 +$$

$$+2(x_1 + x_2 + \cdots + x_{m-1})x_m + x_m^2. \tag{4}$$

From (3) and (4), it follows that

$$x_m^3 \leq 2(x_1 + x_2 + \cdots + x_{m-1})x_m + x_m^2$$

or

$$x_m^2 \leq 2(x_1 + x_2 + \cdots + x_{m-1}) + x_m$$

and, by using (2), we obtain

$$x_m^2 \leq 2(m-1)x_m - (m-1)m + x_m.$$

This is equivalent to

$$x_m^2 - (2m-1)x_m + (m-1)m \leq 0$$

or

$$(x_m - m)(x_m - (m-1)) \leq 0.$$

Since $x_m > m-1$, it follows that $x_m \leq m$, hence $x_m = m$. Taking again into account that $x_1, x_2, \ldots, x_m$ are pairwise distinct yields $x_1 = 1$, $x_2 = 2, \ldots, x_m = m$.

All solutions to the equation are given by the $m!$ permutations of $\{1, 2, \ldots, m\}$.

Remark. If we give up distinctiveness, then our equation has other solutions as well. For example if $m = 6$,

$$1^3 + 2^3 + 2^3 + 3^3 + 4^3 + 6^3 = (1+2+2+3+4+6)^2.$$

Exercises and Problems

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)

2. Prove that for all positive integers n, the following equation is solvable in integers

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

(Dorin Andrica)

3. Prove that for all integers $n \geq 1$, there exist integers x, y, z such that

$$x^2 + y^2 + z^2 = 3^{2^n}.$$

(Dorin Andrica)

4. The integer $t_k = \dfrac{k(k+1)}{2}$ 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 quite famous for his contributions to mathematics even though he was only considered 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 proved to have a monumental impact on the world of mathematics through his findings 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 can't reach any rungs.

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

The *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 where an n for which $P(n)$ was true, you could construct a sequence $n > n_1 > n_2 > \ldots$ all of which would be greater than k, but for the nonnegative integers, no such descending is possible.

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

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

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 $n_1 \geq n_2 \geq \ldots$, then there exists i_0 such that $n_{i_0} = n_{i_0+1} = \ldots$*

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 $2|x_1$, so $x_1 = 2x_2$, $x_2 \in \mathbb{Z}_+$. Then $4x_2^3 + y_1^3 = 2z_1^3$, 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 $x_1 > x_2 > x_3 > \ldots$ But this contradicts FMID Variant 1.

Example 2. *Solve in nonnegative integers the equation*

$$2^x - 1 = xy$$

(Putnam Mathematical Competition)

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 $p_1 | 2^q - 1$. From Fermat's Little Theorem we have $p_1 | 2^{p_1 - 1} - 1$, therefore $q \leq p_1 - 1 < p_1$.

Let us prove now that $q|x$. 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 $p_1 | 2^r - 1$, which contradicts the minimality of q.

Thus $q|x$ 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: $p_1 > p_2 > \ldots$, in contradiction with 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* $(n^2 - mn - m^2)^2 = 1$.

(22nd IMO)

Solution. Note that $(m, n) = (1, 1)$ satisfies the relation $(n^2 - mn - m^2)^2 = 1$. Also, if a pair (m, n) satisfies this relation and $0 < m < n$, then $m < n < 2m$, 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 $0 < n-m < m$.

By FMID Variant 2, the transformation $(m, n) \to (n-m, m)$ 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:

$$(1,1) \to (2,1) \to (3,2) \to (5,3) \to \ldots$$

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 $F_{15}^2 + F_{16}^2 = 3514578$.

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.

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 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 $\alpha = \dfrac{1+\sqrt{5}}{2}$, $\beta = \dfrac{1-\sqrt{5}}{2}$, and for the second, $\alpha = \dfrac{1+\sqrt{5}}{2\sqrt{5}}$, $\beta = -\dfrac{1-\sqrt{5}}{2\sqrt{5}}$.

We obtain

$$x_n = \left(\frac{1+\sqrt{5}}{2}\right)^{2n+1} + \left(\frac{1-\sqrt{5}}{2}\right)^{2n+1} \tag{1}$$

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

Using the relations (1) and (2) 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

$$a_1 + b_1 > a_2 + b_2 > a_3 + b_3 > \ldots$$

in contradiction with 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

$$0 = x_1^2 + y_1^2 + x_1 + y_1 + 1 - x_1 y_1 z_1$$

$$= (y_1 z_1 - x_1 - 1)^2 + y_1^2 + (y_1 z_1 - x_1 - 1) + y_1 + 1 - (y_1 z_1 - x_1 - 1) y_1 z_1,$$

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 $x_1 > x_2 > x_3 > \ldots$, in contradiction with 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

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

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 $v_1 \geq v_2 \geq v_3 \geq \ldots$ 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 $\alpha = \dfrac{3+\sqrt{21}}{2\sqrt{21}}$ and $\beta = -\dfrac{3-\sqrt{21}}{2\sqrt{21}}$, therefore

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

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

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

Exercises and Problems

1. Find all triples (x, y, z) of positive integers 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 equation in integers x, y, z, u

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

4. Solve the equation in positive integers

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

5. Determine all integral solutions to

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

(5^{th} USA Mathematical Olympiad)

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.

7. Solve in positive integers x, y, u, v the system

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

8. 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)

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

(Mathematics Magazine)

10. 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 a rank k such that $(x, y) = (x_k, x_{k+1})$.

(Romanian Mathematical Olympiad)

11. Find all pairs of nonnegative integers (m, n) such that

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

(42^{nd} IMO USA Team Selection Test)

12. 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

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

(20^{th} 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 the equation*

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

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

(Titu Andreescu)

Solution. Writing the equation in the form

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

yields $x_1 = 1$ and

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

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

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

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

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

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

Remark. Substituting back into the equation yields the identity

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

Example 2. *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 be both true, because adding them up 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 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 by 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 the integral solutions to the equation

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

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

(21^{st} 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 $N = n_0 n_1 + n_1 n_2 + \cdots + n_{l-1} n_l$. 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 work 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*

$$x^3 + 2y^3 + 4z^3 - 6xyz = 1. \quad (1)$$

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

(USA Proposal for the 38^{th} 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

$$(x + ys + zx^2)(x + ys\omega + zs^2\omega^2)(x + ys\omega^2 + zs^2\omega) = 1. \qquad (2)$$

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

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

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

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

hence $|u - vs|, |vs - ws^2|, |ws^2 - u|$ 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 $x + vs + ws^2 \geq 1 + s + s^2$, a contradiction. Similarly, assuming $w \leq -1$

yields $x + vs + ws^2 \leq -(1 + s + s^2)$, a contradiction. Hence $w = 0$, yielding the inequalities

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

The second and third condition imply $-1 \leq u, v \leq 1$, which yields only the solutions $(u, v, w) = (1, 0, 0)$ or $(-1, 1, 0)$. The third solution fails the first condition, so we deduce $(u, v, w) = (1, 0, 0)$ and conclude that

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

as desired.

Exercises and Problems

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)

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 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, 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.

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 measurements 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) 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)

CHAPTER 2

Some Classical Diophantine Equations

2.1. Linear Diophantine Equations

An equation of the form

$$a_1x_1 + \cdots + a_nx_n = b \tag{2.1.1}$$

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

The main result concerning linear diophantine equations is the following:

Theorem 2.1.1. *The equation (2.1.1) is solvable if and only if* $gcd(a_1, \ldots, a_n)|b$.

In case of solvability, all integer solutions to (2.1.1) can be expressed in terms of $n-1$ *integral parameters.*

Proof. Let $d = gcd(a_1, \ldots, a_n)$.

If b 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.

If $d|b$, then we obtain the equivalent equation

$$a_1'x_1 + \cdots + a_n'x_n = b'$$

where $a_i' = a_i/d$ for $i = 1, \ldots, n$ and $b' = b/d$. Clearly, we have $gcd(a_1', \ldots, a_n') = 1$.

We use induction on the number n of the variables. In the case $n = 1$ the equation has the form $x_1 = b$ or $-x_1 = b$, and thus the unique solution does not depend on any parameter.

We now assume that $n \geq 2$ and that the solvability property holds for all linear equations in $n-1$ variables. Our goal is to prove the solvability of equations in n variables. Set $d_{n-1} = gcd(a_1, \ldots, a_{n-1})$. Then any solution $(x_1, \ldots, x_n)$ of (2.1.1) satisfies the congruence

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{d_{n-1}},$$

which is equivalent to

$$a_nx_n \equiv b \pmod{d_{n-1}} \tag{2.1.2}$$

Multiplying both sides of (2.1.2) by $a_n^{\varphi(d_{n-1})-1}$, where φ is Euler's function, and taking into account that $a_n^{\varphi(d_{n-1})} \equiv 1 \pmod{d_{n-1}}$, we obtain

$$x_n \equiv c \pmod{d_{n-1}},$$

where $c = a_n^{\varphi(d_{n-1})-1}b$. It follows that $x_n = c + d_{n-1}t_{n-1}$, with $t_{n-1} \in \mathbb{Z}$. Substituting in (2.1.1) and rearranging yields the equation in $(n-1)$ variables

$$a_1x_1 + \cdots + a_{n-1}x_{n-1} = b - a_nc - a_{n-1}d_{n-1}t_{n-1}.$$

It remains to show that $d_{n-1} | (b - a_nc - a_{n-1}d_{n-1}t_{n-1})$, which is equivalent to $a_nc \equiv b \pmod{d_{n-1}}$. The last relation is true because of the choice of c. Therefore we can divide the last equation by d_{n-1}, and obtain

$$a_1'x_1 + \cdots + a_{n-1}'x_{n-1} = b' \tag{2.1.3}$$

where $a_i' = a_i/d_{n-1}$ for $i = 1, \ldots, n-1$ and $b' = (b - a_n c)/d_{n-1} - a_n t_{n-1}$. Since $gcd(a_1', \ldots, a_{n-1}') = 1$, by the induction hypothesis the equation (2.1.3) is solvable for each $t_{n-1} \in \mathbb{Z}$ and its solutions can be written in terms of $n-2$ integral parameters. if we add to these solutions, $x_n = c + d_{n-1} t_{n-1}$, we obtain solutions to (2.1.1) in terms of $n-1$ parameters. □

Corollary 2.1.2. *Let a_1, a_2 be relatively prime integers. If (x_1^0, x_2^0) is a solution to the equation*

$$a_1 x_1 + a_2 x_2 = b, \tag{2.1.4}$$

then all of its solutions are given by

$$\begin{cases} x_1 = x_1^0 + a_2 t \\ x_2 = x_2^0 - a_1 t \end{cases} \tag{2.1.5}$$

where $t \in \mathbb{Z}$.

Example 1. *Solve the equation*

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

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

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

A solution to this equation is $x = -1 + 3s$, $y = 1 - s$. Applying (2.1.5) 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

$$a_1x_1 + \cdots + a_nx_n = N$$

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 him who asked what is the largest amount of money that cannot be paid by using coins worth $a_1, \ldots, a_n$ cents).

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

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

Solution. Suppose that $N > ab-a-b$. From Corollary 2.1.2 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 $0 \leq y_0 - at \leq a - 1$. 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 only need 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 $a|(y+1)$ and $b|(x+1)$, 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 explicitely 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 $d_i = gcd(a_1, \ldots, a_i)$. Erdös 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

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

where

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

Suppose that the equation

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

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

Theorem 2.1.3. *1) The generating function of the sequence* $(A_n)_{n\geq 1}$ *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) By using the geometric series, we have

$$\frac{1}{1-x^{a_k}} = 1 + x^{a_k} + x^{2a_k} + \dots, \quad k = 1, \dots, m$$

hence

$$f(x) = (1 + x^{a_1} + x^{2a_1} + \dots)\dots(1 + x^{a_m} + x^{2a_m} + \dots) =$$

$$= 1 + A_1 x + \dots + A_n x^n + \dots$$

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 which cannot be expressed in the form $xbc + yca + zab$, where x, y, z are nonnegative integers.

(24^{th} 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

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1q}x_q = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2q}x_q = 0 \\ \cdots\cdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pq}x_q = 0 \end{cases}$$

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 exist j such that $x_j \neq 0$;

c) $|x_j| \leq q$ for any $j = 1, 2, \ldots, q$.

(18^{th} IMO)

2.2. Pythagorean Triples and Related Problems

One of the most celebrated diophantine equation is the so-called *pythagorean equation*

$$x^2 + y^2 = z^2 \tag{2.2.1}$$

Studied in detail by Pythagoras in connection with the right-angled triangles whose sidelengths 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 the 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) where x_0, y_0, z_0 are pairwise relatively prime is called *primitive solution.*

Theorem 2.2.1. *Any primitive solution (x, y, z) in positive integers to the equation (2.2.1) 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 $m > n$.

Proof. The integers x and y cannot be both 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

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

shows that the triple given by (2.2.2) is indeed a solution to the equation (2.2.1) and y is even.

Moreover, if $gcd(x, y, z) = d \geq 2$, then d divides

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

and d divides

$$2n^2 = (m^2 + n^2) - (m^2 - n^2).$$

Since m and n are relatively prime it follows that $d = 2$. Hence $m^2 + n^2$ is even, in contradiction with 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

$$x = b - c = m^2 - n^2, \quad y = 2mn, \quad z = b + c = m^2 + n^2. \quad \square$$

A triple (x, y, z) of the form (2.2.2) is called a *pythagorean triple.*

In order to list systematically all the primitive solutions to the equation (2.2.1), we assign values 2,3,4, ... for the number m successively and then for each of these values we take those integers n which are relatively prime to m, less than m and even whenever m is odd.

Here is the table of the first twenty primitive solutions listed according to the above-mentioned rule.

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 the 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 the 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 the 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

$$x^2+4l^2+4m^2=(x+u)^2$$

or

$$u^2=4(l^2+m^2)-2ux.$$

Therefore u^2 is even, so $u = 2n$ for some positive integer n. It follows that $x=\dfrac{l^2+m^2-n^2}{n}$ and $t=x+u=x+2n=\dfrac{l^2+m^2+n^2}{n}$, 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

$$l=\frac{y}{2},\quad m=\frac{z}{2},\quad n=\frac{t-x}{2}$$

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 the 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 ten solutions to the equation (2.2.4) 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) The integral solutions to the equation (2.2.4) can be written in the following form

$$x = l^2 + m^2 - n^2, \quad y = 2lm \quad z = 2mn, \quad t = l^2 + m^2 + n^2,$$

where l, m, n are integers.

Note that in this form it is possible to obtain the same solution more than once. On the other hand, this form of the solutions is quite similar to the one for the solutions to (2.2.1).

2) 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 rectangular hyperparallelepiped in $\mathbb{R}^k$ and the length x_{k+1} of its diagonal, respectively. All integral solutions to the equation (2.2.6) are given by

$$\begin{aligned} x_1 &= m_1^2 + m_2^2 + \cdots + m_{k-1}^2 - m_k^2 \\ x_2 &= 2m_1 m_k \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_k &= 2m_{k-1} m_k \\ x_{k+1} &= m_1^2 + m_2^2 + \cdots + m_{k-1}^2 + m_k^2 \end{aligned}$$

where $m_1, m_2, \ldots, m_k$ are arbitrary integers.

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 $z|xy$ 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 $gcd(a, b, c) = 1$. The 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 by using (2.2.7) we deduce that $c|d$, 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 the equation (2.2.7) are given by

$$x = k(m^4 - n^4), \quad y = 2kmn(m^2 + n^2), \quad z = 2kmn(m^2 - n^2)$$

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

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 up 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 $d|x$ and $d\left|\left(\frac{z+w}{2} + \frac{z-w}{2}\right)\right. = z$. From the first equation in (2.2.11) we then obtain $d|y$, in contradiction with $gcd(x,y) = 1$.

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

$$2y^2 = 2(m^2 - n^2) \cdot 4mn,$$

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, 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 with the minimality of $x^2 + y^2$.

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

$$x^2 + y^2 = 1997(x - y).$$

(Bulgarian Mathematical Olympiad)

Solution. The solution are

$$(x, y) = (170, 145) \text{ or } (1827, 145).$$

We have

$$x^2 + y^2 = 1997(x - y)$$

$$(x + y)^2 + ((x - y)^2 - 2 \cdot 1997(x - y)) = 0$$

$$(x + y)^2 + (1997 - x + y)^2 = 1997^2.$$

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 $m > n$, $1997/2 \leq$

$m^2 \leq 1997$. Thus we only need to consider $m = 34, 41, 44$. The only solution is $(m, n) = (34, 29)$. Thus

$$(a, b) = (1972, 315),$$

which leads to our final solutions.

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

$$2(m^4 + n^4), \quad m^4 + 6m^2n^2 + n^4$$

is a perfect square.

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)

4. Determine all pythagorean triangles whose areas are numerically equal to their perimeters.

5. Prove that there is no pythagorean triangle whose area is a perfect square.

6. Prove that the number of primitive pythagorean triangles with a given inradius r is a power of 2.

2.3. Other Remarkable Equations

2.3.1. Some Quadratic Diophantine Equations and Related Problems

We begin 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 2.3.1. *All integral solutions to (2.3.1) are given by*

$$\begin{cases} x = k(an^2 - 2mn) \\ y = k(m^2 - n^2) \\ z = k(amn - m^2 - n^2) \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(an^2 - 2mn) \\ z = k(amn - m^2 - n^2) \end{cases} \tag{2.3.2}$$

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

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 the 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 the equation (2.3.1) is equivalent to

$$x(x + ay) = (z - y)(z + y) \tag{2.3.3}$$

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 $z = k(amn - m^2 - n^2)$ and get the solutions (2.3.2). □

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 way, we may show that the solutions to the equation

$$x^2 + axy + by^2 = z^2 \tag{2.3.5}$$

are given by

$$\begin{cases} x = k(m^2 - bn^2) \\ y = k(an^2 - 2mn) \\ z = k(amn - m^2 - bn^2) \end{cases} \tag{2.3.6}$$

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

3) Using the above remark we can solve the diophantine equation

$$x^2 + uxy + vy^2 = z^2.$$

Its 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 the equation (2.3.1) can be expressed as follows

$$\begin{cases} x = k(2mn + an^2) \\ y = k(m^2 - n^2) \\ z = k|m^2 + amn + n^2| \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(2mn + an^2) \\ z = k|m^2 + amn + n^2| \end{cases} \tag{2.3.7}$$

where $k, m, n \in \mathbb{Z}_+^*$, $2m + an > 0$, $m > n$.

Aside from the case $a = 0$, when we obtain the pythagorean equation, the following two cases present interest:

The case $a = 1$. The 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 integers solutions are given by

$$\begin{cases} x = k(2mn + n^2) \\ y = k(m^2 - n^2) \\ z = k(m^2 + mn + n^2) \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(2mn + n^2) \\ z = k(m^2 + mn + n^2) \end{cases} \tag{2.3.9}$$

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

The solutions (2.3.9) give all triples of positive integers (x, y, z) which are the sidelengths of a triangle whose opposite angle to z is $120°$.

The case $a = -1$. The equation (2.3.1) becomes

$$x^2 - xy + y^2 = z^2 \tag{2.3.10}$$

Its positive integral solutions are given by

$$\begin{cases} x = k(2mn - n^2) \\ y = k(m^2 - n^2) \\ z = k(m^2 - mn + n^2) \end{cases} \qquad \begin{cases} x = k(m^2 - n^2) \\ y = k(2mn - n^2) \\ z = k(m^2 - mn + n^2) \end{cases} \tag{2.3.11}$$

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

The solutions (2.3.11) characterize all triples of positive integers (x, y, z) which are the sidelengths of a triangle whose angle which opposes to 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 positive integers k, m, n with $m > n$, such that

$$k(m^2 + mn + n^2) = 49.$$

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 $(x, y) = (21, 35)$.

It is natural to ask in what situations the solutions (x, y) to the equations (2.3.8) and (2.3.10), respectively, 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 $(x, y, z) = (k, 0, k^2)$, $(x, y, z) = (0, k, k^2)$, $k \in \mathbb{Z}_+$.

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

$$4z^2 - (2x^2 + y^2)^2 = 3y^4 \tag{2.3.13}$$

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

If $gcd(2z + 2x^2 + y^2, 2z - 2x^2 - y^2) = d$, then d is odd and d divides both z and $2x^2 + y^2$. From (2.3.13) it follows that $d|3y$. If $d > 3$, then $d|y$ and $d|2x^2$, i.e. $gcd(x, y) \geq d$, a contradiction. If $d = 3$, it follows that $3|z$ and from (2.3.12) we obtain $3|(2x^2 + y^2)$ so $3|y$. Therefore $3|x$ 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,

$$4x^2 = 3a^4 - 2a^2b^2 - b^4 = (a^2 - b^2)(3a^2 + b^2).$$

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

$$(x, y, st) = (k, 0, k^2) \text{ or } (x, y, st) = (0, k, k^2),$$

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 $(x, y, z) = (k, 0, k^2), (0, k, k^2), (k, k, k^2)$, $k \in \mathbb{Z}_+$.

Proof. We may assume that $gcd(x, y) = 1$ and that xy is minimal. Write the equation as

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

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

$$x = d_1X, \quad b = d_1B, \quad y = d_2Y, \quad a = d_2A, \quad XY = 2AB.$$

Since $gcd(X, B) = 1$ and $gcd(Y, A) = 1$, it follows that

$$(X, Y) = (2A, B) \text{ or } (X, Y) = (A, 2B).$$

Hence

$$x = 2d_1A, \quad b = d_1B, \quad y = d_2B, \quad a = d_2A$$

or

$$x = d_1A, \quad b = d_1B, \quad y = 2d_2B, \quad a = d_2A.$$

In the first case,

$$4d_1^2A^2 - d_2^2B^2 = d_2^2A^2 - d_1^2B^2$$

i.e.

$$d_1^2(4A^2 + B^2) = d_2^2(A^2 + B^2). \tag{2.3.15}$$

The condition $gcd(a,b) = 1$ implies $gcd(A,B) = 1$. Let $gcd(4A^2 + B^2, A^2 + B^2) = D$. Then $D|(4A^2 + B^2 - A^2 - B^2) = 3A^2$, and since $A^2 + B^2 \not\equiv 0 \pmod 3$, it follows that $gcd(D,3) = 1$, hence $D|A^2$ and $D|(A^2+B^2-A^2) = B^2$. The condition $gcd(A,B) = 1$ now implies $D = 1$ and from (2.3.15) we obtain

$$A^2 + B^2 = C^2 \text{ and } 4S^2 + B^2 = D^2 \tag{2.3.16}$$

for some positive integers C and D.

We may suppose that B is odd since, if B were even, we could out $B = 2B_1$ 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 $pq \leq a \leq xy/2$, and so the method of descent applies since p and q are not both odd. It follows that $xy = 0$, yielding the solutions $(k,0,k^2)$, $(0,k,k^2)$, $k \in \mathbb{Z}_+$.

The other alternative gives

$$d_1^2A^2 - 4d_2^2B^2 = d_2^2A^2 - d_1^2B^2,$$

and so

$$d_1^2(A^2 + B^2) = d_2^2(A^2 + 4B^2).$$

Now $A = p^2 - q^2$, $B = pq$ and $pq \leq b \leq xy/2$ and so the method of descent applied 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 (k,k,k), $k \in \mathbb{Z}_+$. $\square$

Example 3. *Prove that four distinct squares cannot form an arithmetical sequence.*

Solution. Let the squares be a^2, b^2, c^2, d^2, arranged in increasing order. Then

$$a^2 + c^2 = 2b^2, \quad b^2 + d^2 = 2c^2.$$

Without loss of generality, we may assume that a, b, c, d are all odd. We have

$$a^2(2c^2 - b^2) = d^2(2b^2 - c^2),$$

and so

$$2(a^2c^2 - b^2d^2) = a^2b^2 - c^2d^2.$$

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

$$x^4 - x^2y^2 + y^4 = (z^2 + w^2)^2.$$

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 with $a < b < c < d$.

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 (x_1^2, y_1^2, z_1) 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

$$gcd(z_1 - x_1^2, z_1 + x_1^2) = 2 \tag{2.3.18}$$

Indeed, if $d|(z_1 - x_1^2)$ and $d|(z_1 + x_1^2)$, then $d|2z_1$ and $d|2x_1^2$. But $gcd(z_1, x_1) = 1$ and z_1 is odd, so $d = 2$.

Since $y_1^4 = (z_1 - x_1^2)(z_1 + x_1^2)$, 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

$$4b^4 = (a^2 - x_1)(a^2 + x_1).$$

Since $gcd(a, b) = 1$, we have $gcd(a, x_1) = 1$ and we see, as in the proof of (2.3.18), that $gcd(a^2 - x_1, a^2 + x_1) = 2$. Consequently

$$a^2 - x_1 = 2x_2^4 \text{ and } a^2 + x_1 = 2y_2^4,$$

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's 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 $(xy')^2 \equiv -3 \pmod{p}$. 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 $p|(a^2x^2 - y^2)$. It is clear that $gcd(a,p) = 1$ and if we denote $b = [\sqrt{p}]$, 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 denote $x = u_1 - u_2$, $y = |v_1 - v_2|$. Therefore, $0 < x, y \leq b < \sqrt{p}$ and $ax + y \equiv 0 \pmod{p}$, i.e. $a^2x^2 - y^2 \equiv 0 \pmod{p}$. We obtain $p|((a^2+3)x^2 - (3x^2+y^2)$, 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 $3p = 3x^2 + y^2$, 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 $p|x^2 + 3y^2$, then $p|x$ and $p|y$. 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 $n = a^2b$, 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 $b = p_1 p_2 \ldots p_m = x^2 + 3y^2$, 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 $n_1 n_2 = (x_1x_2 + 3y_1y_2)^2 + 3(x_1y_2 - x_2y_1)^2$. Finally, $n = a^2b = (ax)^2 + 3(ay)^2$. □

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* α, β *such that* $\alpha \not\equiv \beta \pmod{2}$, $gcd(\alpha, 3\beta) = 1$ *and*

$$x_0 = \alpha(\alpha^2 - 9\beta^2), \quad y_0 = 3\beta(\alpha^2 - \beta^2), \quad z_0 = \alpha^2 + 3\beta^2.$$

Proof. Let (x_0, y_0, z_0) be a triple of integers satisfying the above conditions. From the identity

$$\alpha^2(\alpha^2 - 9\beta^2)^2 + 3(3\beta(\alpha^2 - \beta^2))^2 = (\alpha^2 + 3\beta^2)^3$$

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 $gcd(\alpha, 3\beta(\alpha^2 - \beta^2)) = gcd(\alpha, \alpha^2 - \beta^2) = gcd(\alpha, -\beta^2) = 1$ and that $gcd(\alpha^2 - 9\beta^2, 3\beta) = gcd(\alpha^2, 3\beta) = 1$. Taking into account the

condition $\alpha \not\equiv \beta \pmod 2$, we have

$$gcd(\alpha^2 - 9\beta^2, \alpha^2 - \beta^2) = gcd(-8\beta^2, \alpha^2 - \beta^2) =$$

$$= gcd(\beta^2, \alpha^2 - \beta^2) = gcd(\beta^2, \alpha^2) = 1.$$

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 by 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 α_1, β_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

$$a = \alpha_1(\alpha_1^2 - 9\beta_1^2), \quad b = 3\beta_1(\alpha_1^2 - \beta_1^2).$$

It is not difficult to see that $a \not\equiv b \pmod 2$ and $gcd(a, 3b) = 1$. We have

$$p^6t^3 = p^3z_0^3 = (a^2 + 3b^2)(x_0^2 + 3y_0^2) = (ax_0 + 3by_0)^2 + 3(bx_0 - ay_0)^2 =$$

$$= (ax_0 - 3by_0)^2 + 3(bx_0 + ay_0)^2.$$

Also

$$(bx_0 + ay_0)(bx_0 - ay_0) = b^2x_0^2 - a^2y_0^2 = b^2x_0^2 - (p^3 - 3b^2)y_0^2 =$$

$$= b^2(x_0^2 + 3y_0^2) - p^3y_0^2 = b^2z_0^3 - p^3y_0^2 = b^2p^3t^3 - p^3y_0^2,$$

therefore $p^3|(bx_0 + ay_0)(bx_0 - ay_0)$. Since $gcd(abx_0y_0, p) = 1$, it follows that the relations $p^3|bx_0 + ay_0$ and $p^3|bx_0 - ay_0$ 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 and 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 α_2 and β_2 satisfying the properties $\alpha_2 \not\equiv \beta_2 \pmod 2$, $gcd(\alpha_2, 3\beta_2) = 1$, $c = \alpha_2(\alpha_2^2 - 9\beta_2^2)$, $d = 3\beta_2(\alpha_2^2 - \beta_2^2)$ and $t = \alpha_2^2 + 3\beta_2^2$. From the above relations it follows that

$$z_0 = pt = (\alpha_1^2 + 3\beta_1^2)(\alpha_2^2 + 3\beta_2^2) = (\alpha_1\alpha_2 + 3\beta_1\beta_2)^2 + 3(\alpha_1\beta_2 - \alpha_2\beta_1)^2.$$

Denoting

$$\alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2, \quad \beta = \varepsilon(\alpha_2\beta_1 - \alpha_1\beta_2)$$

we obtain $z_0 = \alpha^2 + 3\beta^2$ and

$$x_0 = \alpha(\alpha^2 - 9\beta^2), \quad y_0 = 3\beta(\alpha^2 - \beta^2).$$

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. *The 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. Denote

$$x_0 + y_0 = 2u \quad \text{and} \quad x_0 - y_0 = 2v.$$

We obtain $x_0 = u + v$, $y_0 = u - v$ and from (2.3.22) it follows that

$$2u(u^2 + 3v^2) = z_0^3 \tag{2.3.24}$$

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 $gcd(2u, u^2 + 3v^2) = gcd(u, u^2 + 3v^2) = gcd(u, 3v^2) = gcd(u, 3)$.

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 α, β such that $gcd(\alpha, 3\beta) = 1$, $\alpha \not\equiv \beta \pmod 2$ and

$$s = \alpha^2 + 3\beta^2, \quad u = \alpha(\alpha^2 - 9\beta^2), \quad v = 3\beta(\alpha^2 - \beta^2).$$

Therefore, $2u = t^3 = (2\alpha)(\alpha - 3\beta)(\alpha + 3\beta)$. The factors 2α, $\alpha - 3\beta$, $\alpha + 3\beta$ 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,

$$|XYZ| = \sqrt[3]{|2\alpha(\alpha^2 - 9\beta^2)|} = \sqrt[3]{2u} = \sqrt[3]{x_0 + y_0} < |\sqrt[3]{x_0y_0}| < |x_0y_0z_0|,$$

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 $gcd(3u_1^2 + v^2, 3) = 1$. From (2.3.25) it follows that $u_1 = 3u_2$, $u_2 \in \mathbb{Z}$, and $2u_2(3u_1^2 + v^2) = z_1^2$.

Since $gcd(2u_2, 3u_1^2 + v^2) = 1$, 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 α, β 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 $u_2 = \beta(\alpha^2 - \beta^2)$ and $m^3 = 2\beta(\alpha - \beta)(\alpha + \beta)$.

Taking into account that the integers 2β, $\alpha - \beta$ 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

$$|XYZ| = \sqrt[3]{|2\beta(\alpha^2 - \beta^2)|} < |\sqrt[3]{2u}| = |\sqrt[3]{x_0 + y_0}| < |x_0y_0z_0|$$

which contradicts the minimality of $|x_0y_0z_0|$. □

Remarks. 1) The 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 the equation (2.3.26) has no nonzero integer solutions for x, y, z when $n > 2$.

Around 1630, Fermat wrote a note on a margin of a page of Diophantus' *Arithmetica*:

"I have discovered a truly remarkable proof which this margin is too small to contain."

Fermat's proof was never found but this theorem became famous, capturing the attention of mathematics world.

Along 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 ($n = 5$, $n = 14$), 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 4000000 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 the equation (2.3.26).

The final chapter in the story began in 1955, although at this stage the work was not thought of as connected with Fermat's Last Theorem. Yutaka Taniyama asked some questions about elliptic curves, i.e. curves of the form $y^2 = x^3 + ax + b$ for constants a and b. Further work by Weil and Shimura produced a conjecture, now known as the Shimura-Taniyama-Weil Conjecture. In 1986, the connection was made between the Shimura-Taniyama-Weil Conjecture and Fermat's Last Theorem by

Frey, showing that Fermat's Last Theorem was far from being some unimportant curiosity in number theory but was in fact related to fundamental properties of space. Further work by other mathematicians showed that a counterexample to Fermat's Last Theorem would provide a counterexample to the Shimura-Taniyama-Weil Conjecture. The proof of Fermat's Last Theorem was completed in 1993 by Andrew Wiles, a United Kingdom 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, the second on June 22. In the final lecture on Wednesday, June 23, 1993 at around 10.30 in the morning, Wiles announced his proof of Fermat's Last Theorem as a corollary to his main results. Having written the theorem on the blackboard he said "*I will stop here* and sat down". In fact Wiles had proved the Shimura-Taniyama-Weil Conjecture for a class of examples, including those necessary to prove Fermat's Last Theorem. This, however, is not the end of the story. On December 4, 1993 Andrew Wiles made the following statement:

"*The key reduction of (most cases of) the Taniyama-Shimura conjecture to the calculation of the Selmer group is correct. However the final calculation of a precise upper bound for the Selmer group in the semisquare case (of the symmetric square representation associated to a modular form) is not yet complete as it stands. I believe that I will be able to finish this in the near future using the ideas explained in my Cambridge lectures.*"

In fact, from the beginning of 1994, Wiles began to collaborate with Richard Taylor in an attempt to fill the holes in the proof. However they decided that one of the key steps in the proof, using methods due

to Flach, could not be made to work. They tried a new approach with a similar lack of success. In August 1994 Wiles addressed the International Congress of Mathematicians but was no nearer to solving the difficulties. Taylor suggested a last attempt to extend Flach's method in the way necessary and Wiles, although convinced it would not work, agreed mainly to enable him to convince Taylor that it could never work. Wiles worked on it for about two weeks, then suddenly inspiration struck.

"*In a flash I saw that the thing that stopped if* [the extension of Flach's method] *working was something that would make another method I had tried previously work.*"

On October 6, 1994, Wiles sent the new proof to three colleagues including Faltings. All liked 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 suprising is 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.

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 (y^2, z, x^2) is a primitive pythagorean triple, so we have the following two cases:

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.

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

$$x^2 = 4p^4 + q^4 \text{ and } y = 2pq.$$

Hence $(2p^2, q^2, x)$ 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

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

It is not difficult to see that

$$gcd(x^2 - y^2, x^2 + y^2) = 1 \text{ or } gcd(x^2 - y^2, x^2 + y^2) = 2.$$

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 (k, k, k^2), $k \in \mathbb{Z}$.

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

$$(u + v)^4 + 6(u^2 - v^2)^2 + (u - v)^4 = 16z^2,$$

which is equivalent to

$$u^4 + v^4 = 2z^2.$$

From the previous example it follows that $(u, v, z) = (k, k, k^2)$, yielding the solutions $(x, y, z) = (k, 0, k^2)$ and $(x, y, z) = (0, k, k^2)$, $k \in \mathbb{Z}$.

Remark. Another variant of this problem was given in the second part of Problem 2 in Section 2.2.

Exercises and Problems

1. Prove that the equation

$$x^2 + xy + y^2 = 36^2$$

is not solvable in positive integers.

2. Find all pairs of positive integers such that

$$x^2 - xy + y^2 = 729$$

(Turkish Mathematical Olympiad)

3. 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)

4. Solve in integers the equation

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

5. Find all triples (x, y, z) of nonnegative integers satisfying the equation $x^4 + 14x^2y^2 + y^4 = z^2$.

6. Solve in positive integers the equation

$$3x^4 + 10x^2y^2 + 3y^4 = z^2.$$

7. Find all distinct squares a^2, b^2, c^2 which form an arithmetical sequence.

8. Solve in integers the equation

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

(Titu Andreescu)

9. Find all integral triples (x, y, z) satisfying the equation

$$x^4 - 6x^2y^2 + y^4 = z^2.$$

10. If a and b are distinct positive integers, then $2a(a^2 + 3b^2)$ is not a cube.

(Titu Andreescu)

11. Show that the equation $x^6 - y^6 = 4z^3$ is not solvable in positive integers.

(Titu Andreescu)

12. 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)

CHAPTER 3

Pell's-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* ≥ 3 *with integral coefficients. Consider the corresponding homogeneous polynomial*

$$F(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n.$$

If m *is a nonzero integer, then 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 when the degree of F is $n = 2$. In this case, if $F(x, y) = x^2 - Dy^2$, where D is a nonsquare positive integer, then for all nonzero integers m, the general Pell's equation

$$x^2 - Dy^2 = m$$

has either no solution or it has infinitely many integral solutions.

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 Cromwell's mathematician John Pell. However, there is no evidence that Pell, who

taught at the University of Amsterdam, had ever considered solving such equations. They would be more aptly called Fermat's equations, since Fermat first investigated properties of nontrivial solutions of each equations. Nevertheless, Pellian 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 were 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 well known to Archimedes.

Archimedes's *problema bovinum* took two thousand years to solve. According to a manuscript discovered in the Wolfenbüttel library in 1773 Archimedes became upset with Apollonius of Perga for criticizing one of his works. He devised a cattle problem that would involve immense calculation to solve and sent it off to Apollonius.

The smallest herd satisfying seven conditions in eight unknowns after some simplifications, lead to the Pell's equation $x^2 - 4729494y^2 = 1$. The least positive solution, for which y has 41 digits, was discovered by Carl Amthov in 1880. His solution implies that the number of white bulls has over 2×10^5 digits.

In *Arithmetica*, Diophantus asks for rational solutions to equations of the type $x^2 - dy^2 = 1$. In the case where $d = m^2 + 1$, Diophantus offered the integral solution $x = 2m^2 + 1$ and $y = 2m$. Pell's equations are 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 the 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 the Pell's equation $x^2 - 61y^2 = 1$ to be $x = 226153980$ and $y = 1766319049$.

In 1657, Fermat stated without proof that if d was positive and nonsquare, then Pell's equation 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, 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 $x^2 - 151y^2 = 1$ and $x^2 - 313y^2 = 1$. He cautioned them not to submit rational solutions for 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 was a cube and none but unity was a fourth power. He devised a method, involving solutions to Pell's equations, to determine natural numbers that were 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 square.

The Diophantine quadratic equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \qquad (3.1.1)$$

with integral coefficients a, b, c, d, e, f reduces in its main case to a Pell-type equation. Next, we will sketch the general method of reduction. The equation (3.1.1) represents a conic in the xOy Cartesian plane, therefore solving (3.1.1) in integers means finding all lattice points situated on this

conic. We will solve the 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) by $\Delta = b^2 - 4ac$. 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. If $\Delta = 0$, then the conic given by (3.1.1) is a parabola. If $2ae - bd = 0$, then the equation (3.1.1) becomes $(2ax + by + d)^2 = d^2 - 4af$ and it is not difficult to solve. In the case $2ae - bd \neq 0$, by performing the substitutions $X = 2ax + by + d$ and $Y = (4ae - 2bd)y + 4af - d^2$, the equation (3.1.1) reduces to $X^2 + Y = 0$ which is also 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, the equation (3.1.1) reduces to a general Pell-type equation

$$X^2 - DY^2 = N. \tag{3.1.2}$$

To illustrate the process described above, we will consider the equation:

$$2x^2 - 6xy + 3y^2 = -1.$$

(Berkely Math. Circle 2000-2001 Monthly Contest #4, Problem 4)

We notice that $\Delta = 12 > 0$, 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 the Pell's equation $X^2 - 3Y^2 = 1$.

3.2. Solving Pell's Equation by Elementary Methods

We will present an elementary approach to solving the Pell's equation due to Lagrange.

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 positive integers and the general solution is given by $(u_n, v_n)_{n\geq 1}$,

$$u_{n+1} = u_0u_n + Dv_0v_n, \quad v_{n+1} = v_0u_n + u_0v_n, \quad u_1 = u_0, \quad v_1 = v_0 \tag{3.2.2}$$

where (u_0, v_0) is its fundamental solution, i.e. the minimal solution different from $(1, 0)$.

Proof. First, we will prove that the 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 $l_k = [k\sqrt{D}+1]$, $k = \overline{0, c_1}$, yields $0 < l_k - k\sqrt{D} \leq 1$, $k = \overline{0, c_1}$, 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 $\left(\frac{p-1}{c_1}, \frac{p}{c_1}\right)$, $p = \overline{1, c_1}$ and $c_1 + 1$ numbers of the form $l_k - k\sqrt{D}$, $k = \overline{0, c_1}$.

From the inequalities above it follows that $|(l_i - l_j) - (j - i)\sqrt{D}| < \frac{1}{c_1}$ 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

$$|t_1^2 - Dw_1^2| < 2\frac{w_1}{c_1}\sqrt{D} + \frac{1}{c_1} < 2\sqrt{D} + 1.$$

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 the properties

$$|t_2^2 - Dw_2^2| < 2\sqrt{D} + 1 \quad \text{and} \quad |t_1 - t_2| + |w_1 - w_2| \neq 0.$$

By continuing this procedure, we find 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 with $|t_s - t_r| + |w_s - w_r| \neq 0$.

Let $t_0 = t_s t_r - Dw_s w_r$ 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, $t_0 = t_s t_r - Dw_s w_r \equiv t_s^2 - Dw_0^2 \equiv 0(\mathrm{mod}|k|)$, and it follows immediately 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 Pell's equation (3.2.1).

We show now that the pair (u_n, v_n) defined by (3.2.2) satisfies Pell's equation (3.2.1). We proceed by induction with respect to n. Clearly, (u_0, v_0) is a solution to the equation (3.2.1). If (u_n, v_n) is a solution to this equation, then

$$u_{n+1}^2 - Dv_{n+1}^2 = (u_0 u_n + Dv_0 v_n)^2 - D(v_0 u_n + u_0 v_n)^2 =$$

$$= (u_0^2 - Dv_0^2)(u_n^2 - Dv_n^2) = 1,$$

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 positive integer n,

$$u_{n-1} + v_{n-1}\sqrt{D} = (u_0 + v_0\sqrt{D})^n. \tag{3.2.4}$$

Let $z_n = u_{n-1} + v_{n-1}\sqrt{D} = (u_0 + v_0\sqrt{D})^n$ and note that $z_1 < z_2 < \cdots < z_n < \ldots$. We will prove now that all solutions to the equation (3.2.1) are of the form (3.2.4). Indeed, if the 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 $1 < (u+v\sqrt{D})(u_m - v_m\sqrt{D}) < u_0 + v_0\sqrt{D}$, and therefore $1 < (uu_m - Dvv_m) + (u_m v - uv_m)\sqrt{D} < u_0 + v_0\sqrt{D}$. On the other hand, $(uu_m - Dvv_m)^2 - D(u_m v - uv_m)^2 = (u^2 - Dv^2)(u_m^2 - Dv_m^2) = 1$, i.e. $(uu_m - Dvv_m, u_m v - uv_m)$ is a solution of (3.2.1) smaller than (u_0, v_0), in contradiction with the assumption that (u_0, v_0) was the minimal one. □

Remarks. 1) The relations (3.2.1) could be written in the following useful matrix form

$$\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} u_0 & Dv_0 \\ v_0 & u_0 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$

from where

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} u_0 & Dv_0 \\ v_0 & u_0 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}. \tag{3.2.5}$$

If

$$\begin{pmatrix} u_0 & Dv_0 \\ v_0 & u_0 \end{pmatrix}^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

then it is well-known that each of a_n, b_n, c_n, d_n is a linear combination of λ_1^n, λ_2^n, where λ_1, λ_2 are the eigenvalues of the matrix $\begin{pmatrix} u_0 & Dv_0 \\ v_0 & u_0 \end{pmatrix}$.

By using (3.2.5) after an easy computation it follows that

$$u_n = \frac{1}{2}[(u_0 + v_0\sqrt{D})^n + (u_0 - v_0\sqrt{D})^n],$$
$$v_n = \frac{1}{2\sqrt{D}}[(u_0 + v_0\sqrt{D})^n - (u_0 - v_0\sqrt{D})^n] \tag{3.2.6}$$

2) The solutions to Pell's equation given in one of the forms (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 the 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. Since this technique is not part of our presentation, we consider useful to include a table containing the fundamental solutions for $D \leq 103$.

D	u_0	v_0	D	u_0	v_0	D	u_0	v_0
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

Example 1. *Recall that* $t_m = \dfrac{m(m+1)}{2}$ *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 $(u_0, v_0) = (3, 1)$ and by formulas (3.2.6) we obtain

$$u_n = \frac{1}{2}[(3+\sqrt{8})^n + (3-\sqrt{8})^n], \quad v_n = \frac{1}{2\sqrt{8}}[(3+\sqrt{8})^n - (3-\sqrt{8})^n], \; n \geq 1.$$

It follows that

$$2x_n + 1 = u_n = \frac{1}{2}[(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}],$$

hence

$$x_n = \begin{cases} \left[\dfrac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}\right]^2, & n \text{ odd} \\ \left[\dfrac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2}\right]^2, & n \text{ even} \end{cases}$$

Remark. Every other x satisfying $t_x = y^2$ is 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)

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

$$x_n = \frac{1}{2}[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n], \quad y_n = \frac{1}{2\sqrt{2}}[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n],$$

$n \geq 1$. 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 $(m+1)$-uples 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 $n \geq 0$.

Exercises and Problems

1. Find all positive integers n such that $\dfrac{n(n+1)}{3}$ is a perfect square.

(Dorin Andrica)

2. Find all triangles having sidelenghts consecutive integers and area also an integer.

3. Consider the system of equation

$$\begin{cases} x + y = z + u \\ 2xy = zu \end{cases}$$

Find the largest value of the real constant m such that $m \leq \dfrac{x}{y}$ for any positive integral solution (x, y, z, u) of the system, with $x \geq y$.

(42^{nd} IMO Shortlist)

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 the equation (3.3.1) does not have solutions in positive integers.*

Proof. Assume that (3.3.1) has a solution (x_0, y_0), where x_0, y_0 are positive integers. Then $ax_0^2 - by_0^2 = 1$, 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 integer k_1 and k_2. The relation $k_1^2x_0^2 - k_2^2y_0^2 = 1$ can be written as $(k_1x_0 - k_2y_0)(k_1x_0 + k_2y_0) = 1$. It follows that

$$1 < k_1x_0 + k_2y_0 = k_1x_0 - k_2y_0 = 1,$$

a contradiction. □

We will call *Pell's resolvent* of (3.3.1) the equation

$$u^2 - abv^2 = 1. \tag{3.3.2}$$

Theorem 3.3.2. *Suppose that the equation (3.3.1) has solutions in positive integers and let (A, B) be its smallest solution. The general solution to (3.3.1) is $(x_n, y_n)_{n\geq 0}$, where*

$$x_n = Au_n + bBv_n, \quad y_n = Bu_n + aAv_n, \tag{3.3.3}$$

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 the equation (3.3.1). Indeed,

$$ax_n^2 - by_n^2 = a(Au_n + bBv_n)^2 - b(Bu_n + aAv_n)^2 =$$

$$= (aA^2 - bB^2)(u_n^2 - abv_n^2) = 1 \cdot 1 = 1.$$

Conversely, let (x, y) be a solution to the equation (3.3.1). Then (u, v), where $u = aAx - bBy$ and $v = Bx - Ay$, is a solution to Pell's resolvent (3.3.2). Solving the above system of linear equations with unknowns x and y yields $x = Au + bBv$ and $y = Bu + aAv$, i.e. (x, y) has the form (3.3.3). □

Example 1. *Solve in positive integers the equation*

$$6x^2 - 5y^2 = 1.$$

Solution. Its smallest solution is $(A, B) = (1, 1)$. 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 $u_0 = 11$, $v_0 = 2$.

A closed form for these solutions can be found by using the formulas (3.2.6). 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

$$3x^2 - 2y^2 = 1. \tag{3.3.4}$$

The smallest solution to this equation is $x = y = 1$. Its Pell's resolvent is $u^2 - 6v^2 = 1$, with the fundamental solution $(u_0, v_0) = (5, 2)$. From Theorem 3.3.2, the general solution to the equation (3.3.4) is given by $x_m = u_m + 2v_m$, $y_m = u_m + 3v_m$, $m \geq 0$ where

$$u_m = \frac{1}{2}[(5+2\sqrt{6})^m+(5-2\sqrt{6})^m], \quad v_m = \frac{1}{2\sqrt{2}}[(5+2\sqrt{6})^m-(5-2\sqrt{6})^m].$$

We obtain

$$n = y_m^2 - x_m^2 = (u_m + 3v_m)^2 - (u_m + 2v_m)^2 = v_m(2u_m + 5v_m), \quad m \geq 0.$$

Exercises and Problems

1. Prove that there are infinitely many quadruples (x, y, u, v) of positive integers such that $x^2 + y^2 = 6(z^2 + w^2) + 1$ with $3|x$ and $2|y$.

(Dorin Andrica)

2. a) Find all positive integers n such that $n + 1$ and $3n + 1$ are simultaneously perfect squares.

b) If $n_1 < n_2 < \cdots < n_k < \ldots$ 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 $n \geq 1$.

(40^{th} IMP Shortlist)

3.4. The Negative Pell's Equation

While the 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 value of d.

Next, we will write the solutions to the equation (3.4.1) by using our method in Section 3.3.

The equation (3.4.1) is known as the *negative Pell's equation.* From the Theorem 3.3.2 the following theorem follows:

Theorem 3.4.1. *Suppose that the equation (3.4.1) has solutions in positive integers and let (A, B) be its smallest solution. The general solution to (3.4.1) is given by $(x_n, y_n)_{n\geq 0}$ where*

$$x_n = Bu_n + dAv_n, \quad y_n = Au_n + Bv_n \tag{3.4.2}$$

and $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's equation $u^2 - dv^2 = 1$.

Remarks. 1) By using formulas (3.4.2) we obtain the solutions to the negative Pell's equation in explicit form:

$$\begin{aligned} x_n &= \frac{1}{2}(B + A\sqrt{d})(u_0 + v_0\sqrt{d})^n + \frac{1}{2}(B - A\sqrt{d})(u_0 - v_0\sqrt{d})^n \\ y_n &= \frac{1}{2}\left(A + \frac{B}{\sqrt{d}}\right)(u_0 + v_0\sqrt{d})^n + \frac{1}{2}\left(A - \frac{B}{\sqrt{d}}\right)(u_0 - v_0\sqrt{d})^n. \end{aligned} \tag{3.4.3}$$

2) 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 true.

Theorem 3.4.2. *If p is a prime, $p \equiv 1(\mathrm{mod}4)$, then the negative Pell's equation $x^2 - py^2 = -1$ is solvable in positive integers.*

Proof. Let (u_0, v_0) be the fundamental solution to the Pell's resolvent $u^2 - pv^2 = 1$. Then $u_0^2 - 1 = pv_0^2$, and u_0 cannot be even, for in this case we should have $-1 \equiv p(\mathrm{mod}4)$. Hence u_0 is odd and the numbers $u_0 - 1$ and $u_0 + 1$ have the greatest common divisor 2. Therefore $u_0 \pm 1 = 2\alpha^2$ and $u_0 \mp 1 = 2p\beta^2$, where α and β are positive integers such that $v_0 = 2\alpha\beta$. By elimination of u_0 we get $\pm 1 = \alpha^2 - p\beta^2$. Since $\beta < v_0$, we cannot have the upper sign. Thus the lower sign must be taken and the theorem is proved. □

The principal method of determining the fundamental solution to negative Pell's equation (3.4.1) also involves continued fractions. The following table contains the fundamental solution, 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

$$x_n = u_n + 2v_n, \quad y_n = u_n + v_n, \quad n \geq 1,$$

where

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

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

Then

$$x_n = \frac{1}{2}[(1 + \sqrt{2})^{2n-1} + (1 - \sqrt{2})^{2n-1}],$$

$$y_n = \frac{1}{2\sqrt{2}}[(1+\sqrt{2})^{2n-1} - (1-\sqrt{2})^{2n-1}], \quad n \geq 1.$$

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 $a_n = [\sqrt{n^2 + (n+1)^2}]$, $n \geq 1$. Prove that there are infinitely many n's such that $a_n - a_{n-1} > 1$ and $a_{n+1} - a_n = 1$.

Part 2

Solutions to Exercises and Problems

CHAPTER 1

Elementary Methods for Solving Diophantine Equations

1.1. The Decomposition Method

1. Write the equation in the form $(x+2y)(x+4y)+3(x+2y)=2$ or $(x+2y)(x+4y+3)=2$. We obtain the solutions $(0,-1)$, $(3,-2)$, $(3,-1)$, $(6,-2)$.

2. Let $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$. From the Remark in Example 2, it follows that $(1+2\alpha_1)\dots(1+2\alpha_k)=5$. Hence $k=1$ and $\alpha_1=2$. Thus $n=p^2$, where p is a prime.

3. 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 $\nu(N)$ the number of all its divisors. We have

$$s(m,n)=\nu(mn)=\nu(m)+\nu(n)-\nu(gcd(m,n))$$

with the convention $\nu(1)=0$.

If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $m = p_1^{\beta_1} \dots p_k^{\beta_k}$, where some of the exponents can be zero, it follows that

$$s(m,n) = (1+\alpha_1)\dots(1+\alpha_k) + (1+\beta_1)\dots(1+\beta_k)$$

$$-\{[1+\min(\alpha_1,\beta_1)]\dots[1+\min(\alpha_k,\beta_k)]\}.$$

4. 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).

5. 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. Write the equation in the form $(x^3+1)^2 + (x^3+1) = y^4 + 1$, or equivalently, $(2x^3+1)^2 - 4y^4 = 5$. 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. The equation is equivalent to the 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 $(-1,-1)$, $(8,-10)$, $(9,-10)$, $(9,-21)$.

8. It is convenient to note that $a-1 = x$, $b-1 = y$ and $c-1 = z$. Then we have conditions: $1 \leq x < y < z$ and $xyz | (xy+yz+zx+x+y+z)$.

The idea of a solution is to point out that we cannot have $xyz \leq xy + yz + zx + x + y + z$ 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 decreasing function in each one of variables x, y, z. By symmetry and because x, y, z are distinct numbers,

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

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

$$xy + yz + zx + x + y + z = kxyz \qquad (1)$$

where $k = 1$ or $k = 2$.

Observe that $f(3,4,5) = \dfrac{59}{60} < 1$. Thus $x \in \{1,2\}$. Also $f(2,3,4) = \dfrac{35}{24} < 2$. 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 under 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 under the form: $(y - 3)(z - 3) = 11$ we find $y - 3 = 1$, $z - 3 = 11$. Thus, it has a unique solution: $y = 4$, $z = 15$.

From *Case 2* and *Case 3* we obtain respectively: $a = 2$, $b = 4$, $c = 8$ and $a = 3$, $b = 5$, $c = 16$. These are the solutions to the problem.

9. Let x, y be lengths of the legs and let z be the one of the hypothenuse. 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, as it is never equals 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. 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).

1.2. Solving Diophantine Equations Using Inequalities

1. The equation is equivalent to $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{4}{3}$. Considering $x \leq y \leq z$, it follows that $\frac{3}{x} \geq \frac{4}{3}$, i.e. $x \leq \frac{9}{4}$. Therefore $x \in \{1,2\}$. Analysing the two cases we obtain the solutions (1,4,12), (1,6,6), (2,2,3) and all their permutations.

2. 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.

3. 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. 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 non-positive. Now observe that if (x,y) is a solution, then $(-x,-y)$ is also a solution, hence $-x$ must be non-positive. Therefore (0,0) is the only solution.

5. 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. 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. The solutions are $(\pm 1, 0)$, $(\pm 4, 3)$, $(\pm 4, 5)$. We must have $y \geq 0$. As 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. *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 $b \geq 3$, $6a \leq 2ab = a + b + 7 \Rightarrow a \leq b/5 + 7/5$, 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 Y 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. *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 either $v < xyzuv \leq 5v$ 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

$$x_1 x_2 \ldots x_n = x_1 + x_2 + \cdots + x_n.$$

10. 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

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

$$1\leq y-x$$

$$9\leq 3z$$

$$20\leq 5w.$$

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.

11. 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 with 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.

1.3. The Parametric Method

1. 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. 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 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 infinitely many.

Remark. The same argument holds for the diophantine equation

$$x^2+y^2 = z^{2n+1}+z$$

where n is a positive integer.

3. 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. 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 $k_1, k_2 \in \mathbb{Z}_+$.

5. 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.

6. Writing the equation in the equivalent form

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

shows that $\dfrac{xy}{x + y + 1}$ must be an integer. Let $x + y + 1 = u$. It follows that $\dfrac{x(u - x - 1)}{u} \in \mathbb{Z}$ or, equivalently, $\dfrac{x(x + 1)}{u} = v \in \mathbb{Z}$. 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 $w(w + 1)$.

7. *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 $\beta - \alpha | k$. 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. Note that $2002 = 3^4 + 5^4 + 6^4$. A family of solutions is given by

$$x_k = 3 \cdot 2002^k, \quad y_k = 5 \cdot 2002^k, \quad z_k = 6 \cdot 2002^k, \quad w_k = 4k+1, \quad k \in \mathbb{Z}_+$$

9. A family of solutions to the first equation is given by

$$(3m^2 + 2mn - n^2, 3m^2 - 2mn - n^2, 4mn, 3m^2 + n^2), \quad m, n \in \mathbb{Z}_+$$

A family of solutions to the second equation is

$$(m + n, m - n, 2m, 3m^2 + n^2), \quad m, n \in \mathbb{Z}_+$$

Remark. Note that the equation

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

has also infinitely many solutions. A family of 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 $a, b, c \in \mathbb{Z}$.

10. 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. 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 $3|y$. Since $z \geq 2$, $3^2|y^z$, but 3^2 does not divide $33(3x^2 + 300x + 50 \cdot 199)$, a contradiction.

2. 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. 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. 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. We show that the congruence

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

has no solution, which would 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. *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

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca)$$

the 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

$$\frac{1}{2}[(3x-3y)^2+(3x-4)^2+(3y-4)^2]\geq 0,$$

it follows that $3x+3y+4>0$, hence from (2), $3x+3y+4=1$ or $3x+3y+4=37$. The latter case is not possible since it would imply $x+y=11$ and $(3x-3y)^2+(3x-4)^2+(3y-4)^2=2$, which cannot occur simultaneously (x and y have different parities, hence $|3x-3y|\geq 3$).

Thus $3x+3y+4=1$ and $9x^2+9y^2+16-9xy-12x-12y=74$. We obtain the solutions $(-1,0)$ and $(0,-1)$.

Remark. Compare this solution to the one given to Problem 4 in 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

$$9s^2-12s+16-\frac{37}{3s+4}\in\mathbb{Z},$$

from where $3s+4|37$. We obtain $3s+4\in\{-1,1,37,-37\}$, hence $s\in\{-1,11\}$.

If $s=11$, then $p=\dfrac{11^3+1}{37}\notin\mathbb{Z}$.

If $s=-1$, then $p=0$ and we obtain the solutions $(-1,0)$, $(0,-1)$.

7. 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 solution in this case.

8. The equation is equivalent to

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

Let p be a prime divisor of $4x-1$. Then $4x^2 \equiv -1 \pmod{p}$ i.e $(2z)^2 \equiv -1 \pmod{p}$. From Little Fermat's Theorem, we obtain $(2z)^{p-1} \equiv 1 \pmod{p}$.

Hence

$$1 \equiv (2z)^{p-1} \equiv ((2z)^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

therefore $p \equiv 1 \pmod{4}$.

Thus any prime divisors of $4x - 1$ must be congruent to 1 (mod 4), hence $4x - 1 \equiv 1 \pmod 4$, a contradiction.

9. 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. 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 $d = 1$. 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

$$d^{dv^2-1} \geq 2^{2v^2-1} \geq 2^{2v-1} > v \text{ for } v = 1, 2, 3, \ldots$$

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 α and β be the largest integers such that $p^\alpha | u$ and $p^\beta | d$. Then, from (5), we have $\alpha d = \beta(u - d)$ and, hence, $\alpha > \beta$. It follows that $d|u$, 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 $d^{k-2} \geq 2^{k-2} > k$, showing that (6) is impossible for such k.

1.5. The Method of Mathematical Induction

1. For $n = 2$, we have $x_2 = y_2 = 1$. Suppose now that, for a given 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

$$\frac{x_n + y_n}{2} \text{ and } \frac{x_n - y_n}{2}$$

is odd (as their sum is odd). If, for example, $\dfrac{x_n + y_n}{2}$ is odd, then

$$\frac{x_n + 17y_n}{2} = 8y_n + \frac{x_n + y_n}{2}$$

is also odd (as a sum of an odd and an even number), 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 $\dfrac{x_n - y_n}{2}$ 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. 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. If $n = 1$, we have $x_1 = 1$, $y_1 = z_1 = 2$. Assume that there exist integers x_n, y_n, z_n such that

$$x_n^2 + y_n^2 + z_n^2 = 3^{2^n}$$

and define

$$x_{n+1} = x_n^2 + y_n^2 - z_n^2, \quad y_{n+1} = 2y_n z_n, \quad z_{n+1} = 2x_n y_n.$$

We have

$$x_{n+1}^2 + y_{n+1}^2 + z_{n+1}^2 = (x_n^2 + y_n^2 - z_n^2)^2 + 4y_n^2 z_n^2 + 4x_n^2 z_n^2 =$$

$$= (x_n^2 + y_n^2 + z_n^2)^2 = (3^{2^n})^2 = 3^{2 \cdot 2^n} = 3^{2^{n+1}}.$$

4. 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

$$\frac{1}{t_2} + \frac{1}{t_3} + \cdots + \frac{1}{t_{k-1}} + \frac{k+1}{t_k} = \frac{2}{2 \cdot 3} + \frac{2}{3 \cdot 4} + \cdots + \frac{2}{(k-1)k} + \frac{2}{k} =$$

$$= 2\left[\left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{k-1} - \frac{1}{k}\right)\right] + \frac{2}{k} = 1,$$

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 $k > 3$

$$\frac{2}{t_3}+\frac{1}{t_3}+\frac{1}{t_4}+\cdots+\frac{1}{t_{k-1}}+\frac{k+1}{t_k} = \frac{1}{3}+\frac{2}{3\cdot 4}+\frac{2}{4\cdot 5}+\cdots+\frac{2}{(k-1)k}+\frac{2}{k} =$$

$$= \frac{1}{3}+2\left[\left(\frac{1}{3}-\frac{1}{4}\right)+\left(\frac{1}{4}-\frac{1}{5}\right)+\cdots+\left(\frac{1}{k-1}-\frac{1}{k}\right)\right]+\frac{2}{k} = 1,$$

and the left-hand side is a sum of reciprocals of $(k-1)+(k+1) = 2k = n$ triangular numbers.

5. 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

$$(x_1, x_2, \ldots, x_{n-1}, x_n, x_{n+1}, x_{n+2}, x_{n+3}) =$$

$$= (a_1, a_2, \ldots, a_{n-1}, 2a_n, 2a_n, 2a_n, 2a_n)$$

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. 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

$$\frac{1}{y_0^2} = \frac{1}{x_0^2} \cdot \frac{1}{12^2} = \frac{1}{x_0^2}\left(\frac{1}{15^2} + \frac{1}{20^2}\right) = \frac{1}{15^2} \cdot \frac{1}{x_0^2} + \frac{1}{20^2}\left(\frac{1}{x_1^2} + \cdots + \frac{1}{x_s^2}\right) =$$

$$= \frac{1}{y_1^2} + \frac{1}{y_2^2} + \cdots + \frac{1}{y_s^2} + \frac{1}{y_{s+1}^2}.$$

This completes the proof by induction.

7. 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

$$ax + by = a(nu - bt) + b(at - nv) = n. \quad \square$$

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 found above is not the best possible. For example, if $m = 3$, this lower bound is $2^3+(2^3-1)\cdot[(2^3-1)^3-1]+1 = 2403$. far larger than 412 obtained in Example 4.

8. 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

$$1 = 4^2+7^2-8^2, \quad 3 = 4^2+6^2-7^2, \quad 5 = 4^2+5^2-6^2, \quad 7 = 6^2+14^2-15^2,$$

we have exhausted the case k odd as well.

9. 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

$$x_{n+1}^2+(x_{n+1}+1)^2 = (3x_n+2y_n+1)^2+(3x_n+2y_n+2)^2 = (4x_n+3y_n+2)^2,$$

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. 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 $0 < a_1 < a_2 < \dots$

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

$$2(a_1 + \cdots + a_n) \leq 2(1 + 2 + \cdots + a_n) = a_n(a_n + 1) \leq (a_{n+1} - 1)a_{n+1},$$

it is enough to show that

$$3a_{n+1}^2 - (2n+3)a_{n+1} \geq (a_{n+1} - 1)a_{n+1}.$$

The last inequality is equivalent to $a_{n+1} \geq n + 1$, which is evident. □

Without loss of generality, suppose that $0 < x_1 < x_2 < \cdots < x_m$. Then

$$x_1 \geq 1, \dots, x_m \geq m.$$

We have

$$x_1^2 + \cdots + x_m^2 = \frac{2m+1}{3}(x_1 + \cdots + x_m)$$

and by the Lemma,

$$x_1^2 + \cdots + x_{m-1}^2 \geq \frac{2m-1}{3}(x_1 + \cdots + x_{m-1}).$$

It follows that

$$x_m^2 \leq \frac{2}{3}(x_1 + \cdots + x_{m-1}) + \frac{2m+1}{3}x_m.$$

Since $x_{m-1} \leq x_m - 1$, $x_{m-2} \leq x_m - 2, \ldots, x_1 \leq x_m - (m-1)$ we also have

$$x_1 + \cdots + x_{m-1} \leq (m-1)x_m - \frac{(m-1)m}{2}.$$

Then

$$x_m^2 \leq \frac{2(m-1)}{3}x_m - \frac{(m-1)m}{3} + \frac{2m+1}{3}x_m$$

or

$$x_m^2 - \frac{4m-1}{3}x_m + \frac{(m-1)m}{3} \leq 0.$$

That is $(x_m - m)\left(x_m - \frac{m-1}{3}\right) \leq 0$, and since $x_m > \frac{m-1}{3}$, it follows that $x_m \leq m$, 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. 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 the one 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 $x_1 > x_2 > x_3 > \ldots$, in contradiction to FMID Variant 1. Thus the only solution is (0,0,0).

2. The only solution to this equation is $x = y = z = 0$. First, note that x, y, and z cannot all be odd, as then $x^2 + y^2 + z^2 - 2xyz$ would be odd and therefore non-zero. 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 $|x_1|>|x_2|>|x_3|>\ldots$, which contradicts FMID Variant 1.

3. 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, the Fermat's Little Theorem gives $u^4 \equiv 1 \pmod 5$, 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 $u_1^4 > u_2^4 > u_3^4 > \ldots$, in contradiction to FMID Variant 1.

4. 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 $x_1 > x_2 > x_3 > \ldots$, which is not possible.

5. We show, by considering the equation modulo 4 for all possibilities of a, b, c being even of odd, that it is necessary they all be even. We can

also take them to all be non-negative. 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

$$a_1^2 + b_1^2 + c_1^2 = 4a_1^2b_1^2, \text{ where } a_1 \leq a,\ b_1 \leq b,\ c_1 \leq c.$$

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) 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 a 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 recursion

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

The sequences $(a_n)_{n \geq 1}$ and $(b_n)_{n \geq 1}$ satisfy the same recursion: $x_{n+1} = 3x_n - x_{n-1}$, $x_1 = 1$, $x_2 = 2$. This recursion 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}) and (F_{2n-1}, F_{2n+1}), for $n \geq 1$.

Remarks. 1) Some variants of this problem appeared in various mathematical competitions and trainings. We will mention here the following:

Find all pairs (m, n) of positive integers having the property that $mn|(m-n)^2+1$.

(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. By 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. 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 $x|x^2+y^2+1$ and $y|x^2+y^2+1$, 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 $x^2 + y^1 + 1 = 3xy$ 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

$$(x, y, u, v) = (F_{2n-1}, F_{2n+1}, F_{2n-3}, F_{2n+3}), (F_{2n+1}, F_{2n-1}, F_{2n+3}, F_{2n-3})$$

where $n \geq 1$ and $F_{-1} = 1$.

Remark. Other variants of this problem appeared in various mathematical competitions and trainings. We will mention here the following:

Prove that there are infinitely many pairs (a, b) of positive integers such that $a|b^2 + 1$ and $b|a^2 + 1$.

(Tournament of Towns)

8. 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}) or (F_{2n+1}, F_{2n-1}), $n \geq 1$.

Hence an infinite family of solutions to our equation is given by

$$(x, y, z) = (3F_{2n+1}, 3F_{2n-1}, 3), \quad n \geq 1$$

9. 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.

10. Let $f(x, y) = x^2 + axy - y^2$. We have $f(x_1, x_2) = f(1, a) = 1$. By 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

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

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 $(x, y) = (x_k, x_{k+1})$.

11. 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 recursive 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. Also note that for $a' = b$ and $b' = 3b - a$, $(b', 3b' - a') = (a, b)$. 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

$$L_{2k+4} = L_{2k+3} + L_{2k+2} = (L_{2k+2} + L_{2k+1}) + L_{2k+2}$$

$$= (L_{2k+2} + (L_{2k+2} - L_{2k})) + L_{2k+2} = 3L_{2k+2} - L_{2k}$$

for $k \geq 0$. For $g = 5$, the Fibonacci numbers satisfy an analogous recursive 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 $k \geq 0$.

12. Assume, by way of contradiction, that we have a triple of positive integers (x_0, y_0, z_0) with $x_0 y_0 - z_0^2 = 1$ 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 $2 \leq x_0 \leq y_0$ 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 $x_1, y_1, z_1 \geq 1$. Indeed, the inequalities

$$z_0^2 = x_0 y_0 - 1 < x_0 y_0 \leq \left(\frac{x_0 + y_0}{2}\right)^2$$

implies $z_0 < \dfrac{x_0 + y_0}{2}$, i.e. $y_1 \geq 1$. Also, the inequality

$$z_0^2 = x_0 y_0 - 1 \geq x_0^2 - 1 \text{ implies } z_0 \geq x_0 - 1.$$

If $z_0 = x_0 - 1$, then $x_0(y_0 - x_0 + 2) = 2$, which is not possible since $x_0 \geq 2$ and $y_0 - x_0 + 2 \geq 2$.

If $z_0 = x_0$, then $x_0(y_0 - x_0) = 1$, which is not possible since $x_0 \geq 2$. Therefore $z_1 = z_0 - x_0 \geq 1$.

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

$$x_0 = m^2 + n^2, \quad x_0 + y_0 - 2z_0 = p^2 + q^2, \text{ and } z_0 - x_0 = mp + nq,$$

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

$$(4s)! = (2s)!(4s+1-1)(4s+1-2)\ldots(4s+1-2s) \equiv$$

$$\equiv (2s)!(-1)^{2s}(2s)! \equiv ((2s)!)^2 \pmod{p}.$$

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. Assume a non-trivial 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

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

Cleary $6|n$. If $n = 6m$, then

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

and therefore $3|c$. 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

$$2a^2 \equiv 0, 2 \pmod 8$$

$$b^2 \equiv 0, 1, 4 \pmod 8$$

$$3d^2 \equiv 0, 3, 4 \pmod 8$$

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. When $y = 1$ the left hand side is 0 hence we can't 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 $c \equiv y-1 \pmod{lcm(y-1, y+1)}$. When y is even, $lcm(y-1, y+1) = y^2-1$; when y is odd, $lcm(y-1, y+1) = \frac{1}{2}(y^2-1)$.

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 $(y-1)|10 \Rightarrow y = 2, 3, 6$, 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. 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. 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 $(x+1)|n$. Specifically, this means that $3|n$.

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. 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 cicle (1) are different.

6. 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 $3|k$, 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 $(x^2-x+xy)+(y^2-y)=y(y-1)\geq 0$, and the inequality $n\geq 2m$ follows.

From 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. When $p=2$, we have $q^n = 13$, which is impossible. Otherwise, p is odd and $5|2^p+3$. Because $n>1$, we must have $25|2^p+3^p$. 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 $5|p$. Thus $p=5$, but the equation $q^n = 2^5 + 3^5 = 5^2 \cdot 11$ has no solutions.

8. If $a=0$, then b must be a perfect square, and vice versa. Now assume 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 $(-4, -4)$, $(-6, -5)$, $(-5, -6)$, and $(0, n^2)$, $(n^2, 0)$, $(n, 1-n)$, where n is any integer.

9. 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 lest 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. 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 non-zero 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 $x = y = z$, as $gcd(x, y) = gcd(y, z) = gcd(z, x) = 1$. This means that $x = y = z = 1$ and $t = 8$. Therefore we have obtained 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) $b = 2$, $c = 1 \Rightarrow a = 5$ and we return to case (2).

ii) $b = 3,\ c = 1 \ \Rightarrow\ a = 3$. 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 thus obtained by permutations of x, y, z.

CHAPTER 2

Some Classical Diophantine Equations

2.1. Linear Diophantine Equations

1. 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

$$(x, y, z) = (1 - 5s + 5t, 1 + 3s, 1 + 2t), \quad s, t \in \mathbb{Z}.$$

2. *First step.* 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 $a | bc(x + 1)$.

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.

Second step. Any number N, $N > 2abc-ab-bc-ca$, can be expressed in the form $N = xbc + yca + zab$.

First, observe that $2abc - ab - bc - ca + 1 > 0$. Then

$$\frac{1}{abc}(2abc-ab-bc-ca+1) = 2-\frac{1}{a}-\frac{1}{b}-\frac{1}{c}+\frac{1}{abc} > 2-\frac{1}{1}-\frac{1}{2}-\frac{1}{3}+\frac{1}{abc} > 0.$$

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 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. 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. 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. 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 λ. 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 ± 1. Since Δ is clearly an integer, we must have $\Delta = \pm 1$.

6. 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 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 disjunct 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 $(y_1, y_2, \ldots, y_q)$ 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 $|y_j| \leq p$ and $|z_j| \leq p$, we see by the triangle inequality that $|x_j| = |y_j - z_j| \leq |y_j| + |z_j| \leq 2p$, so $|x_j| \leq q$; (c) also is satisfied.

2.2. Pythagorean Triples and Related Problems

1. 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. 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 with 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. 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. Applying formulas (2.2.3), the sidelengths of the triangle are of the form

$$k(m^2 - n^2), \quad 2kmn, \quad k(m^2 + n^2).$$

The condition in the problem is equivalent to

$$k^2mn(m^2 - n^2) = 2km(m + n),$$

which reduces to

$$kn(m - n) = 2.$$

A simple case analysis shows that the only possible triples (k, m, n) are (2,1,2), (1,2,3), (1,3,1), yielding the pythagorean triangles 6-8-10 and 5-12-13.

5. 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 $a = b$ could not possible 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.

6. Let a, b, c be the sidelengths 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 $m > n$, n is even, and

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

We obtain $n(m-n) = r$.

Write $r = 2^k l$, where l is an odd integer. From the relations $n = 2^k d$, $m - n = \frac{l}{d}$ it follows that a pair (m, n) is uniquely determined by a pair $\left(d, \frac{l}{d}\right)$, where d is a divisor of l and $gcd\left(d, \frac{l}{d}\right) = 1$. The number of pairs $\left(d, \frac{l}{d}\right)$ satisfying $gcd\left(d, \frac{l}{d}\right) = 1$ is $2^{\mu(l)}$, where $\mu(l)$ denotes the number of prime divisors of l.

2.3. Other Remarkable Equations

1. Assume that the equation $x^2 + xy + y^2 = 36^2$ is solvable. By 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.

2. From the general form of solutions in (2.3.11), the problem reduces to finding all positive integers k, m, n, $m > n$ such that

$$k(m^2 - mn + n^2) = 27.$$

In the following table we give all pairs (m, n) for which

$$m^2 - mn + n^2 \leq 28.$$

m	n	$m^2 - mn + n^2$
2	1	3
3	1	7
4	1	13
5	1	21
3	2	7
4	2	12
5	2	19
6	2	28
4	3	13
5	3	19
6	3	27
5	4	21
6	4	28

If $k = 1$, then $m = 6$ and $n = 3$. If $k = 9$, then $m = 2$ and $n = 1$. In both cases we obtain the solution $(x, y, z) = (27, 27, 27)$.

3. 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.

4. Without loss of generality we may assume that $gcd(x, y) = 1$. Also, note that x and y cannot have different parities. 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

$$(k(m^2+2mn-2n^2),k(2mn-m^2),k(m^2-mn+n^2))$$

and

$$(k(m^2+2mn-2n^2),k(m^2-2mn),k(m^2-mn+n^2))$$

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

5. 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

$$(x, y, z) = (2k, 0, k^2), (0, 2k, k^2) \text{ and } (x, y, z) = (l, l, 4l^2),$$

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

6. *Solution 1.* 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

$$(x, y, z) = (k, k, 4k^2), \quad k \in \mathbb{Z}_+.$$

7. 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 $(m^2 + 2mn - n^2, m^2 + n^2, |m^2 - 2mn - n^2|)$ where $m, n \in \mathbb{Z}_+$, $m > n$.

8. *Solution 1.* Multiplying 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 $x - y = 0$.

9. 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 $(x, y, z) = (k, 0, k^2)$ and $(x, y, z) = (0, k, k^2)$, $k \in \mathbb{Z}$.

10. 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 in nonzero integers.

11. 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

$$2(x^2 - y^2)[(x^2 - y^2)^2 + 3(xy)^2]$$

is a perfect cube. But this contradicts the result in Problem 10.

12. 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 with the result in Theorem 2.3.8.

CHAPTER 3

Pell's-Type Equations

3.2. Solving Pell's Equation by Elementary Methods

1. Let $\dfrac{n(n+1)}{3} = y^2$, 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

$$x_m = \frac{1}{2}[(7+2\sqrt{12})^m + (7-2\sqrt{12})^m],$$

$$y_m = \frac{1}{2\sqrt{12}}[(7+2\sqrt{12})^m - (7-2\sqrt{12})^m].$$

It follows that

$$2n_m + 1 = x_m = \frac{1}{2}[(2+\sqrt{3})^{2m} + (2-\sqrt{3})^{2m}], \quad m \geq 1,$$

hence the desired numbers are

$$n_m = \left[\frac{(2+\sqrt{3})^m - (2-\sqrt{3})^m}{2}\right]^2 = 3\left[\frac{(2+\sqrt{3})^m - (2-\sqrt{3})^m}{2\sqrt{3}}\right]^2,$$

$m \geq 1$.

Remark. Note that all n's with this property are of the form $3k^2$.

2. Let the sides be $z-1, z, z+1$. The semiperimeter s and the area A are $\dfrac{3z}{2}$ and $A = \dfrac{z\sqrt{3(z^2-4)}}{4}$, 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 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

$$x_n = \frac{1}{2}[(2+\sqrt{3})^n + (2-\sqrt{3})^n], \quad y_n = \frac{1}{2\sqrt{3}}[(2+\sqrt{3})^n - (2-\sqrt{3})^n], \; n \geq 1.$$

The sides of the triangles are $2x_n - 1, 2x_n, 2x_n + 1$ and the areas are $A = 3x_n y_n$.

3. 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 $x/y \geq 1$ 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 mase as close to $3 + 2\sqrt{2}$ as we like, so the desired 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, 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.

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

1. The equation $3r^2 - 2s^2 = 1$ has minimal solution $(A, B) = (1, 1)$ 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 $3|x$, $2|y$.

2. 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 $(u_k,v_k)_{k\geq 1}$, where

$$u_k=\frac{1}{2}[(2+\sqrt{3})^k+(2-\sqrt{3})^k],\quad v_k=\frac{1}{2\sqrt{3}}[(2+\sqrt{3})^k-(2-\sqrt{3})^k],\quad k\geq 1$$

hence

$$n_k=x_k^2-1=(u_k+v_k)^2-1=\frac{1}{6}[(2+\sqrt{3})^{2k+1}+(2-\sqrt{3})^{2k+1}-4],\quad k\geq 1.$$

b) We have

$$n_kn_{k+1}+1=\left\{\frac{1}{6}[(2+\sqrt{3})^{2k+2}+(2-\sqrt{3})^{2k+2}-8]\right\}^2,\quad k\geq 1.$$

3. 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 $u^2-5v^2=1$, satisfies the equation. In this respect we have

$$5x_n^2-y_n^2=5(3u_n+6v_n)^2-(6u_n+15v_n)^2=9u_n^2-45v_n^2=$$

$$= 9(u_n^2 - 5v_n^2) = 9 \cdot 1 = 9$$

for all $n \geq 1$.

It is clear that $u_n^2 - 5v_n^2 = 1$ implies u_n odd and v_n even for all $n \geq 1$.

It follows that the sequences $(a_n), (b_n)$, where

$$a_n = \frac{x_n - 1}{2} = \frac{3u_n - 1}{2} + 3v_n, \quad b_n = \frac{y_n}{2} + 3u_n + 15\frac{v_n}{2}, \quad n \geq 1$$

are strictly increasing and $a_n(a_n + 1)$ divides $b_n^2 + 1$.

3.4. The Negative Pell's Equation

1. The equation is equivalent to

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

Performing the substitutions $X = x + y$, $Y = x - y$, $x \geq y$, 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

$$u_n = \frac{1}{2}[(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n], \quad v_n = \frac{1}{2\sqrt{2}}[(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n].$$

We obtain

$$X_n = u_n + 2v_n = \frac{1}{2}[(1 + \sqrt{2})^{2n+1} + (1 - \sqrt{2})^{2n+1}]$$

$$Y_n = u_n + v_n = \frac{1}{2\sqrt{2}}[(1 + \sqrt{2})^{2n+1} - (1 - \sqrt{2})^{2n+1}]$$

hence

$$x_n = \frac{1}{2}(X_n + Y_n) = \frac{1}{4\sqrt{2}}[(1+\sqrt{2})^{2n+2} - (1-\sqrt{2})^{2n+2}],$$

$$y_n = \frac{1}{2}(X_n - Y_n) = \frac{1}{4\sqrt{2}}[(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n}].$$

The sequence $(P_m)_{m\geq 1}$, given by

$$P_m = \frac{1}{2\sqrt{2}}[(1+\sqrt{2})^m - (1-\sqrt{2})^m]$$

is known as *Pell's sequence*. It satisfies the recursive 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

$$(x_n, y_n) = \left(\frac{1}{2}P_{2n+2}, \frac{1}{2}P_{2n}\right), \quad (x_n, y_n) = \left(\frac{1}{2}P_{2n}, \frac{1}{2}P_{2n+2}\right), \quad n \geq 1$$

where the second solution followed by the symmetry in x and y.

2. 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 $5 < y < 2y \leq x$, as $4y^2 \leq 5y^2 - 1 = x^2$. Therefore $2(x^2+1) = 5y \cdot 2y$ divides $x!$.

3. 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

$$a_{n-1} = [\sqrt{(n-1)^2 + n^2}] = [\sqrt{y^2 - 4n}]$$

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,

$$a_{n+1} = [\sqrt{(n+1)^2 + (n+2)^2}] = [\sqrt{y^2 + 4n + 4}].$$

Since $n < y < 2n + 1$, we easily get

$y + 1 < \sqrt{y^2 + 4n + 4} < y + 2$, so $a_{n+1} - a_n = (y + 1) - y = 1$.

Bibliography

[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 probleme de matematică pentru concursuri* (Romanian), Universitatea "Babeş-Bolyai" Cluj-Napoca, 1979.

[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*, 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.

[AndreFe] Andreescu, T., Feng, Z., *Mathematical Olympiads 1999-2000, Problems and Solutions From Around the World*, Mathematical Association of America, 2001.

[AndreGe] Andreescu, T., Gelca, R., *Mathematical Olympiad Challenges*, Birkhäuser, Boston-Basel-Berlin, 2000.

[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.

[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., *Theorie des numbers*, Tome II, Paris, 1924.

[Co] Cohen, H., *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[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 în numere întregi* (Romanian), Editura Tehnică, Bucureşti, 1954.

[HaWr] Hardy, G.H., Wright, E.M., *Theory of Numbers*, 3^{rd} edition, 1954.

[Hu] Hurwitz, A., *Lectures on Number Theory*, Springer-Verlag, 1986.

[Le] 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] Sierpinski, W., *Elementary Theory of Numbers*, Polski Academic Nauk, Warsaw, 1964.

[Sie2] Sierpinski, W., *Ce ştim şi ce nu ştim despre numerele prime* (Romanian), Editura Ştiinţifică, Bucureşti, 1966.

[Sie3] Sierpinski, 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.

Index

.....

.....

.....

.....

Narodne novine d.d., Zagreb – (123) 110735
Oznaka za narudžbu: **UT-XI/11-8**