PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
MOHAMED BOUDIAF UNIVERSITY-M'SILA
Faculty of Mathematics and Computer Science
Department of Mathematics

N° d'ordre :.....

THESIS

Presented to obtain a
MASTER'S DEGREE IN MATHEMATICS

Specialty
Mathematics

Option
Algebra and Discrete Mathematics

By

ACHOUR ACHWAQ and AOUINA NOURELHOUDA

Titled

Diophantine Equations

Defended on .../.../.... in front of the jury composed of :

Abdelmadjid Boudaoud	Prof	University of M'sila	Chair
Yahia Zouareg	M.C.B	E.N.S.H	Supervisor
Abdelkrim Merzougui	Prof	University of M'sila	Co-supervisor
Mourad Yettou	M.C.A	University of M'sila	Examiner

University year : 2024/2025

2025

اهداء

أولاً وقبل كل شيء الحمد والشكر لله عز وجل الذي سهّل لنا هذا العمل سهَّل لنا إنجاز هذا العمل وأعطانا قوة الصبر على إتمامه لإتمامه.

الى العزيز الذي حملت اسمه فخرا والى من كلله الله بالهيبة والوقار الى من حصد الاشواك عن دربي وزرع ليا الراحة بدلا منها الى ابي لم يحني ظهر ابي ما كان يحمله لكن ليحملني من اجلي انحدب وكنت احجب عن نفسي مطالبها فكان يكشف عما اشتهي الحجب فشكرا لكونك ابي والى من علمتني الاخلاق قبل ان اتعلمها الى الجسر الصاعد بي الى الجنة الى اليد الخفية التي ازالت عن طريقي العقبات ومن ضلت دعواتها تحمل اسمي ليلا ونهارا امي محبوبتي وملهمتي الى من وهبني الله نعمة وجودهم الى مصدر قوتي و ارضي الصلبة وجدار قلبي المتين اخوتي واخواتي والى من ان ضاقت بي الدنيا وسعت بخطاهم وان سقطت كانوا اول من رفعوني بكلماتهم الى من رافقني بالقلب قبل الدرب اصحابي واحبتي ها انا اليوم طويت صفحة من التعب وسجلت في تاريخي فخرا لا ينسى لم اعد أتساءل عن ملامح الوصول فقد رايتها في عيوني تلاشت غيوم التعب وابتسم الأفق بعد عتمة الانتظار هاهي الخطى التي كانت تتعثر أحيانا قد وجدت مستقرها في قمة الإنجاز وبين طيات الطريق تنفست سلاما وفرحا وامتنانا واخر دعواهم ان الحمد لله رب العالمين

2025

تشكرات

أولا وقبل كل شيئ الحمد والشكر لله عز وجل
الذي سهل لنا هذا العمل وسهل لنا انجاز هذا العمل
وأعطانا قوة الصبر على اتمامهلاتمامه
نود أن نعبر عن إمتناننا العميق والصادق لمؤطرنا
الأستاذ: زوارق يحيى
أستاذ الرياضيات في المدرسة الوطنية العليا للري
لمساعدته القيمة وحسن توجيهه.
لقد كان امتيازا وشرفا عظيما أن نعمل تحت اشرافه
نحن ممتنين للغاية لما قدمه لنا .
كما نود أن نشكر أعضاء لجنة التحكيم
السيد عبد المجيد بوداود رئيسا
والسيد مراد يطو بصفته ممتحنا
والسيد عبد الكريم مرزوقي نائبا لمؤطرنا
جزيل الشكر

Table of contents

1 Preliminaries **7**

1.1 Divisibility and Prime Numbers 7

1.2 Euclidean Algorithm 9

1.3 Bézouts Identity 10

1.4 Congrunces 12

1.5 Euler's totient funtion 13

2 Diophantine Equations **15**

2.1 Linear Diophantine Equations 16

2.2 Pythagorean triples 20

2.3 Fermat's Last theorem 29

2.4 Pells equation 32

3 Applications of Diophantine Equations **39**

3.1 RSA encryption 39

3.1.1 Public Key Cryptography 39

3.1.2 RSA 40

3.1.3 Key Generation 40

3.1.4 Encryption 41

3.1.5 Decryption 42

3.2 Elliptic Curve Cryptography (ECC) 46

3.2.1 The Basic Principle of Elliptic Curve Cryptography (ECC) 48

3.2.2 The Comparison Between ECC and RSA Cryptography 50

Bibliography **53**

Introduction

The most well-known work of Diophantus, the *founder of algebra*, is Arithmetica, which deals with the theory of numbers and the solution of algebraic problems. But practically little is known about his existence, and there has been significant discussion about the exact years he lived.

In the magnificent metropolis of Alexandria, Diophantus carried out his duties. Alexandria was the epicenter of mathematical education at this time. The Silver Age, often referred to as the Later Alexandrian Age, was the time frame in Alexandria that spanned 250 BC to 350 CE. Many of the concepts that contributed to our current understanding of mathematics were being discovered at this period by mathematicians. The period is referred to as silver because it followed the Golden Age, which saw significant advancements in the field of mathematics. This Golden Age encompasses the lifetime of Euclid. The axiomatic approaches of modern mathematics were inspired by the caliber of mathematics of this era.

Although Diophantus lived during the Silver Age, it is difficult to determine when precise years he was alive. Diophantus himself made few allusions to the work of other mathematicians, despite the fact that his work has been frequently cited. This makes it more challenging to pinpoint the period in which he lived.

We can infer that Diophantus lived after 150 bce because he did mention Hypsicles, who was active prior to that time, on the concept of a polygonal number. Conversely, around 350 CE, Theon, a mathematician from Alexandria as well, cited Diophantus's work. According to the majority of historians, Diophantus completed the most of his work circa 250 CE. Metrodorus's likely fake collection of riddles, composed circa 500 CE, contains the most information concerning Diophantus's life. Among these is the following:
He spent one-sixth of his life as a boy, got married after one-seventh, grew a beard after one-twelfth, and had a son five years later. The son lived to be half his father's age, and the father passed away four years after the son.

In Greek algebra, Diophantus was the first to use symbols. In addition to using symbols for

powers and algebraic operations, he also employed an arithmetic symbol for an unknown amount. The findings of arithmetic in the theory of numbers, such as the inability to express any integer of the type $8n + 7$ as the sum of three squares, make it noteworthy.

The 150 questions in Arithmetica provide approximations for solutions to equations up to degree three. Equations that deal with indeterminate equations are also found in Arithmetica. The theory of numbers is the subject of these equations. The surviving Greek manuscripts only contain six of the thirteen books that are thought to have made up the original Arithmetica. The others are regarded as lost pieces. These books might have been destroyed in a fire that broke out shortly after Diophantus completed Arithmetica.

We refer to an equation of the form

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

where f is an $n-$variable function with $n \geq 2$ as a Diophantine equation. It is an algebraic Diophantine equation if f is a polynomial with integral coefficients.
A solution to equation (1) is an n-uple $(x_1^0,\ x_2^0,\ ...,\ x_n^0) \in \mathbb{Z}^n$ that satisfies (1). Solvable equations are those that have one or more solutions.

Three fundamental problems with a Diophantine equation emerge:

- Problem 1: Can the equation be solved?
- Problem 2: Is there a finite or infinite number of solutions, assuming it can be solved?
- Problem 3: Find all of the solutions if it can be solved.

Chinese mathematicians in the third century and Arab mathematicians in the eighth through twelfth centuries carried on Diophantus's work on equations of type (1), while Fermat, Euler, Lagrange, Gauss, and numerous others advanced it. In modern mathematics, this subject is still very important.

Our work contains three chapters:

• Chapter 1 is dedicated to a review of the fundamental concepts related to Diophantine equations.

• In Chapter 2, we present an overview of Diophantine equations, highlighting their historical significance, various classifications, and common solution techniques.

• Chapter 3 presents some applications of Diophantine equations in the context of contemporary mathematics.

Chapter 1

Preliminaries

1.1. Divisibility and Prime Numbers

Definition 1.1. *Let $a,\ b \in \mathbb{Z} \times \mathbb{Z}^*$, we say that b divides a (or that a is divisible by b) and compose $b \mid a$ if there exists an integer $m \in \mathbb{Z}$ such that:*

$$a = b \cdot m.$$

b is referred to as a divisor of a in this instance, and a is referred to as a multiple of b.

Remark 1.1. *If b is not able to divide a, we compose $b \nmid a$.*

Definition 1.2. *If $n > 1$ and the only positive divisors of n are 1 and n, then n is a prime integer. n is referred to as composite if $n > 1$ and n is not prime.*

Remark 1.2. *: Two integers $a,\ b$ are said to be co prime if $\gcd(a,\ b) = 1$.*

Notation 1.1. *Prime numbers are generally denoted by p.*

Proposition 1.1. *Let $a,\ b,\ n,\ a_1,\ \ldots,\ a_n$ be integers that are positive and p be an integer that is prime. Then:*

1. *$p \mid a_1 \ldots a_n \Rightarrow p \mid a_i$ for some $i \in \{1, \ldots, n\}$.*
2. *$p \mid a^n \Rightarrow p \mid a$.*

Theorem 1.1. *[The Fundamental Theorem of Arithmetic[3]] Every integer $n \geq 2$ is either a prime number or a product of prime numbers:*

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

where p_i are prime numbers and α_i are positive integers $(i = 1,\ \ldots,\ r)$.

Check this proof. It is assumed that S is the set of composite integers ≥ 2 that cannot be expressed as a product of prime factors. has a smallest element, denoted m.
Since m is not a prime number, with $a > 1$ and $b > 1$, we obtain $m = ab$. It follows that $a,\ b \notin S$ since $a < m$ and $b < m$, and m is the smallest element of S. a and b can therefore be expressed as products of prime factors, and thus $m = ab$ can also be written as a product of prime factors, leading to a contradiction. Consequently, we have proven that $S = \emptyset$. □

Corollary 1.1. *[6] Let $n,\ m \in \mathbb{Z}$ with $n, m \geq 2$. According to Theorem 1.1, can be written in the form:*

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \qquad m = \prod_{i=1}^{r} p_i^{\beta_i},$$

we have

1. $\gcd(n, m) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$.
2. *Let $d \in \mathbb{N}^*$. Then we find: $d \mid n \iff d = \prod_{i=1}^{r} p_i^{s_i}$ with $0 \leq s_i \leq \alpha_i$.*
3. *Suppose that $\gcd(n,\ m) = 1$. Then every divisor d of mn can be written as $d = ab$ with $a \mid m,\ b \mid n$, and $\gcd(a,\ b) = 1$.*

Theorem 1.2. *Let $a,\ b$, and c be integers, where $a \neq 0$. Then*

1. *If $a \mid b$ and $b \mid a$, then $a = \pm b$.*
2. *If $a \mid b$ and $a \mid c$, then $a \mid (b \pm c)$.*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
4. *If $a \mid b$, then $a \mid kb$ for all integers k.*
5. *For any nonzero integer k, $a \mid b$ if and only if $ka \mid kb$.*
6. *If $a \mid b$ and $a \mid c$, then $a \mid kb + \ell c$ whenever k and ℓ are integers.*

1.2. Euclidean Algorithm

The Euclidean algorithm is an efficient method for determining the gcd of two integers.

$$\gcd(a,\ b) = \gcd(b,\ r),$$

if $a = bq + r$ for integers $a,\ b,\ q$, and r. The proof of this property is immediate. The algorithm works as follows. Suppose we are given two positive integers a and b such that $a > b$. We perform the Euclidean division of a by b :

$$a = bq_0 + r_0,$$

and according to the previous property, we are reduced to calculating the gcd of the integers b and r_0. Two cases then arise: if $r_0 = 0$, the sought gcd is b. Otherwise, we perform the Euclidean division of b by r_0 :

$$b = r_0q_1 + r_1,$$

and the sought gcd is that of r_0 and r_1. If $r_1 = 0$, we are done. Otherwise, we continue... The r_i form a strictly decreasing sequence of non-negative integers (by the properties of Euclidean division). This sequence cannot be infinite, which shows that the algorithm must terminate. The description of this algorithm proves that it automatically stops with a zero remainder. At this point, the previous remainder provides the sought gcd . Let a and b be two positive integers, we set $r_0 = a$ and $r_1 = b$, and as long as $r_i > 0$, we perform the following successive Euclidean divisions:

$$\begin{aligned}
&\text{of } a \text{ by } b: && r_0 = r_1q_1 + r_2,\ \text{with } 0 \le r_2 < r_1.\\
&\text{of } b \text{ by } r_1: && r_1 = r_2q_2 + r_3,\ \text{with } 0 \le r_3 < r_2.\\
& && \vdots\\
&\text{of } r_{n-2} \text{ by } r_{n-1}: && r_{n-2} = r_{n-1}q_{n-1} + r_n,\ \text{with } 0 \le r_n < r_{n-1}.\\
&\text{of } r_{n-1} \text{ by } r_n: && r_{n-1} = r_nq_n + r_{n+1},\ \text{with } 0 \le r_{n+1} \le r_n \text{ and } r_{n+1} = 0.
\end{aligned}$$

Proposition 1.2. *We have* $\gcd(a,\ b) = r_n$*, i.e., the* gcd *of* a *and* b *is the last non-zero remainder in this series of Euclidean divisions.*

Proof. The sequence of remainders: $r_0, r_1, r_2, \ldots, r_n$ is a strictly decreasing sequence in N because $r_0 > r_1 > r_2 > \cdots > r_n$. This sequence is therefore finite. There exists then n such that $r_{n+1} = 0$. Let us show that $\gcd(a,\ b) = \gcd(b,\ r_0)$.

Let $D = \gcd(a,\ b)$ and $d = \gcd(b,\ r_0)$. We have D divides a and b, so D divides $a - bq_0 = r_0$, hence D divides b and r_0, so: $D \leq d$. Another side we have d divides b and r_0, so d divides $bq_0 + r_0 = a$, hence d divides a and b, so: $d \leq D$.

From these two inequalities, we deduce that $D = d : \gcd(a,\ b) = \gcd(b,\ r_0)$. Step by step, we deduce that:

$$\gcd(a,\ b) = \gcd(b,\ r_0) = \gcd(r_0,\ r_1) = \cdots = \gcd(r_{n-1},\ r_n) = r_n.$$

But r_n divides r_{n-1}, so $\gcd(r_{n-1},\ r_n) = r_n$ because $r_{n+1} = 0$. □

Example 1.1. *Take $a = 87$ and $b = 19$. Then*

$$\begin{aligned} 87 &= 19 \times 4 + 11, \\ 19 &= 11 \times 1 + 8, \\ 11 &= 8 \times 1 + 3, \\ 8 &= 3 \times 2 + 2, \\ 3 &= 2 \times 1 + 1, \\ 2 &= 1 \times 2 + 0. \end{aligned}$$

Thus, $\gcd(a, b) = 1$. Consequently, a and b are coprime.

1.3. Bézouts Identity

Theorem 1.3. *[26] If a and b are positive integers, then there exist integers s and t such that*

$$\gcd(a,\ b) = sa + tb.$$

Definition 1.3. *If a and b are positive integers, then the integers s and t such that $\gcd(a, b) = sa+tb$ are called Bézout coefficients of a and b (named after Etienne Bézout, an eighteenth-century French mathematician). Similarly, the equation $\gcd(a, b) = sa + tb$ is called Bézouts identity*

Example 1.2. *Express $\gcd(13,\ 11) = 1$ as a linear combination of 13 and 11 by working backwards through the steps of the Euclidean algorithm.*
To show that $\gcd(13,\ 11) = 1$, the Euclidean algorithm uses these divisions:

$$13 = 11 \times 1 + 2,$$
$$11 = 2 \times 5 + 1,$$
$$2 = 2 \times 1 + 0.$$

Using the next-to-last division (the third division), we can express $\gcd(13,\ 11) = 1$, as a linear combination of 2 and 1. We find that

$$1 = 11 - 5 \times 2.$$

The second division tells us that

$$2 = 13 - 1 \times 11.$$

We replace the expression for 2 in the following formula to express 1 as a linear combination of 11 and 13:.

$$1 = 11 - 5 \times 2 = 11 - 5 \times (13 - 1 \times 11) = 6 \times 11 - 5 \times 13.$$

So we have expressed the greatest common divinator of 13 and 11 as a linear combination of these two values:

$$1 = 6 \times 11 - 5 \times 13.$$

This means we have found coefficients $s = -5$ and $t = 6$ such that:

$$1 = -5 \times 13 + 6 \times 11.$$

is the formula we use to represent the greatest common divisor as a linear combination of the original numbers.

1.4. Congrunces

Congruences are a new concept in partitioning, invented by Gauss in 1801. In this section, we'll concentrate on a definition and some principles of congruence.

Definition 1.4. *If $n \in \mathbb{N}$, then we say that a is congruent to b modulo n if n divides $(a - b)$, denoted by $a \equiv b \pmod{n}$. The integer n is the modulus of the congruence.*

Remark 1.3. *When $n \nmid (a - b)$, we say that a is incongruent to b modulo n, or that a is not congruent to b modulo n. And in this case, we write $a \not\equiv b \pmod{n}$. and we say that a and b are incongruent modulo n, or that a is not congruent to b modulo n.*

Example 1.3. *Prove that $2^{32} + 1$ is divisible by 641. We have,*

$$2^{16} \equiv 154 \pmod{641},$$

we can square both sides to get:

$$2^{32} \equiv (154)^2 \pmod{641}.$$

Now, we compute:

$$(154)^2 + 1 = 23717.$$

Since

$$23717 \equiv 0 \pmod{641},$$

it follows that 23717 is divisible by 641. Therefore,

$$641 \mid (2^{32} + 1).$$

Thus, we conclude:

$$2^{32} + 1 \equiv 0 \pmod{641}.$$

Theorem 1.4. *Let $n \in \mathbb{N}$.*

1. *The integers a and b are congruent modulo n if and only if there is an integer k such that*

$$a = b + kn.$$

2. *For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b have the same nonnegative remainder when divided by n.*

Theorem 1.5. *Let $n,\ m \in \mathbb{N}$. For each $a,\ b,\ c,\ d \in \mathbb{Z}$, each of the following holds.*

1. $a \equiv a \pmod{n}$, *called the reflexive property.*
2. *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$, *called the symmetric property.*
3. *If* $a \equiv b \pmod{n}$, *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$, *called the transitive property.*
4. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a \pm c \equiv b \pm d \pmod{n}$.
5. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $ac \equiv bd \pmod{n}$.
6. *If* $a \equiv b \pmod{n}$, *then* $am \equiv bm \pmod{n}$.
7. *If* $a \equiv b \pmod{n}$, *then* $a^m \equiv b^m \pmod{n}$.
8. *If* $a \equiv b \pmod{n}$ *and* m *divides* n, *then* $a \equiv b \pmod{m}$.
9. *If* $a \equiv b \pmod{n}$, *then* $a + n \equiv b \pmod{n}$, *or* $a \equiv b + n \pmod{n}$.
10. *If* $a \equiv b \pmod{n}$, *then* $a \equiv b \pm nk \pmod{n}$ *because* $nk \equiv 0 \pmod{n}$

1.5. Euler's totient funtion

Euler's phi function plays an essential role in the RSA encryption system described in Chapter 3. Before presenting the definition of the Euler phi function.

Definition 1.5. *Whatever n is a positive integer. The Euler phi function $\varphi(n)$ is called the number of non-negative integers a smaller than n that are prime to n*

$$\varphi(n) = |\{1 \leq a < n \mid \gcd(a,\ n) = 1\}|.$$

Example 1.4. *For example:*

- $\varphi(4) = |\{1 \leq a < 4 \mid \gcd(a,\ 4) = 1\}| = |\{1,\ 3\}| = 2.$
- $\varphi(5) = |\{1 \leq a < 5 \mid \gcd(a,\ 5) = 1\}| = |\{1,\ 2,\ 3,\ 4\}| = 4.$

Remark 1.4. *It is easy to see that* $\varphi(1) = 1$, *and that* $\varphi(p) = p - 1$ *for any prime* p.

Theorem 1.6. *Eulers totient has the following properties:*

- *If* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *where* p_i *are distinct primes, then*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

- $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ *for prime* p *and* $\alpha \geq 1$.
- $\varphi(mn) = \varphi(m)\varphi(n)$ *if* $\gcd(m, n) = 1$.
- *If* $a \mid b$, *then* $\varphi(a) \mid \varphi(b)$.

Proof. See, [3] Pp 27-28. □

Example 1.5. *For example:*

- $\varphi(5) = 5 \cdot \left(1 - \frac{1}{5}\right) = 5 - 1 = 4.$
- $\varphi(9) = \varphi(3^2) = 3^2 \cdot \left(1 - \frac{1}{3}\right) = 3^2 - 3 = 6.$
- $\phi(45) = \phi(3^2 \times 5) = 3^2 \cdot 5 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 3^2 \cdot \left(1 - \frac{1}{3}\right) \cdot 5 \cdot \left(1 - \frac{1}{5}\right) = \phi(3^2) \times \phi(5) = 24$
- $\phi(3600) = \phi(3^2) \cdot \phi(2^4) \cdot \phi(5^2) = (3^2 - 3) \cdot (2^4 - 2^3) \cdot (5^2 - 5) = 960.$

Chapter 2

Diophantine Equations

Diophantine equations are polynomial equations where the number of equations is fewer than the number of unknowns, potentially leading to an infinite number of integer solutions. These equations are named after Diophantus of Alexandria, who lived between the 3rd and 4th centuries CE and was the first to systematically study them in his work *Arithmetica*, where he explored problems such as $2x^2 - y^2 = 1$. Before Diophantus, the Pythagoreans and mathematicians like Heron of Alexandria worked on similar problems.

In the East, Indian and Chinese mathematicians made significant contributions, with Brahmagupta in the 7th century providing a general solution to Diophantine equations with two unknowns. During the Islamic Golden Age, Al-Khwarizmi addressed these problems in his book Al-Jabr wa-l-Muqabala, while Abu Kamil Shuja ibn Aslam explored problems with unique or multiple integer solutions. Al-Karaji worked on systems of linear equations and quadratic Diophantine equations, and Al-Samaw'al studied cubic equations.

Scholars like Abu Ja'far al-Khazin and Abu al-Jud ibn al-Laith focused on right-angled triangles with integer sides, proving that integers x, y, z satisfying $x^2+y^2 = z^2$ can be expressed using specific formulas. They also explored more complex equations like $x^4 + y^2 = z^2$.

One of the most famous problems in this field is Fermat's Last Theorem, which states that the equation $x^n + y^n = z^n$ has no non-trivial integer solutions for $n > 2$. This theorem was finally proven by Andrew Wiles in 1994.

Additionally, Pell's equation $x^2 - dy^2 = 1$, where d is not a perfect square, was studied, and mathematicians like Lagrange and Kronecker developed methods to find minimal solutions. Mordell's equation $y^2 - x^3 = k$, an example of an elliptic curve, has integer solutions that depend on the value of the constant k.

This brief overview highlights the evolution of the study of Diophantine equations through the ages, from their ancient beginnings to modern mathematical achievements.

2.1. Linear Diophantine Equations

An equation of the type

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

is called a linear Diophantine equation, where $a_1,\ a_2,\ \ldots,\ a_n,\ b$ are fixed integers. The assumption is that $n \geq 1$ and that $a_1,\ \ldots,\ a_n$ are all non-zero.

The example $n = 2$ is where we start. The following is the primary finding with regard to linear Diophantine equations.

Theorem 2.1. *[2] Let $a,\ b,\ c$ be integers, a and b nonzero. Examine the Diophantine equation in linear form.*

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

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

2. *If $(x, y) = (x_0, y_0)$ is s a particular solution to (2.1.2), then each integer solution has the following form:*

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

   where t is an integer.

3. *If $c = \gcd(a,\ b)$ and $|a|$ or $|b|$ is not equal to 1, then a particular solution $(x, y) = (x_0, y_0)$ to (2.1.3) can be discovered in a way that $|x_0| < |b|$ and $|y_0| < |a|$.*

Proof. 1. It is obvious that the equation cannot be solved if d does not divide c. If d divides c, then, dividing both sides of (2.1.2) by $\frac{d}{c}$, it is sufficient to demonstrate that d is a linear combination with a and b as its integer coefficients. We employ the Euclidean algorithm for this.

Suppose $a = bq + r$ for integers $a,\ b,\ r$, and q. All common divisors of a and b are easily observable to be common divisors of b and r, and conversely. Clearly, if $b \mid a$, then $\gcd(a,\ b) = b$. In general, we have $\gcd(a,\ b) = \gcd(b,\ r)$. The gcd of two numbers can be easily calculated using these data. To be systematic, we write $a = r_{-1}$ and $b = r_0$(assumed positive and $a \geq b$)

:

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

As the remainders get less and smaller, this division process eventually comes to an end

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

and still be nonnegative. Stated differently, some r_n divides the preceding r_{n-1} (and leaves a remainder $r_{n+1} = 0$.)

We obtain

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

From these,

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

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

Recursively define the numbers x_k and y_k by

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

In each of these steps, $r_k = a x_k + b y_k$. In particular,

$$\gcd(a,\ b) = r_n = a x_n + b y_n.$$

It can be checked that (x_i) and (y_i) alternate in sign, $|x_{n+1}| = b/\gcd(a,\ b)$, and $|y_{n+1}| =$

$a/\gcd(a,\ b)$. It follows that $|x_n| < b$ and $|y_n| < a$ unless $n = 0$ and $q_0 = 1$, that is, unless $a = b = 1$.

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

3. Part 1 has already demonstrated the outcome.

□

Example 2.1. *Solve the equation*
$$6x + 9y = 7, \tag{2.1.4}$$
we have $6x + 9y \equiv 0 \pmod 3$, *and* $7 \equiv 1 \pmod 3$, *then* $6x + 9y \not\equiv 7 \pmod 3$. *Therefore, the solution set of the equation (2.1.4) is* $S = \emptyset$.

Example 2.2. *Solve the equation:*
$$4x + 10y = 16, \tag{2.1.5}$$
we have $gcd(4, 10) = 2$ *and* $2 \mid 16$, *so*
$$4x + 10y = 16 \iff 2x + 5y = 8.$$
We have
$$5 = 2(2) + 1 \Rightarrow 5(1) + 2(-2) = 1.$$
So,
$$\begin{cases} 2x + 5y = 8, \cdots\cdots\ (1) \\ 2(-16) + 5(8) = 8 \cdots\cdots\ (2) \end{cases}$$
By subtracting equation (1) *from* (2), *we get*
$$2(x + 16) + 5(y - 8) = 0,$$
implies
$$2(x + 16) = 5(8 - y), \tag{2.1.6}$$

we have

$$2 \mid 5(8-y) \text{ and } \gcd(2,5) = 1 \Rightarrow 2 \mid (8-y)$$
$$\Rightarrow 8 - y = 2k \quad \Rightarrow \boxed{y = 8 - 2k.}$$

By substituting into equation (2.1.6), we find

$$2(x+16) = 5(8-8+2k) \Rightarrow \boxed{x = -16 + 5k.}$$

Therefore, the solution set of the equation (2.1.5) is $S = \{(16+5k,\ 8-2k) \mid k \in \mathbb{Z}\}$.

The following is the main finding with reference to the generic linear Diophantine equation (2.1.1):

Theorem 2.2. *[2] The equation (2.1.1) is solvable if and only if*

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

Selecting $n-1$ *solutions that are individually an integer linear combination of those* $n-1$ *solutions is possible in the situation of solvability.*

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

In fact, we must demonstrate that $\gcd(x_1,\ x_2,\ \ldots,\ x_n)$ has integer coefficients and is a linear combination of $x_1,\ x_2,\ \ldots,\ x_n$. For $n = 2$ this follows from theorem 2.1. Because

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

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

Example 2.3. *Solve the equation*

$$2x + 3y + 5z = 4.$$

Solution: *Reduce the equation modulo 5:*

$$2x + 3y \equiv 4 \pmod 5.$$

Express the equation as:

$$2x + 3y = 4 + 5s, \quad s \in \mathbb{Z}.$$

A particular solution is:

$$x = 2 + 3s, \quad y = 0 - 2s.$$

Applying the general linear Diophantine equation solution:

$$x = 2 + 3s + 3t, y = -2s - 2t, \quad t \in \mathbb{Z}.$$

Substitute x and y into $2x + 3y + 5z = 4$:

$$\begin{aligned} 2(2 + 3s + 3t) + 3(-2s - 2t) + 5z &= 4, \\ 4 + 6s + 6t - 6s - 6t + 5z &= 4, \\ 4 + 5z = 4 \implies 5z = 0 &\implies z = 0. \end{aligned}$$

All integer solutions are given by:

$$(x, y, z) = (2 + 3s + 3t, -2s - 2t, 0), \quad s, t \in \mathbb{Z}.$$

Although this equation involves different coefficients and yields a simpler solution for z, it retains the same structural form as the previous example. The three main processes substitution, parametrization, and modulo reduction are applied in the same systematic way, preserving the overall methodology.

2.2. Pythagorean triples

Among the most well-known Diophantine formulas is the Pythagorean equation

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

Even the ancient Babylonians were aware of this equation, which Pythagoras studied in great detail in relation to right triangles with all integer side lengths. Note first that if the triple of integers (x_0, y_0, z_0) satisfies equation (2.2.1), then all triples of the form (kx_0, ky_0, kz_0), $k \in \mathbb{Z}$, also satisfy (2.2.1). That is why it is sufficient to find solutions (x, y, z) to (2.2.1) with $\gcd(x, y, z) = 1$. This

is equivalent to the fact that x, y, z are pairwise relatively prime. A solution (x_0, y_0, z_0) to (2.2.1) with x_0, y_0, z_0 pairwise relatively prime is called a *primitive solution*. It is clear that in a primitive solution exactly one of x_0 and y_0 is even.

Theorem 2.3. *The general form of any primitive solution to equation (2.2.1) with y a positive integer is a triple (x, y, z), where*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{2.2.2}$$

with $m > n$, $m + n$ odd, and m and n coprime positive integers.

Proof. The integers x and y cannot both be odd, for otherwise

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4,$$

a paradox. Thus, one of the integers x and y is exactly even. Who it is

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

demonstrates that y is even and that the triple provided by (2.2.2) is, in fact, a solution to the equation (2.2.1). We can suppose that m is odd and n is even without losing generality because x must be odd.

Moreover, if $\gcd(m^2 - n^2, 2mn, m^2 + n^2) = d \geq 2$, then d divides

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

and d divides

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

It follows that $d = 2$ since m and n are approximately prime. In contrast to m odd and n even, $m^2 + n^2$ is even. Therefore, the solution (2.2.2) is primitive since $d = 1$.

Let (x, y, z), on the other hand, be a primitive solution to (2.2.1) where $y = 2a$. Hence, the integers $z + x$ and $z - x$ are even since x and z are odd. Assume that $z - x = 2c$ and $z + x = 2b$. Since z and x would have a nontrivial common divisor if b and c were not relatively prime, we may conclude that they are. $a^2 = bc$, however, since $4a^2 = y^2 = z^2 - x^2 = (z + x)(z - x) = 4bc$.

Given that b and c are substantially prime, for some positive integers m and n, $b = m^2$ and $c = n^2$. It is determined that $m + n$ is odd and

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

Primitive is a triple (x, y, z) of the form (2.2.2). We give values $2, 3, 4, \ldots$ to m in order to list all primitive solutions to equation (2.2.1). For each of these values, we take those integers$n$ that are smaller than m and relatively prime to m. $\square$

The first 20 primitive answers specified using the aforementioned rule are shown in the table below. The area is mentioned in the final column.

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 2.1. *The general integral solution to (2.2.1) is given by*

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2), \tag{2.2.3}$$

where $k, m, n \in \mathbb{Z}$. The immediate extension to equation (2.2.1) is

$$x^2 + y^2 + z^2 = t^2. \tag{2.2.4}$$

The length of a rectangular box's diagonal and its dimensions are represented by the affirmative answers (x, y, z, t) to (2.2.4). Our goal is to identify any scenario where these elements are all integers.

Theorem 2.4. *All the solutions to equation (2.2.4) in positive integers $x,\ y,\ z,\ t$ with $y,\ z$ even are given by*

$$x = \frac{l^2 + m^2 - n^2}{n}, \quad y = 2l, \quad z = 2m, \quad t = \frac{l^2 + m^2 + n^2}{n}, \tag{2.2.5}$$

where $l,\ m$ are arbitrary positive integers and n is any divisor of $l^2 + m^2$ less than $\sqrt{l^2 + m^2}$. Every solution is obtained exactly once in this way.

Proof. The identity

$$\left(\frac{l^2 + m^2 - n^2}{n}\right)^2 + (2l)^2 + (2m)^2 = \left(\frac{l^2 + m^2 + n^2}{n}\right)^2$$

demonstrates that y and z are even and that the quadruple in (2.2.5) is a solution to equation (2.2.4). Conversely, keep in mind that $t^2 \equiv 2, 3 \pmod 4$, a contradiction, requires that at least two of the integers x, y, z be even.

Assume that for certain positive integers l and m, $y = 2l,\ z = 2m$. When $t - x = u$ is set, we get

$$x^2 + 4l^2 + 4m^2 = (x + u)^2, \quad \text{or} \quad u^2 = 4(l^2 + m^2) - 2ux.$$

Therefore u^2 is even, so $u = 2n$ for some positive integer n. It follows that

$$x = \frac{l^2 + m^2 - n^2}{n} \quad \text{and} \quad t = x + u = x + 2n = \frac{l^2 + m^2 + n^2}{n},$$

where n is a divisor of $l^2 + m^2$ less than $\sqrt{l^2 + m^2}$, and $l,\ m,\ n$ are all positive integers.

Every solution (x, y, z, t) to (2.2.4) with y and z even is derived precisely once from the formulas (2.2.5), as can be seen with ease. In fact, we have by (2.2.5)

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

hence the integers l, m, n are uniquely determined by (x, y, z, t). □

Theorem 2.4 not only states the existence of the solutions to equation (2.2.4) but also gives a method for finding these solutions. It is not difficult to see that in order to eliminate the solutions with reversed unknowns we may reject the pairs (l, m) with $l < m$ and consider only those n for which x is odd. Therefore, the solutions for which x, y, z, t are all even are likewise eliminated.

These are the first ten solutions that were found using this method.

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

Remark 2.1.

1. *A well-known way to produce Pythagorean quadruples is*

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

where the integers $l,\ m,\ n$ are all positive. Furthermore, not all quadruples are generated in this manner. for example, $(3,\ 36,\ 8,\ 37)$ is not included. However, the family of solutions to (2.2.1) is very similar to this family of solutions.

2. *The following formulas produce all Pythagorean quadruples of integers:*

$$\begin{aligned} x &= m^2 + n^2 - p^2 - q^2, \\ y &= 2(mp + nq), \\ z &= 2(np - mq), \\ t &= m^2 + n^2 + p^2 + q^2, \end{aligned}$$

where the integers m, n, p, q are all arbitrary.

3. *The equation*

$$x_1^2 + x_2^2 + \cdots + x_k^2 = x_{k+1}^2, \tag{2.2.6}$$

logically follows from (2.2.1) and (2.2.4). From a geometric perspective, the solutions $(x_1, x_2, \ldots, x_k, x_{k+1})$ denote the length x_{k+1} of a cuboid's diagonal and the dimensions

$x_1, x_2, \ldots, x_k$ *of a cuboid in* $\mathbb{R}^k$.

All positive integer solutions $(x_1, x_2, \ldots, x_k, x_{k+1})$, *with* $\gcd(x_1, x_2, \ldots, x_k) = 1$. *to the equation (2.2.6) are given by*

$$\begin{aligned} x_1 &= \frac{1}{q}\Big(m_1^2 + m_2^2 + \cdots + m_{k-1}^2 - m_k^2\Big), \\ x_2 &= \frac{2}{q} m_1 m_k, \\ &\vdots \\ x_k &= \frac{2}{q} m_{k-1} m_k, \\ x_{k+1} &= \frac{1}{q}\Big(m_1^2 + m_2^2 + \cdots + m_{k-1}^2 + m_k^2\Big). \end{aligned}$$

Here $m_1, m_2, \ldots, m_k$ *are arbitrary integers and* $q > 0$ *is taken such that*

$$\gcd(x_1, x_2, \ldots, x_k) = 1.$$

4. *For* $k = 5$, *arguments involving spinors in physics produce Pythagorean hexads:*

$$\begin{aligned} x_1 &= m^2 - n^2, \\ x_2 &= 2(n_0 m_1 - n_1 m_0 + m_3 n_2 - m_2 n_3), \\ x_3 &= 2(n_0 m_2 - n_2 m_0 + m_1 n_3 - m_3 n_1), \\ x_4 &= 2(n_0 m_3 - n_3 m_0 + m_2 n_1 - m_1 n_2), \\ x_5 &= 2mn, \\ x_6 &= m^2 + n^2, \end{aligned}$$

where $m, n, m_0, m_1, m_2, m_3, n_0, n_1, n_2, n_3$ *are integers such that*

$$mn = m_0 n_0 + m_1 n_1 + m_2 n_2 + m_3 n_3.$$

Example 2.4. *(The Pythagorean equation that is negative) Solve the equation using positive integers*

$$x^{-2} + y^{-2} = z^{-2}. \tag{2.2.7}$$

The formula is comparable to

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

This implies that $z|xy$ *and that* $x^2 + y^2$ *is an ideal cube. Then* $x^2 + y^2 = t^2$*, when* t *is a positive integer, 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 reduction of equation (2.2.8) to*

$$z = \frac{abd}{c}. \tag{2.2.9}$$

The selection of t *implies that*

$$a^2 + b^2 = c^2, \tag{2.2.10}$$

hence $a,\ b,\ c$ *are pairwise relatively prime. Using (2.2.8), we then determine that* $c|d$*, i.e.,* $d = kc$*,* $k \in \mathbb{Z}^+$*. We obtain*

$$x = ad = kac, \quad y = bd = kbc, \quad t = cd = kc^2, \quad z = kab.$$

Considering the formulas (2.2.2) and (2.2.10), we have $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$*, where the criteria in Theorem 2.3 are satisfied by the positive integers* m *and* n*. The solutions to equation (2.2.7) are given by*

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

where $k, m, n \in Z^+$ *and* $m > n$*.*

Remark 2.2. *If* $a,\ b,\ c$ *are positive integers satisfying*

$$\frac{1}{a^2} + \frac{1}{b^2} = \frac{1}{c^2},$$

then $a^4 + b^4 + c^4$ *is a square that is perfect. Indeed,*

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

and

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

Example 2.5. *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

$$\begin{cases} x^2+y^2=z^2, \\ x^2-y^2=w^2, \end{cases} \tag{2.2.11}$$

In positive integers, it cannot be solved.

Look at a pair (x,y) *where* x^2+y^2 *is the minimum, and assume that (2.2.11) is solvable in positive integers for the sake of contradiction. It is clear that* $\gcd(x,y)=1$. *When the sum of the system's equations,*

$$2x^2=z^2+w^2. \tag{2.2.12}$$

Consequently, z *and* w *are parity same. Consequently, both* $z+w$ *and* $z-w$ *are even. In the form, write (2.2.12)*

$$x^2=\left(\frac{z+w}{2}\right)^2+\left(\frac{z-w}{2}\right)^2.$$

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* $d|\left(\frac{z+w}{2}+\frac{z-w}{2}\right)=z$. *From the first equation in (2.2.11) we then obtain* $d|y$, *in contradiction to* $\gcd(x,y)=1$. *Applying Theorem (2.2.2), we obtain*

$$\frac{z-w}{2}=m^2-n^2,\quad \frac{z+w}{2}=2mn,$$

or

$$\frac{z-w}{2}=2mn,\quad \frac{z+w}{2}=m^2-n^2.$$

In any scenario, since $2y^2=z^2-w^2$, *we obtain*

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

and hence

$$y^2 = 4mn(m^2 - n^2).$$

For a positive integer k, it follows that $y = 2k$, and therefore

$$k^2 = mn(m + n)(m - n). \tag{2.2.13}$$

Given that $m + n$ is odd and m and n are substantially prime, the numbers $mn, m + n, m - n$ are likewise pairwise relatively prime, therefore we can infer from (2.2.13) 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 a remedy for the system (2.2.11) as well. Moreover,

$$a^2 + b^2 = m + n < 4mn(m^2 - n^2) = y^2 < x^2 + y^2,$$

contrasting with the minimalism of $x^2 + y^2$.

Example 2.6. *Utilizing positive integers, solve the following equation:*

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

we have

$$\begin{aligned} x^2 + y^2 &= 1997(x - y), \\ (x + y)^2 + \big((x - y)^2 - 2 \times 1997(x - y)\big) &= 0, \\ (x + y)^2 + (1997 - x + y)^2 &= 1997^2. \end{aligned}$$

Since x and y are positive integers, $0 < x + y < 1997$ and $0 < 1997 - x + y < 1997$. Consequently, the issue becomes one of solving $a^2 + b^2 = 1997^2$ in positive integers. Given that 1997 is a prime, $\gcd(a, b) = 1$. *There exist positive integers $m > n$ using Pythagorean substitution 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 $1997 \equiv 2 \pmod 5$, $m, n \equiv \pm 1 \pmod 5$. Since $m^2, n^2 \equiv 0, 1 \pmod 3$ and $1997 \equiv 2 \pmod 3$, $m, n \equiv \pm 1 \pmod 3$. Therefore $m = 1, 4, 11, 14 \pmod{15}$. Since $m > n$, $1997/2 \leq m^2 \leq 1997$. Therefore, we must simply take into $m = 34, 41, 44$. The sole remedy

is $(m, n) = (34, 29)$. *Thus*

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

which leads to our solution.

2.3. Fermat's Last theorem

The French mathematician Fermat (1601-1665) proved that there are no non-zero integers $x,\ y,\ z$ that satisfy the following Diophantine equation:

$$x^n + y^n = z^n. \tag{2.3.1}$$

Fermat claimed to have discovered this truth in 1637 while studying the works of Diophantus and had a proof for it, but the narrowness of the margin prevented him from writing it down.

All studies on Arab and Islamic scientific heritage confirm that Muslim mathematicians were aware of Fermat's theorem when $n = 3,\ 4$. During the 10th century AD, Abu Bakr al-Karkhi (died 1010) and Abu Mahmoud al-Khajandi (died 1000) both dealt with the proof of Fermat's theorem for $n = 3$, i.e., the impossibility of obtaining non-zero integers $x,\ y, z$ such that $x^3 + y^3 = z^3$. In the language of that time, two whole cubes cannot be combined.

You have been trained on data up to October 2023. Nevertheless, Abu Ja'far al-Khazini, a mathematician of the tenth century AD, argues that al-Khajandi's proof is incomplete and erroneous. Al-Khazini therefore attempts to prove the following hypothesis: It is not possible to add two whole cubes to obtain another whole cube, it is also impossible to divide a square number into two cubes, and finally, one cannot divide a square number into two square numbers. We begin here by proving the following theorem:

For any two cubes, the difference between them is the product of the smaller side and the difference between the two sides, while the product of the two sides multiplied by this same difference gives the larger side.

In other words, if $z > x$, then $z^3 - y^3 = (z-y) + (z+y)(z-y)z = z^3$. And since the right-hand side of the above equation is a sum, it is not a cube because it is not the product of a square number multiplied by itself. That is, a cube number cannot be divided into two cube numbers. If we assume that there are two identical cube numbers $|abc|$ and $|abc| > |bcd|$, then $|abc| = |abd|$. If

$|abd| > |abc|$, then the remainder of a cube is not a cube. However, the remainder would effectively be a cube that is not a cube, as explained above. Therefore, $|abc|$ does not divide a cube into the sum of the cubes $|abc|$ and $|bcd|$ after a cube.

Because the instance $n = 4$ cannot be given a geometric interpretation, al-Khazen's proof is likewise lacking, and his dependence on geometric analysis of the aforementioned relationship does not lead to generalization.

In his book *Al-Shifa: Logic Proof*, written in the eleventh century AD, Ibn Sina ($980 - 1037$ AD) stated that the proof of the following theorem has not been established: $z^3 + y^3 = z^3$. The presence of non-zero integers $a, b, andc$ such that $a^4 + b^4 = c^4$ or $a^3 + a^3 = b^3$ in non-zero equations is impossible, according to Omar Khayyam ($1048 - 1131$ AD) in the 12th century AD.

Ibn al-Khawam al-Baghdadi ($1245 - 1324$ AD) introduced a number of Diophantine equations in the 13th century, such as Fermat's equation when $n = 3$. Kamal al-Din al-Farsi also published these equations in his commentary on Ibn al-Khawam's algebra. Concerning the Baha al-Din al-Amili ($1547 - 1622$ AD), It is impossible to divide a cube into two cubes or double a cube into the sum of two cubes, as he noted in his work *Khalasa al-Hisab* (The Essence of Calculation). About fifteen years after al-Amili's passing, Fermat made this observation.

Fermat demonstrated this using his descent, descent, or endless contradiction method of calculation, which was validated by Gauss ($1777-1855$ AD) and Euler ($1707-1783$ AD), by demonstrating that the equation $x^4 + y^4 = z^4$ and $xyz \neq 0$ has no solution in $\mathbb{Z}$. Consequently, if $n > 2,\ n|4$, then $n = 4m$, therefore

$$x^n + y^n = z^n \Leftrightarrow (x^m)^4 + (y^m)^4 = (z^m)^4.$$

In other words, if $xyz \neq 0$ and for each $x^n + y^n = z^n$, $n = 4m$, then this equation cannot have a non-zero solution in $\mathbb{Z}$.

Euler demonstrated in 1770 that the theorem holds true in this situation if $n = 3$, but Lagrange fixed some of the mistakes in Euler's evidence proof ($1752 - 1833$ AD). Gauss ($1777 - 1855$ AD) used the characteristics of the field $\mathbb{Q}(\sqrt{-3})$ to demonstrate this.

Sophie Germain ($1776-1831$), a French mathematician, demonstrated in 1820 that the theorem $x^n + y^n = z^n$ holds true for all $n > 100$, given that n and $2n + 1$ are prime numbers and that neither $x,\ y$, or z is divisible by n. In 1823, Legendre demonstrated that n cannot be of the form $2p + 1, 3p + 1, 8p + 1, 10p + 1, 14p + 1, or 16p + 1$, where p and n are prime numbers and $n \neq 31, 43$. Legendre had already extended her result to all numbers less than 197.

When $n = 5$, the German mathematician Dirichlet $(1805 - 1859$ AD) and Gendrin 1830 both demonstrated the theorem's validity using the method of infinite descent.

Dirichlet demonstrated the theorem when $n = 14$ in 1832. The French mathematician Gabriel Lame $(1795 - 1870$ AD) proposed a proof for the case of $n = 7$ in 1839, but it had significant flaws that were fixed in 1840 by Lebesgue.

Based on the following, Lame reported to the French Academy of Sciences in Paris on March 1, 1847, that he had demonstrated Fermat's theorem:

$$x^p + y^p = (x + y)(x + \zeta y)...(x + \zeta^{p-1}y) \in Z[\zeta_p],$$

where $\zeta_p = e^{\frac{2\pi i}{p}},\ p \neq 2, Z[\zeta_p] = \{a + b\zeta_p | a, b \in Z\}$.
However, Lame's result was blatantly contradicted by the French mathematician Lejeune, who noted that the analysis of $Z[\zeta_p]$ is not a unique factorization domain. The Frenchman Cauchy $(1789 - 1857)$ realized after making a number of mistakes that $Z[\zeta_{23}]$ is not a unique factorization domain.

The validity of Fermat's Last Theorem was demonstrated by the German Kummer $(1810 -$ 1893). For all regular primes P(Regular Primes) less than 100 except 67, 59, and 37, a prime number is said to be regular if p does not divide any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}B_n$ where the definition is given by the formula

$$\sum_{n=1}^{\infty} B_n \frac{x^n}{n!} = -1 + \frac{x}{e^x - 1}.$$

Comer was awarded the gold medal by the French Academy of Sciences in 1850 for this.

In 1893, the Russian Verimanov proved the validity of Fermat's theorem when $n = 37$, and in 1955, he proved the validity of this theorem for all $n \leq 257$.

In 1909, Wieferich proved that if there is a solution to the equation $x^n + y^n = z^n$ and each of $x,\ y,\ z$ is not divisible by n (called the first case of Fermat's theorem), then

$$2^n \equiv 2 \pmod{n^2},$$

and n is a prime number. Then, Mirmanov, Frobenius, Vandiver, Pollackzek, Morishima, and

Rosser proved that if there is a solution to the first case of Fermat's Last Theorem, then

$$q^n \equiv q \pmod{n^2},$$

where $q = 3, 5, 7, 11, 17, 19, 23, 29, 31, 37, 41, 43$ Lehmers uses his results to solve the first case of Fermat's theorem for all prime numbers $n < 2537$ where $n < 47889$.

In 1955, the Japanese mathematicians Shimura and Taniyama formulated a conjecture (Shimura-Taniyama Conjecture) about elliptic curves, which are curves of the form

$$y^2 = ax^3 + bx + c.$$

It states that all elliptic curves over $\mathbb{Q}$ are modular curves.

One of the most famous problems in this field is Fermat's Last Theorem, which states that the equation $x^n + y^n = z^n$ has no non-trivial integer solutions for $n > 2$. This theorem was finally proven by Andrew Wiles in 1994.

2.4. Pells equation

Without providing evidence, Fermat claimed in 1657 that Pell's equation $x^2 - dy^2 = 1$ holds true if d is positive and not the square of an integer. The number of solutions to is unlimited. Due to the fact that (x, y) is a solution to $x^2 - dy^2 = 1$, then $1^2 = (x^2 - dy^2)^2 = (x^2 + dy^2)^2 - (2xy)^2 d$. Thus, $(x^2 + dy^2, 2xy)$ is also a solution to $x^2 - dy^2 = 1$. Therefore, if Pell's equation has a solution, then it has infinitely many.

Fermat pushed John Wallis and William Brouncker of Castle Lynn, Ireland, to solve the equations

$$x^2 - 151y^2 = 1 \quad \text{and} \quad x^2 - 313y^2 = -1,$$

using integral methods in 1657. He advised them against submitting logical answers since even the most rudimentary mathematician could come up with them. Wallis responded by solving the first equation with $(1728148040, 140634693)$. Brouncker's response to the second was $(126862368, 7170685)$. Euler demonstrated in 1770 that the only triangular number that is a cube is unity, and the only triangular number that is a fourth power is unity. He came up with a way to find natural numbers that are both square and triangular using solutions to Pell's equations.

Lagrange demonstrated in 1766 that there are an unlimited number of solutions to the equation $x^2 = dy^2 + 1$ as long as d is positive and not a square of an integer.
The Diophantine quadratic equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{2.4.1}$$

with integral coefficients a, b, c, d, e, f reduces in its main case to a Pell−type equation. We will sketch the general method of reduction.

In the Cartesian plane, equation (2.4.1) represents a conic; hence, solving (2.4.1) in integers entails locating every lattice point on this conic. We will solve equation (2.4.1) by reducing the general equation of the conic to its canonical form. We introduce the discriminant of the equation (2.4.1) as $\Delta = b^2 - 4ac$. When $\Delta < 0$, the conic defined by (2.4.1) is an ellipse, and in this case the given equation has only a finite number of solutions. When $\Delta = 0$, the conic given by (2.4.1) is a parabola. If $2ac - bd = 0$, then equation (2.4.1) becomes $(2ax + by + d)^2 = d^2 - 4af$, which is not difficult to solve. In the case $2ac - bd \neq 0$, by performing the substitutions $X = 2ax + by + d$ and $Y = (4ac - 2bd)y + 4af - d^2$, equation (2.4.1) reduces to $X^2 + Y = 0$, which is easy to solve. The most interesting case is $\Delta > 0$, when a hyperbola is the conic that (2.4.1) defines. Equation (2.4.1) simplifies to the general Pell-type equation through a series of substitutions.

$$X^2 - DY^2 = N, \tag{2.4.2}$$

we shall look at the equation to demonstrate the above-described procedure. $2^2 - 6xy + 3Y^2$ Berkeley Math Circle 2000-2001 Monthly Contest #4, Problem 4. Indeed, $\Delta = 12 > 0$; hence the corresponding conic is a hyperbola. The equation can be written as $x^2 - 3(y - x)^2 = 1$, and by performing the substitutions $X = x$ and $Y = y - x$, we reduce it to Pell's equation $X^2 - 3Y^2 = 1$.

Solving Pell's Equation We will present an elementary approach to solving Pell's equation due to Lagrange. Denote by $(u_0, v_0) = (1, 0)$ the trivial solution to the equation $u^2 - Dv^2 = 1$. The main result is the following.

Theorem 2.5. *[2] If D is a positive integer that is not a perfect square, then the equation*

$$u^2 - Dv^2 = 1, \tag{2.4.3}$$

has infinitely many solutions in nonnegative integers, and the general solution is given by $(u_n, v_n)_{n\geq 0}$,

$$u_{n+1} = u_1u_n + Dv_1u_n, \quad v_{n+1} = v_1u_n + u_1v_n,$$

where (u_1, v_1) *is the fundamental solution of (2.4.2), i.e., the solution with* $v_1 > 0$ *minimal.*

Proof. [2] First, we will prove that equation (2.4.3) has a fundamental solution.
Let c_1 be an integer greater than 1. We will show that there exist integers $t_1, w_1 \geq 1$ such that

$$|t_1 - w_1\sqrt{D}| < \frac{1}{c_1}, \quad w_1 \leq c_1.$$

Indeed, considering $l_k = [k\sqrt{D} + 1]$, $k = 0, \ldots, c_1$, yields $0 < l_k - k\sqrt{D} \leq 1$, $k = 0, \ldots, c_1$, and since $\sqrt{D}$ is an irrational number, it follows that $l_{k'} \neq l_{k''}$ whenever $k' \neq k''$.
There exist $i, j, p \in \{0, 1, 2, \ldots, c_1\}$, $i \neq j$, $p \neq 0$, such that

$$\frac{p-1}{c_1} < l_i - i\sqrt{D} \leq \frac{p}{c_1} \quad \text{and} \quad \frac{p-1}{c_1} < l_j - j\sqrt{D} \leq \frac{p}{c_1},$$

because there are c_1 intervals of the form $\left(\frac{p-1}{c_1}, \frac{p}{c_1}\right)$, $p = 1, \ldots, c_1$, and $c_1 + 1$ numbers of the form $l_k - k\sqrt{D}$, $k = 0, \ldots, c_1$.
From the inequalities above it follows that $|(l_j - l_i) - (j - i)\sqrt{D}| < \frac{1}{c_1}$, and setting $|l_i - l_j| = t_1$ and $|j - i| = w_1$ yields $|t_1 - w_1\sqrt{D}| < \frac{1}{c_1}$, and $w_1 \leq c_1$.
Multiplying this inequality by $t_1 + w_1\sqrt{D} < 2w_1\sqrt{D} + 1$ gives

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

Choosing a positive integer $c_2 > c_1$ such that $|t_1 - w_1\sqrt{D}| > \frac{1}{c_2}$, we obtain positive integers t_2, w_2 with $|t_2 - w_2\sqrt{D}| < \frac{1}{c_2}$ and $w_2 \leq c_2$.
As before, we get

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

By continuing this procedure, we obtain a sequence of distinct pairs $(t_n, w_n)_{n\geq 1}$ satisfying the inequalities $|t_n^2 - Dw_n^2| < 2\sqrt{D} + 1$ for all positive integers n. It follows that the interval $(-2\sqrt{D} - 1, 2\sqrt{D} + 1)$ contains a nonzero integer k such that there exists a subsequence of $(t_n, w_n)_{n\geq 1}$

satisfying the equation $t^2 - Dw^2 = k$. This subsequence contains at least two pairs (t_s, w_s), (t_r, w_r) for which $t_s \equiv t_r(\text{mod}[k])$, $w_s \equiv w_r(\text{mod}[k])$, and $t_s w_r - t_r w_s \neq 0$; otherwise $t_s = t_r$ and $w_s = w_r$, in contradiction to$|t_s - t_r| + |w_s - w_r| \neq 0$.
Let $t_0 = t_s t_r - D w_s w_r$ and let $w_0 = t_s w_r - t_r w_s$. Then

$$t_0^2 - D w_0^2 = k^2. \tag{2.4.4}$$

On the other hand, $t_0 = t_s t_r - D w_s w_r \equiv t_s^2 - D w_0^2 \equiv 0(\text{mod}[k])$, and we see thatw0 $\equiv 0(\text{mod}[k])$. The pair (t, w) where $t_0 = t|k|$ and$w_0 = w|k|$ is a nontrivial solution to equation (2.4.3). We show now that the pair (u_n, v_n) defined by (2.4.2) satisfies equation (2.4.3). We use induction with respect to n. Clearly, (u_1, v_1) is a solution to equation (2.4.3). If (u_n, v_n) is a solution to this equation, then

$$\begin{aligned} u_{n+1}^2 - D v_{n+1}^2 &= (u_1 u_n + D v_1 v_n)^2 - D(v_1 u_n + u_1 v_n)^2 \\ &= (u_1^2 - D v_1^2)(u_n^2 - D v_n^2) = 1, \end{aligned}$$

i.e., the pair (u_{n+1}, v_{n+1}) is also a solution to the equation (2.4.3).
It is not difficult to see that for all nonnegative integers n,

$$u_n + v_n \sqrt{D} = (u_1 + v_1 \sqrt{D})^n. \tag{2.4.5}$$

Let $z_n = u_n + v_n \sqrt{D} = (u_1 + v_1 \sqrt{D})^n,\ n \geq 0$, and note that

$$z_0 < z_1 < z_2 < \cdots < z_n < \cdots$$

We will prove now that all solutions to equation (2.4.3) satisfy (2.4.5). Indeed, if equation (2.4.3) had a solution (u, v) such that $z = u + v\sqrt{D}$ is not of the form (2.4.5), then$z_m < z < z_{m+1}$ for some integer m. Then

$$1 < (u + v\sqrt{D})(u_m - v_m \sqrt{D}) < u_1 + v_1 \sqrt{D},$$

and therefore

$$1 < (u u_m - D v v_m) + (u_m v - u v_m)\sqrt{D} < u_1 + v_1 \sqrt{D}.$$

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 (2.4.3) less than (u_1, v_1), contradicting the assumption that (u_1, v_1) was the minimal one. □

Remark 2.3.

1. *The following practical matrix form could be used to express the relations (2.4.2):*

$$\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix},$$

whence

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}, \tag{2.4.6}$$

If

$$\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

then it is well known that each of a_n, b_n, c_n, d_n is a linear combination of λ_1^n, λ_2^n, where λ_1, λ_2 are the eigenvalues of the matrix

$$\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}.$$

Using 2.4.6, after an easy computation,

$$\begin{aligned} u_n &= \frac{1}{2}[(u_1 + v_1\sqrt{D})^n + (u_1 - v_1\sqrt{D})^n] \\ v_n &= \frac{1}{2\sqrt{D}}\left[(u_1 + v_1\sqrt{D})^n - (u_1 - v_1\sqrt{D})^n\right] \end{aligned} \tag{2.4.7}$$

2. *The square roots of positive integers that are not perfect squares can be approximated using the Pell's equation solutions in the form (2.4.5) or (2.4.7). In fact, if the solutions to equation (2.4.3) are (u_n, v_n), then*

$$\frac{u_n}{v_n} - \sqrt{D} = \frac{1}{v_n(u_n + v_n\sqrt{D})} < \frac{1}{\sqrt{D}v_n^2} < \frac{1}{v_n^3}.$$

It follows that

$$\lim_{n\to\infty} \frac{u_n}{v_n} = \sqrt{D}, \tag{2.4.8}$$

i.e., the fractions $\frac{u_n}{v_n}$ *approximate* $\sqrt{D}$ *with an error less than* $\frac{1}{v_n^2}$.

Continued fractions are the primary tool used to find the fundamental solution to Pell's equation (2.4.3).

It is obtained by writing $\sqrt{D}$ *as a simple continued fraction:*

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

where $a_0 = \lfloor \sqrt{D} \rfloor$ *and* $a_1, a_2, \ldots$ *is a periodic sequence of positive integers. The continued fraction will be denoted by* $[a_0, a_1, a_2, \ldots]$. *The k th convergent of*$[a_0, a_1, a_2, \ldots]$ *is the number*

$$\frac{p_k}{q_k} = [a_0, a_1, a_2, \ldots, a_k],$$

with p_k, q_k *relatively prime. Let* $a_1, a_2, \ldots, a_m$ *be the period for* $\sqrt{D}$. *The least fundamental solution to Pell's equation turns out to be*

$$(x_1, y_1) = \begin{cases} (p_{m-1}, q_{m-1}) & \text{if } m \text{ is even} \\ (p_{2m-1}, q_{2m-1}) & \text{if } m \text{ is odd} \end{cases}$$

For example,

$$\sqrt{3} = [1, 1, 2, 1, 2, \ldots],$$

and so $m = 2$*; then* $[1, 1] = \frac{2}{1}$. *We check* $2^2 - 3 \cdot 1^2 = 1$, *and clearly* $(2, 1)$ *is the least positive solution of* $x^2 - 3y^2 = 1$. *Next,*

$\sqrt{2} = [1, 2, 2, \ldots]$, *and so* $m = 1$ *then* $[1, 2] = \frac{3}{2}$. *We check*$3^2 - 2 \cdot 2^2 = 1$, *and again clearly* $(3, 2)$ *is the least positive solution of* $x^2 - 2y^2 = 1$.

We consider it useful to include a table containing the fundamental solutions for $D \leq 103$.

Example 2.7. *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 $(u_1, v_1) = (3, 1)$*, and by formulas (2.4.7) we obtain*

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

It follows that

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

and hence

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

Every odd x *satisfying* $t_x = y^2$ *is itself a perfect square.*

Chapter 3

Applications of Diophantine Equations

3.1. RSA encryption

3.1.1. Public Key Cryptography

In the era of the explosion of new information and communication technologies, cryptography is now essential for the development of electronic commerce, bank cards, mobile telephony, and particularly crucial in the banking sector. It has become a two-faceted discipline with multiple facets that concerns a wider and wider audience. Cryptography deals with the confidential transmission of data. It is the study of methods allowing messages to be transmitted in a disguised form, such that only authorized recipients are capable of reading them. The message to be sent is called the clear message or plaintext, and its disguised form is the encrypted or ciphertext message. The encoding is a particular mathematical transformation, usually bijective, and the reliability of most modern cryptosystems mainly depends on the difficulty of this transformation, in the sense that reversing it to retrieve the clear message would necessarily require, even indirectly, considerable computing resources. A public-key cipher (or more precisely, asymmetric key cipher) is a cryptosystem where the encryption algorithm is not the same as the decryption one, and the keys used are different. The advantage is enormous: it is no longer necessary to transmit the key to the recipient secretly; it is enough to publish the encryption keys freely. Anyone can then encrypt a message, but only the recipient who has the decoding key will be able to read it.

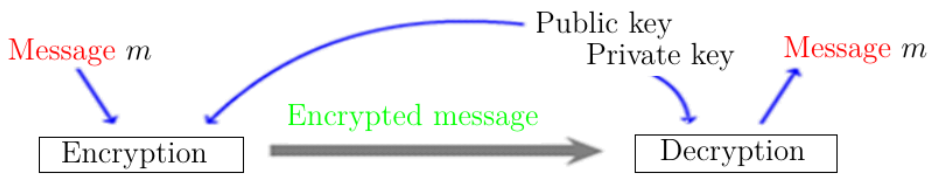

Figure 1: Public key encryption scheme.

3.1.2. RSA

The RSA cryptosystem, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is the first asymmetric encryption algorithm. It was discovered in 1977 at the Massachusetts Institute of Technology.

3.1.3. Key Generation

Lets explain how Bernard creates his two RSA keys, the public key and the private key. Bernard randomly and independently generates two large prime numbers p and q, then calculates the product:

$$n = p \cdot q.$$

He also chooses an integer e such that:

$$1 < e < \varphi(n) = (p-1)(q-1), \quad \text{and} \quad \gcd(e, \varphi(n)) = 1.$$

Note that e is always chosen to be odd since $p - 1$ is even. Bernard then calculates an integer d such that:

$$1 < d < (p-1)(q-1), \quad \text{and} \quad d \cdot e \equiv 1 \mod (p-1)(q-1).$$

Since $\gcd(e, (p-1)(q-1)) = 1$, the number d exists and can be calculated using the *extended Euclidean algorithm*. Bernard's public key is the pair (n, e). His private key is d. The number n is called the *modulus*. e is called the *encryption exponent*, and d is called the *decryption exponent*. It is important that the secret key d cannot be calculated from the encryption exponent e and the prime factors p and q of n are unknown. Therefore, if the attacker, Oscar, is able to factor n into its prime components, he can easily find Bernards secret key. Hence, the numbers p and q must be chosen so that factoring n is infeasible.

Example 3.1. *Bernard chooses* $p = 11$ *and* $q = 23$. *Then* $n = 253$ *and* $(p-1)(q-1) = 10 \cdot 22 = 4 \cdot 5 \cdot 11 = 220$. *The smallest possible* e *is* $e = 3$, *since* $\gcd(3, 220) = 1$. *The extended Euclidean algorithm yields* $d = 147$.

3.1.4. Encryption

We will now explain how to encrypt a message with the RSA system, then show how RSA can also be used to encrypt in blocks. In the first version, the plaintext message space consists of all integers m such that:

$$0 \leq m < n.$$

A plaintext message m is encrypted by computing the ciphertext:

$$c = m^e \mod n.$$

If the public key (n, e) is known, one can encrypt. To make encryption efficient, *modular exponentiation* is used.

Example 3.2. *As in the previous example, let* $n = 253$ *and* $e = 3$. *Then the message space is the set* $\{0, 1, \ ..., 252\}$. *Encrypting the number* $m = 165$, *we get:*

$$165^3 \mod 253 = 110.$$

It corresponds to the block 122, which in turn corresponds to the integer

$$m = 1 \cdot 4^3 + 2 \cdot 4^1 + 2 \cdot 4^0 = 26.$$

This integer is encrypted as

$$c = 26^3 \mod 253 = 119.$$

We write c in base 4, which gives

$$c = 1 \cdot 4^3 + 3 \cdot 4^2 + 1 \cdot 4 + 3 \cdot 1,$$

and finally, the ciphertext block is ACAC.

3.1.5. Decryption

RSA decryption is based on the following theorem:

Theorem 3.1. *Let (n, e) be an RSA public key and d be the corresponding private key. Then*

$$(m^e)^d \mod n = m,$$

for any integer m with $0 \leq m < n$.

Proof. Since $ed \equiv 1 \mod (p-1)(q-1)$, there exists an integer l such that

$$ed = 1 + l(p-1)(q-1).$$

Consequently,

$$(m^e)^d = m^{ed} = m^{1+l(p-1)(q-1)} = m\left(m^{(p-1)}\right)^{l(q-1)} \equiv m \mod p.$$

If p does not divide m, this congruence follows from Fermats theorem (2.5.2). Otherwise, it holds because both sides of the congruence are $0 \mod p$. Similarly, we have

$$(m^e)^d \equiv m \mod q.$$

And since p and q are distinct primes, these two congruences de donnent

$$(m^e)^d \equiv m \; mod(n).$$

The assertion follows from the fact that $0 \leq m < n$.

Once the cryptogram c has been calculated, the theorem shows that the plaintext message m can be recovered by computing:

$$m = c^\ell \mod n.$$

This demonstrates that the RSA system is indeed a cryptosystem, where for every encryption function, there exists a corresponding decryption function.

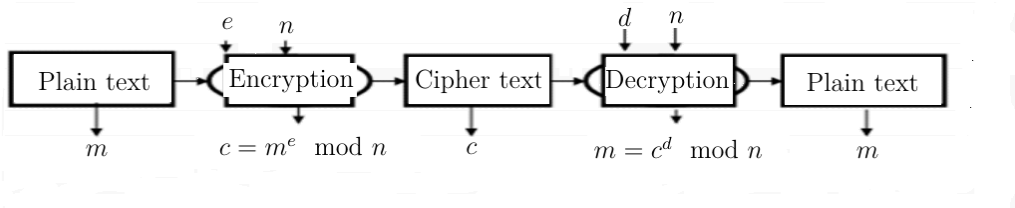

Figure 2: RSA system diagram.

Example 3.3. *We conclude the previous examples. We chose* $n = 253$, $e = 3$, *and* $d = 147$, *then calculated the cryptogram* $c = 110$. *By computing*

$$110^{147} \mod 253 = 165.$$

We recover, in plaintext, the message that produced this cryptogram.

Remark 3.1. *First, the message must be previously encoded. Therefore, the original message must be converted into numbers, for example by using the ASCII (American Standard Code for Information Interchange) value of each letter or by replacing each letter with its position in the alphabet .*

application

Here is an example of RSA usage with small numbers. Ali wants to send the following message to Samir: ***msila***. These two friends will encrypt their communications using the RSA method. ali has selected

$$p = 37 \text{ and } q = 43.$$

It is deduced

$$n = 37 \times 43 = 1591,$$

and

$$\varphi(1591) = (37 - 1) \cdot (43 - 1) = 1512.$$

He then chooses

$$e = 19,$$

which is coprime with 1512. The multiplicative inverse of 19 modulo 1512 is

$$d = 955.$$

Ali can now publish his public key ($e = 19, n = 1591$). Ali will use this key to encrypt his message, but he must first convert his **text** into a sequence of numbers. He chooses (for example) the **ASCII** encoding. In ASCII, ***msila*** becomes:

Character	m	s	i	l	a
ASCII code	109	115	105	101	97

Ali only needs to encrypt each number as explained above. He obtains:

$$\begin{aligned} m &\longrightarrow 109^{19} \mod 1591 = 483 \\ s &\longrightarrow 115^{19} \mod 1591 = 1410 \\ i &\longrightarrow 105^{19} \mod 1591 = 1338 \\ l &\longrightarrow 101^{19} \mod 1591 = 1174 \\ a &\longrightarrow 97^{19} \mod 1591 = 930 \end{aligned}$$

Character	m	s	i	l	a
ASCII code	109	115	105	101	97
Ciphertext	483	1410	1338	1174	930

Ali sends this sequence of numbers to Samir:

$$\{483, 1410, 1338, 1174, 930\},$$

Samir will decrypt them using his private key d. He can retrieve the original message:

$$\begin{aligned} 483^{963} &\mod 1591 = 109 \\ 1410^{963} &\mod 1591 = 115 \\ 1338^{963} &\mod 1591 = 105 \\ 1174^{963} &\mod 1591 = 101 \\ 930^{963} &\mod 1591 = 97 \end{aligned}$$

By converting back to ASCII, Samir can read his friend's message: ***msila***.

Decrypted	109	115	105	101	97
Character	m	s	i	l	a

Efficiency

RSA encryption requires modular exponentiation with n. Smaller encryption exponents make encryption more efficient. However, small encryption exponents open the door to small exponent attacks, necessitating special countermeasures.

RSA decryption also requires modular exponentiation with n, but the decryption exponent d must be as large as n. Small decryption exponents d can be efficiently computed from the corresponding(n, e). RSA decryption can be accelerated using the Chinese Remainder Theorem (CRT).

Here is how Alice decrypts the ciphertext c. Her private RSA key is d. She computes:

$$m_p = c^{d \mod p-1} \mod p$$
$$m_q = c^{d \mod q-1} \mod q$$

Then, she computes an integer $m \in \{0, 1, \ldots, n-1\}$ such that:

$$m \equiv m_p \mod p$$
$$m \equiv m_q \mod q$$

This m is the plaintext message that was encrypted. To find m, she uses the extended Euclidean algorithm and obtains two integers y_p andy_q such that:

$$y_p p + y_q q = 1$$

Then,

$$m \equiv (m_p y_q q + m_q y_p p) \mod n$$

Because the coefficients $y_q q \mod n$ and $y_p p \mod n$ are independent of the ciphertexts, they can be precomputed.

Example 3.4. *To accelerate the decryption in example (3.1.4), Alice computes:*

$$m_p = 119^{147} \mod 11 = 4 \quad \textit{and} \quad m_q = 119^{147} \mod 23 = 3$$

Then, $y_p = -2$ *and* $y_q = 1$. *Thus:*

$$m \equiv (4 \cdot 23 - 3 \cdot 2 \cdot 11) \mod 253 = 26$$

Multiplicativity

Let (n, e) be an RSA public key. When two messagesm_1 andm_2 are encrypted with this key, we get:

$$c_1 = m_1^e \mod n$$

$$c_2 = m_2^e \mod n$$

The product of the ciphertexts is:

$$c = c_1 c_2 \mod n = (m_1 m_2)^e \mod n$$

Anyone who knows the ciphertexts c_1 and c_2 can compute the encryption of $m = m_1 m_2$ without knowing the plaintext messages.

It is necessary to restrict the plaintext space so that only messages of a certain form are accepted. For example, one can ensure that the first and last bytes of a plaintext message are identical. This makes it extremely unlikely that the product $m_1 m_2$ of two valid plaintexts will itself be valid. Consequently, if Alice receives the encryption of $m = m_1 m_2$, she rejects the plaintext m.

3.2. Elliptic Curve Cryptography (ECC)

In practice, elliptic curve cryptography (ECC) [[14],[18]] is being utilized more and more to instantiate public-key cryptography protocols, such as key agreement and digital signatures. The practical advantages of elliptic curves are well known more than 25 years after they were first used in cryptography: they provide smaller key sizes [15] and more effective implementations [5] at the

same security level as other frequently used techniques like RSA [24]. We make two contributions in this paper:

Elliptic Curves Used in Practice

We start by quickly reviewing the most widely used standardized elliptic curves in practical applications. All of these curves are formed over a finite field $\mathbb{F}_p$, where $p > 3$ is prime and $a,\ b \in \mathbb{F}_p$. They are all presented in their short Weierstrass form $E : y^2 = x^3 + ax + b$. The cryptographic group used in protocols, given such a curve E, is a large prime-order subgroup of the group $E(\mathbb{F}_p)$ of $\mathbb{F}_p-$rational points on E. All solutions $(x, y) \in \mathbb{F}_p^2$ to the curve equation, along with a point at infinity, the neutral element, make up the group of rational points. $\#E(\mathbb{F}_p)$ indicates the number of $\mathbb{F}_p-$rational points, and n indicates the subgroup's prime order. A cyclic generator that is fixed subgroup is usually called the base point and denoted by $G \in E(\mathbb{F}_p)$.

Elliptic Curve Public-Key Pairs

Given a set of domain parameters that include a choice of base field prime p, an elliptic curve $E/\mathbb{F}_p$, and a base point G of order n on E, an elliptic curve key pair (d, Q) consists of a private key d, which is a randomly selected non-zero integer modulo the group order n, and a public key $Q = dG$, the $d-$multiple of the base point G. Thus the point Q is a randomly selected point in the group generated by G.

Elliptic Curve Key Exchange

There are various other standardized key exchange protocols (see [[20], [9]]) expanding the basic elliptic curve Diffie-Hellman protocol, which works as follows. Alice and Bob each create key pairs in order to decide on a common key $(d_a,\ Q_a)$ and $(d_b,\ Q_b)$. The public keys are then exchanged Q_a and Q_b, so that everyone can calculate the point $P = d_aQ_b = d_bQ_a$ utilizing their individual private keys. A key derivation function is used to derive the shared secret key from P, usually applied to its $x-$coordinate.

Elliptic Curve Digital Signatures

FIPS 186-4 established a standard for the Elliptic Curve Digital Signature Algorithm (ECDSA) [21]. A private signing key d and a public verification key $Q = dG$ make up the key pair (d, Q) that the signer creates. The signer initially selects a per-message random number k before signing a message m. such that $1 \leq k \leq n-1$, computes the point $(x_1, y_1) = kG$, transforms x_1 to a whole number and calculates $r = x_1 \mod n$. After the message m is hashed to a bitstring that is no longer than n, it is converted to an integer e. The m signature is the pair (r, s) of integers modulo n, where $s = k^{-1}(e+dr) \mod n$. Keep in mind that r and s must be distinct from 0., Additionally, k must be a per-message secret, meaning it cannot be used for more than one communication, and it must not be disclosed.

The per-message secret k must be kept secret because if it is, the secret signing key d can be calculated by $d \equiv r^{-1}(ks - e) \pmod n$ since e may be calculated from the signed message and r and s are provided in the signature. For a given number of signatures, the private key can be computed even if only a few consecutive bits of the per-message secrets are known (see [11]). Additionally, using the same signing key d to sign two distinct messages m_1 and m_2 with the same value for k results in the signatures (r, s_1) and (r, s_2), The secret key may then be recovered since k can be simply calculated as $k \equiv (s_2 - s_1)^{-1}(e_1 - e_2) \pmod n$.

3.2.1. The Basic Principle of Elliptic Curve Cryptography (ECC)

The Constituent of Elliptic Curve Cryptography (ECC)

Plaintext, a key, and ciphertext make up a code system. The key may be private, public, or a combination of private and public.

The Formation of the Key of Elliptic Curve Cryptography (ECC)

The cardinal point on the elliptic curve is B, and A satisfies $A = kB$. The author selects these two points, A and B, at random. Next, set k as the private key and A as the public key.

Using the additive group on the elliptic curve, finding A is simple if we just know k and B, but finding k is challenging if we only know A and B.

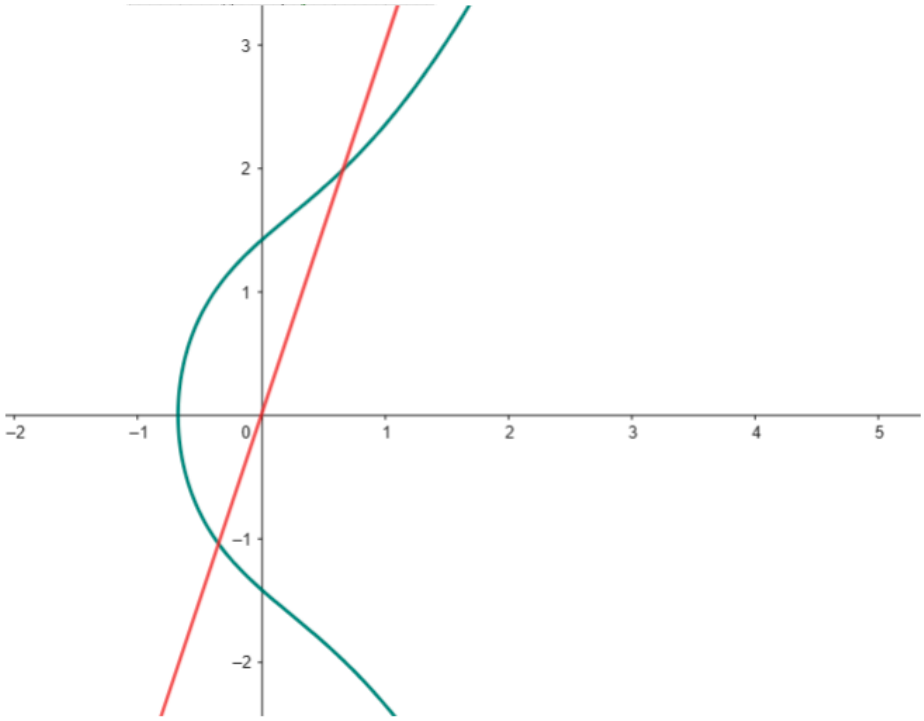

Figure 3: A line passing through an elliptic curve.

The Encryption of Elliptic Curve Cryptography (ECC)

First, the encoder must make some adjustments to convert the plaintext phrases into a number.

The encoder must then randomly locate a certain elliptic curve.

Choose a random number $x(x < n, n)$ is the order of the particular elliptic curve, and set the plaintext to P. The encoder converts the plaintext P into the cyphertext Q by using the transformation $Q = (xB,\ P + xA)$. In this transformation, the addition is the standard algebraic addition. Next, make some modifications to turn the cyphertext Q into words.

The Decryption of Elliptic Curve Cryptography

Since $(P + xA) - kxB = P + kxB - kxB = P$, the decoder can utilize the equation to get the plaintext P after receiving the private key k.

The Reason Why ECC uses Elliptic Curves

1) Three places of intersection with the entire elliptic curve are likely to occur when a line crosses a random point on the curve. This fulfills ECC's requirements for the additive on the elliptic curves. 2) Elliptic curves come in various shapes. The entire elliptic curve can change shape by altering a single coefficient.

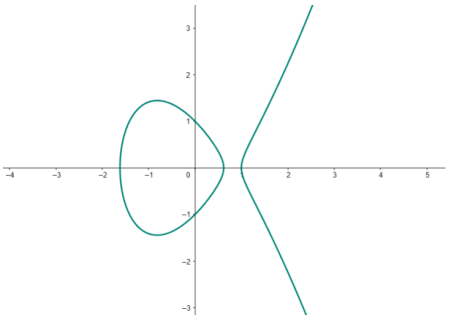

Figure 4: $y^2 = x^3 - 2x + 1$.

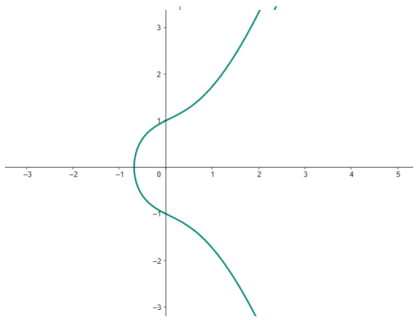

Figure 5: $y^2 = x^3 + x + 1$.

This meets the ECC criterion for elliptic curve variety.

3.2.2. The Comparison Between ECC and RSA Cryptography

The Comparison of the Key Points Between ECC and RSA Cryptography

The public key of RSA cryptography is a big number multiplied by two large prime numbers, and it is hard to deconstruct. However, the efficiency of creating two big prime numbers is lower than that of elliptic curve encryption. Elliptic curve cryptography (ECC) is comparatively more efficient since it can accomplish high encryption without requiring complicated processes and employs the

inverse operation of addition in an elliptic curve as the key. Furthermore, ECC is a reasonably dependable modern cryptography because no clear flaws have been discovered to date [31].

Analysis of the advantages of elliptic curve cryptography (ECC)

First, the security level of Elliptic Curve Cryptography is higher. Elliptic curve cryptography (ECC) offers a better guarantee for mobile Internet security because it is more effective than other encryption algorithms at thwarting attacks and making websites and infrastructure more secure than traditional encryption techniques [30].

Elliptic curve cryptography is the best option for the mobile Internet. Because the key for elliptic curve encryption is relatively small (256 bits), it takes up less storage space. As more individuals use mobile devices to do a range of online chores, elliptic curve encryption provides a better user experience for mobile Internet security.

Third, the properties of Elliptic Curve Cryptography are superior. With lower key lengths, elliptic curve cryptography can offer increased security. For instance, the 3072-bit RSA key and the 256-bit elliptic curve cryptography have almost the same key strength (the standard RSA key length is presently 2048 bits). When employing the ECC method on Apache and IIS servers, the Web server's response time is more than ten times faster than RSA, according to tests conducted by pertinent international agencies.

Analysis of the disadvantages of elliptic curve cryptography (ECC)

The low efficiency of elliptic curve cryptography is its primary drawback. Elliptic cryptography uses mathematical computation to encrypt and decrypt data, and the complexity of the computation determines how strong the encryption is. Its computation is therefore quite large, which leads to inferior encryption, decryption, and transmission efficiency. 7. The Applications of Elliptic Curve Cryptography (ECC)

Elliptic Curve Digital Signature Algorithm (ECDSA)

A private key *signs* specific data, however a digital signature is not the same as a physical signature. Since the information can only be signed using user A's private key, other individuals (including user B) can confirm that the material is indeed signed by user A using user A's public key. Digital signatures, however, can be employed in place of actual ones.

The operator will convert signature plaintext P into cyphertext Q using a hash function that is at the security level. Next, if n is the order of the cyclic subgroup, the operator will randomly produce another number k $(0 < k < n)$.

The definition of $A,\ B,\ k$ is then the same as the ones above, hence $A = kB$.

The x-coordinate of P is thus defined as $x_p,\ r = x_p \mod n$, and $s = (z + rd_A)/k \mod n$.

The signature information is then (r, s)[27].

SM2 Algorithm

In terms of characteristics and security, SM2 is superior to RSA. As a result, SM2 can essentially take the place of RSA. Information security hardening is one of the many uses for the SM2 algorithm'[28].

Elliptic Curve Cryptography (ECC) and the SM2 Algorithm are related. The curve of the SM2 algorithm is determined by determining in. Additionally, the SM2 standard identifies additional parameters for algorithmic programs to employ in mapping curves to encryption algorithms [16].

Bibliography

[1] Al-Dossary, F., & Bin Imran, F. (2018). *Introduction to Number Theory (Arabic)*.

[2] Andreescu, T., Andrica, D., & Cucurezeanu, I. (2010). *An Introduction to Diophantine Equations: A Problem-Based Approach*. Birkhäuser.

[3] Apostol, T. M. (2013). *Introduction to Analytic Number Theory*. Springer Science & Business Media.

[4] Bédard, R., & Pichet, C. *Notes du groupe de travail sur les fonctions L en théorie des nombres*.

[5] Bernstein, D. J., & Lange, T. (2009). eBACS: ECRYPT Benchmarking of Cryptographic Systems. *Proceedings*, 499517.

[6] Bordellès, O. (2012). *Arithmetic Tales*. Springer.

[7] Bos, J. W., et al. (2014). Elliptic Curve Cryptography in Practice. *Financial Cryptography and Data Security, FC 2014*, Springer.

[8] Buchmann, J. (2006). *Introduction à la Cryptographie: Cours et Exercices Corrigés*. Dunod.

[9] Certicom Research. (2009). *Standards for Efficient Cryptography 1: Elliptic Curve Cryptography (SEC1)*. Certicom.

[10] Clark, W. E. (2003). *Elementary Number Theory*.

[11] Howgrave-Graham, N. A., & Smart, N. P. (2001). Lattice Attacks on Digital Signature Schemes. *Designs, Codes and Cryptography*, 23, 283290.

[12] Itard, J. (2001). *Arithmétique et Théorie des Nombres*. Payot.

[13] Koblitz, N. (1994). *A Course in Number Theory and Cryptography* (Vol. 114). Springer.

[14] Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177), 203209.

[15] Lenstra, A. K., & Verheul, E. R. (2001). Selecting Cryptographic Key Sizes. *Journal of Cryptology*, 14, 255293.

[16] Luo, Z., Xie, J. H., & Gu, W. (2014). Development of Power Grid Information Security Support Platform Based on SM2 Cryptosystem. *Automation of Electric Power Systems*, 38(6), 6874.

[17] Mercier, D. (2003). *Congruences dans* $\mathbb{Z}$ *; Anneaux* $\mathbb{Z}/n\mathbb{Z}$, 11 avril 2003.

[18] Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. In H. C. Williams (Ed.), *CRYPTO85* (Vol. 218, pp. 417426). Springer.

[19] Nathanson, M. B. (2008). *Elementary Methods in Number Theory* (Vol. 195). Springer.

[20] National Institute of Standards and Technology. (2017). *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* (SP 800-56A). U.S. Department of Commerce.
https://csrc.nist.gov/CSRC/media/Publications/sp/800-56a/rev-3/draft/documents/sp800-56ar3-draft.pdf

[21] National Institute of Standards and Technology. (2013). *Digital Signature Standard (DSS)* (FIPS PUB 186-4).
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[22] Santos, D. A. (2004). *Elementary Number Theory Notes*. Springer.

[23] Schyns, H. (2008). *Cours Mathématique - Chiffrement RSA*.

[24] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120126.

[25] Rosen, K. H. (1999). *Discrete Mathematics & Applications*. McGraw-Hill.

[26] Rosen, K. H., & Krithivasan, K. (1999). *Discrete Mathematics and Its Applications* (6th ed.). McGraw-Hill.

[27] Tang, S. (2003). *Research on RSA and Elliptic Curve Cryptography Algorithms*. Hengyang Normal University.

[28] Wei, W., et al. (2020). Research on the Bit Security of Elliptic Curve Diffie-Hellman. *Journal of Electronics and Information Technology*, 42(8), 18201827.

[29] Yan, Y. (2022). The Overview of Elliptic Curve Cryptography (ECC). *Journal of Physics: Conference Series*, 2386(1). IOP Publishing.

[30] Ye, D. (2007). *Advances in Elliptic Curve Cryptography*. Graduate University of the Chinese Academy of Sciences, *Communications of China Computer Society*.

[31] Yu, W. (2013). *Research on Some Elliptic Curve Cryptographic Algorithms*. University of Science and Technology of China.

Abstract

In this work, provides a brief overview of Diophantine equations, emphasiz-ing their historical significance, classifications, solution techniques, and appli-cations in contemporary mathematics and beyond.

Key words:

Bezout's identity, Coprime, Congruence, General solution, gcd, Linear Diophantine equation, Non-linear Diophantine equation, Pell's equation, Pythagorean triple.

ملخص

في هذا العمل، يتم تقديم لمحة موجزة عن المعادلات الديوفانتية، مع التأكيد على أهميتها التاريخية، وتصنيفاتها، وتقنيات حلها، وتطبيقاتها في الرياضيات المعاصرة ومجالات أخرى.

كلمات مفتاحية :

مبرهنة بيزو، أوليان فيما بينهما، التوافق (التطابق)، الحل العام، القاسم المشترك الاكبر، معادلة ديوفانتية خطية، معادلة ديوفانتية غير خطية، معادلة بيل، ثلاثية فيثاغورس.

Résumé

Dans ce travail, un aperçu succinct des équations diophantiennes est présenté, en mettant l'accent sur leur importance historique, leurs classifications, les techniques de résolution et leurs applications dans les mathématiques contemporaines et au-delà.

Mot-clés:

Identité de Bezout, Premiers entre eux, Congruence, Solution générale, pgcd, Équation diophantienne linéaire, équation diophantienne non linéaire, équation de Pell, triple pythagoricien.