PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESERACH

Mohamed Boudiaf University of M'sila
Faculty of Mathematics and Informatics
Departement of Mathematics

Master of Mathematics

Mathematics and Informatics
Specialty: Mathematics
Option : Algebra and discrete mathematics

Theme

Some principles of elementary number theory

Persented by :
ZAKAD Fatima and SILINI Khadidja

Publicly presented on :09/06/2024.

in front of the jury :

MIHOUBI Douadi	Pr.	University of M'sila	**Chairpesont**.
BOUDAOUD Abdelmadjid	Pr.	University of M'sila	**Sypervisor**.
HEBOUB Lakhdar	M.C.B.	University of M'sila	**Examinator**.

University years: 2023/2024

Dedications

◇

Praise be to God and thanks be to God.

◇

To My Parents who encouraged and supported me
To Everyone I love and who loves me.

◇

TO My sister Khouloud,Saadia,Naima,Noura,Akila especially Samuona and my brothers Salah and Issa

◇

To all my friends, especially Fattoum, Abeer, Khadija, and Nisreen, who were with me throughout my academic journey with encouragement and support.

◇

To my teachers and professors from primary school to university, thanks, appreciation and respect.

◇

To All members of my families.

◇

To everyone who supported me on the path to success.

◇

To My teachers and classmates.

ZAKAD Fatima

Dedications

◇

To those who have had the greatest support after Allah in every achievement .I have made in my life

◇

To my beloved mother who has been a source of safety who was always by my side encouraging me you have all the thanks and appreciation .

◇

TO my dear father who provided unwavering support you have all thanks and gratitude .

◇

To my brother younes and my sisters Kaouther ,Chaima and my little sister Aicha Manar .

◇

To my beloved all familly thanks for your constant support and encouragement .

◇

To all my friends Khawla ,Marwa and Fatima .

◇

To all my teachers and my collegues

Silini Khadidja

Acknowledgements

In the name of Allah, the Most Gracious, the Most Merciful
We, (ZAKAD Fatima) and (SILINI Khadidja), extend our heartfelt thanks to Allah Almighty for granting us the strength and patience to complete this work and for enabling us to achieve this accomplishment.
We would like to express our sincere gratitude and appreciation to our supervisor, Professor **(BOUDAOUD Abdelmadjid)**, for his continuous support and valuable guidance that played a significant role in directing us throughout the research and writing of this thesis. His patience and dedication had a profound impact on our success.
We also extend our thanks to the head of the jury, Professor **(MIHOUBI Douadi)**, and Professor **(HEBOUB Lakdhar)** and Professor **(ABDELKEBIR Saad)**, for their precious time and efforts in reading and evaluating our work.
We must not forget to express our deep gratitude to our beloved families who have been our mainstay and principal supporters throughout our studies. We thank our parents for all thing and continuous encouragement, and we thank our brothers and sisters for their support and motivation.
We also extend our thanks to all our friends and colleagues for their assistance and encouragement during our study period.
In conclusion, we pray to Allah to grant us all success in what He loves and pleases.

(ZAKAD Fatima) and (SILINI Khadidja)

Thants

Contents

List of Symbols

Notation	Name
$\mathbb{N}$	Naturel nembers 1, 2, 3,.....
$\mathbb{C}$	The set of complex numbers.
$\mathbb{Z}$	The set of integers.
ϕ(n)	Euler's phi function.
$\mathbb{Z}^+$	The set of positive integers.
$\mathbb{Q}$	the set of rational numbers .
$\mathbb{R}$	set of real numbers .
$A \cup B$	union of A and B .
$A \cap B$	entersection of A and B .
$\sum$	summation .
$a\|b$	a divides b .
$\binom{n}{k}$	binnomial cofficient .
(a, b)	greatest common divisor.
$\bigcup_{i=1}^{n} A_i$	union of $A_i, i = 1, 2, ...n$.
$\gcd(m, n)$	The greatest common divisor of m, n .
$lcm(m, n)$	*The last common multiple of* m, n.
$a \equiv b \pmod{n}$	a is congruent to b modulo n .

Introduction

Number theory is divided into two main parts: Elementary number theory and Analytical number theory and is concerned with properties of the natural numbers 1, 2, 3, 4, ..., also called the positive integers. These numbers, together with the negative integers and zero, form the set of integers. A very particular attention is reserved for prime numbers, which form part of positive integers.

To better understand the value of this specialty, it is enough to cite what was said on this subject by the German mathematician Carl Friedrich Gauss (1777–1855): " Mathematics is the queen of the sciences and number theory is the queen of mathematics ".

In mathematics in general, and in number theory in particular, there are a certain number of theorems which have the honor of being called principles. We cite here some of these principles :

1- Well-Ordering principle.

2- Mathematical Induction principle.

3- Binomial Theorem.

4- Pigeonhole principle.

5- Inclusion-Exclusion Principle.

The current dissertation is part of elementary number theory and is entitled "Some principles of elementary number theory ". The dissertation is presented in three chapters, the first of which is devoted to a review of fundamental concepts and tools. In the second chapter, we present the above-mentioned principles and, in some cases, their proofs. The final chapter is devoted to some applications of these principles. We close this thesis with a general conclusion, a summary in three languages (Arabic, French and English) and a bibliography.

1 Preliminary

In this chapter, we will talk about some preliminary, tools and concepts that help us to clarify and understund this work . In this section we mainly used the following references [3], [8], [11].

1.1 Divisibility

Definition 1.1 *[8]*

If $a \neq 0$, b are integers, we say that a divides b if there is an integer c such that $ac = b$. We write this as $a \mid b$, if a does not divide b we write $a \nmid b$.

The following properties should be immediate.

Theorem 1.2

1. If a, b, c, m, n are integers with $c|a$, $c|b$, then $c|(am + nb)$.

2. If x, y, z are integers with $x|y$, $y|z$ then $x|z$.

Proof

There are integers s, t with $sc = a$, $tc = b$. Thus $am + nb = c(sm + tn)$, giving $c|(am + bn)$. Also, there are integers u, v with $xu = y$, $yv = z$. Hence $xuv = z$, giving $x|z$. It should be clear that if $a|b$ and $b \neq 0$ then $1 \leq |a| \leq |b|$.

Example 1.3

1. As $3 \mid 21$ and $3 \mid 33$, Theorem 1.9 tells us that 3 divides $5 \cdot 21 - 3 \cdot 33 = 105 - 99 = 6$.

2. 11/66 and 66/198 then 11/198.

1.1.1 Division Euclidean

Theorem 1.4

If a and b are integers such that b > 0 , then there are unique integers q and r suth that a= bq +r with0≤ r < b .

1.2 Primes and Greatest divisors

1.2.1 GCD and LCM

Definition 1.5 *The greatest common divisor of two integers a and b is the greatest integer that divides both a and b we denote it by (a,b).*

Example 1.6

The greatest common divisor of 24 and 18 is 6 in other words (24,18)=6.

Definition 1.7

Let a and b positive integers . The Least common multiple of a and b denoted by $[a, b]$ is the smalleast positive integer which is divisible by both a and b .

Example 1.8

The Least common multiple of 5 and 8 is $[5, 8]$ =40.

1.2.2 Prime Numbers

The positive integer 1 has just one positive divisor. Every other positive integer has at least two positive divisors, because it is divisible by 1 and by itself. Integers with exactly two positive divisors are of great importance in number theory; they are called primes.

Definition 1.9

A prime is an integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example 1.10

The integers 2, 3, 5, 13, 101, and 163 are primes.

1.2.3 Infinitude of primes

Lemma 1.11

Every integer greater than 1 has a prime divisor.

Proof

We prove the lemma by way of contradiction ; we assume that there is a positive integer greater than 1

having no prime divisors. Then, since the set of positive integers greater than 1 with no prime divisors is nonempty, the well-ordering property tells us that there is a least positive integer n greater than 1 with no prime divisors. Because n has no prime divisors and n divides n, we see that n is not prime. Hence, we can write $n = ab$ with $1 < a < n$ and $1 < b < n$. Because $a < n$, a must have a prime divisor. By Theorem 1.9, any divisor of a is also a divisor of n, so n must have a prime divisor, contradicting the fact that n has no prime divisors. We can conclude that every positive integer greater than 1 has at least one prime divisor. ■

Theorem 1.12

There are infinitely many primes.

Proof

Suppose that there are only finitely many primes, $P_1, P_2, \ldots, P_n$, where n is a positive integer. Consider the integer Q_n, obtained by multiplying these primes together and adding one, that is,

$$Q_n = P_1 P_2 \cdots P_n + 1.$$

By Lemma 1.10, Q_n has at least one prime divisor, say, q. We obtain a contradiction by showing that q is not one of the primes listed. If $q = P_j$ for some integer j with $1 \leq j \leq n$, then since $Q_n - P_1 P_2 \cdots P_n = 1$, because q divides both terms on the left-hand side of this equation, by Theorem 1.11 it follows that $q \mid 1$. This is impossible because no prime divides 1. Consequently, q must be a prime we have not listed. This contradiction shows that there are infinitely many primes. ■

Theorem 1.13 *(Prime Number Theorem)*

The ratio of $\pi(x)$ to $\frac{x}{\log x}$ approaches 1 as x grows without bound.This means

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

1.2.4 The Fundamental Theorem of Arithmetic

Theorem 1.14

Every positive integer greater than 1 can be written uniquely as a product of primes, with the prime factors in the product written in nondecreasing order. Sometimes the fundamental theorem of arithmetic is extended to apply to the integer 1.That is 1 is considered to be written uniquely as the empty product of primes .

Example 1.15

$240 = 2^4 \times 3 \times 5$

$1001 = 7 \times 11 \times 13$

1.2.5 Euclidean Algorithm

We now examine a procedure that avoids factorising two integers in order to obtain their greatest common divisor. It is called the Euclidean Algorithm and it is described as follows.
Let a, b be positive integers. After using the Division Algorithm repeatedly, we find the sequence of equalities

$$a = bq_1 + r_2,\ 0 < r_2 < b$$

$$b = r_2q_2 + r_3,\ 0 < r_3 < r_2$$

$$r_2 = r_3q_3 + r_4,\ 0 < r_4 < r_3$$

.

.

.

.

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n$$

The last non-zero remainder correspands to gcd(a,b).
This algorithm allows us to calculate the gcd without going through the factorization process.

Example 1.16

Find (225,157) by means of the euclidean algorithm we have

$$225=157\times 1+68$$

$$157=68\times 2+21$$

$$68=21\times 3+5$$

$$21=5\times 4+1$$

$$5=1\times 5+0\ .$$

Thus gcd(225,157)=1.

1.3 Linear Diphantine Equation

When we require that solutions of a particular equation come from the set of integers, we have a diophantine equation. These equations get their name from the ancient Greek mathematician Diophantus, who

wrote on equations where solutions are restricted to rational numbers. The equation ax+ by= c, where a, b, and c are integers, is called a linear diophantine equation in two variables.

***Theorem 1.17** [11]*

Let a, b, c be integers, a and b nonzero. Consider the linear Diophantine equation of the form .

$ax + by = c \quad (\star)$

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

2. *If* $(x, y) = (x_0, y_0)$ *is a particular solution to* $(\star)$*, then every integer solution isof the form* $x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t,$

3. *If* $c = \gcd(a, b)$ *and* $|a|$ *or* $|b|$ *is different from 1, then a particular solution* $(x, y) = (x_0, y_0)$ *to* $(\star)canbefoundsuchthat|x_0| < |b|$ *and* $|y_0| < |a|$.

Example 1.18

Solve the following Diophantine equation : $5x + 7y = 8$.

Solution

by Euclidienne algorithem we have

1 = 5.*(3)+7(-2)* $\implies 8 = 5.(24) + 7(-16)$

Then $x_0 = 24,\ y_0 = -16$

$X(t) = 24 + 7t$

$Y(t) = -16 - 5t.$

Where t is integer.

1.3.1 Bezout's Identity

Definition 1.19

For any two positive integers a and b, there exists two integers x and y such that $xa + yb = gcd(a, b)$.

Example 1.20

Suppose that $a = 56$ *and* $b = 15$ *we calculate the greatest common divisor using Euclidean algorithm*

$56 = 15 \times 3 + 11$

$15 = 11 \times 1 + 4$

$11 = 4 \times 2 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

Then $pgcd(56, 15) = 1$.

To find x and y

$1 = 4 - 3 \times 1$

$1 = 4 - (11 - 4 \times 2) \times 1 = 4 \times 3 - 11$

$1 = (15 \times 3 - (56 - 15 \times 3) \times 4 = 15 \times 15 - 56 \times 4.$

Therefore , we can find x and y as follows : $1 = 15.15 - 56.4$ *. Thus* $x = -4$ *and* $y = 15$ *.*

1.3.2 Congruences

The concept of congruence was introduced by Gauss. Although it is a very simple notion, its importance and usefulness in number theory are enormous. This is particularly obvious in that even complicated arguments can be presented in a define concise and clear manner.

Definition 1.21

Let m be a positive integer. If a and b are integers, we say that a is congruent to b modulo m if $m|(a-b)$. If a is congruent to b modulo m, we write $a \equiv b \pmod{m}$. If m does not divide $a - b$, we write $a \not\equiv b \pmod{m}$, and say that a and b are incongruent modulo m. The integer m is called the modulus of the congruence.

Theorem 1.22

If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.

Proof

If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. This means that there is an integer k with $km = a - b$, so that $a = b + km$.

Example 1.23

22 $\equiv 4 \pmod{9}$, *since* $9 \mid (22 - 4)$.

13 $\not\equiv 5 \pmod{9}$, *since* $9 \nmid (13 - 5)$.

1.3.3 Complete set of residues

Definition 1.24

A complete set of residues modulo m is a set of integers which satisfy the following condition:

Every integer is congruent to a unique member of the set modulo m .

In other words the set contains exactly one member of each residue class.

Remark 1.25

- *The division algorithm is used to show that the set of integers 0, 1, 2, ... , m-1 is a complete system of residues modulo m. This is called the set of least non-negative residues modulo m.*

- *use the congruences maked it possible to work with divisibility relation ships much as we work with equalities. Prior to the introduction of congruences, the notation used for divisibility relationships was awkward and difficult to work with. The introduction of a convenient notation helped accelerate the development of number theory.*

1.3.4 Order of an Integer

Definition 1.26

Let a and n be relatively prime integers with $a \neq 0$ and n positive. Then the least positive integer x such that $a^x \equiv 1(mod\ n)$ is called the order of a modulo n and is denoted by $ord_n\ a$.

Example 1.27 *To find the order of 2 modulo 7, we compute the least positive residue modulo 7 of powers of 2.*

$2^1 \equiv 2(mod\ 7)$

$2^2 \equiv 4(mod\ 7)$

$2^3 \equiv 1(mod\ 7)$

Then $ord_7 2 = 3$.

1.3.5 Euler's ϕ function

Definition 1.28

The Euler ϕ function of a positive integer n, denoted by $\phi\ (n)$ counts the number of positive integers less than n that are relatively prime to n .

Example 1.29

Let n be a natural number. How many of the fractions $1/n$, $2/n$, . . . ,$(n-1)/n$, n/n are irreducible is $\phi(n)$.

1.3.6 Theorems of Fermat and Wilson

Theorem 1.30 *(Fermat's Theorem)*

Let p denote a prime. If $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

For every integer a,

$$a^p \equiv a \pmod{p}.$$

Example 1.31

$2^{340} \equiv 1 \pmod{341}$, *where* $341 = 11 \cdot 31$. *Note that* $2^{10} = 1024 = 31 \cdot 33 + 1$.

Thus, $2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$ *and* $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$, $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$ *or* $2^{341} \equiv 2 \pmod{341}$.

After canceling a factor of 2, we get $2^{340} \equiv 1 \pmod{341}$ *so that the converse to Fermat's theorem is false.*

Theorem 1.32 *(Wilson)*

If p *is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Explain with an example how to prove.

Let $p = 13$. *It is possible to divide the integers 2, 3, ..., 11 into* $(p-3)/2 = 5$ *pairs, each product of which is congruent to 1 modulo 13.*

To write these congruences out explicitly: $2 \cdot 7 \equiv 1(mod\ 13)$

$3 \cdot 9 \equiv 1(mod\ 13)$

$4 \cdot 10 \equiv 1(mod\ 13)$

$5 \cdot 8 \equiv 1(mod\ 13)$

$6 \cdot 11 \equiv 1(mod\ 13)$.

Multiplying these congruences gives the result:

$12! =$*(2·7)(3·9)(4·10)(5·8)(6·11)(1.12)*

$\equiv 1.1.1.1.1.(-1)(mod\ 13)$. *So 12!* $\equiv -1(mod\ 13)$.

1.3.7 Euler's Theorem

Theorem 1.33

Let $(a, n) = 1$. *Then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Example 1.34

Find the last two digits of 3^{1000}.

Solution

As $\phi(100) = 40$, *by Euler's Theorem,* $3^{40} \equiv 1 \pmod{100}$. *Thus,*

$$3^{1000} = (3^{40})^{25} \equiv 1^{25} = 1 \pmod{100},$$

and so the last two digits are 01.

2

Some Principles of number theory

In this section, we mainly used the following references [3], [8],[9] [11].

2.1 Well ordering principle

The well ordering principle is a fundamental concept in mathematics, It has many uses especially in proving the principle of mathematical induction .

Theorem 2.1

Every non-empty subset C of the natural numbers has a least element.

Example 2.2

There is no integer in the interval]0,1[.

Solution

Assume to the contrary that the set S of integers in]0,1[is non-empty. As S is a set of positive integers, it must contain a least element say m. Now $0 < m^2 < m < 1$*, and so* $m^2 \in S$ *. But this is saying that S has a positive integer* m^2 *which is smaller than its least positive integer m. This is a contradiction and so* $S = \phi$*.*

2.2 Principle of Mathematical induction

Mathematical induction is a method for proving statements depending on non negative integers.

Theorem 2.3

Principle of Mathematical Induction if a set S of nonnegative integers contains the integer 0 and also contains the integer $n + 1$ *whenever it contains the integer n then* $S = \mathbb{N}$*.*

Corollary 2.4 *[8]*

If a set A of positive integers contains the integer m and also contains $n+1$ *whenever it contains n, where* $n > m$*, then A contains all the positive integers greater than or equal to m .*

Example 2.5

Use mathematical induction to prove that $n! \leq n^n$ *for all positive integers n .*

Solution

Note that $1! = 1 \leq 1^1 = 1$ *. We now present the inductive step .*

Suppose that $n! \leq n^n$ *for some* $n > 1$ *, we prove that* $(n+1)! \leq (n+1)^{n+1}$ *, note that (n+1)! =(n+1)n!* $\leq (n+1).n^n < (n+1)(n+1)^n = (n+1)^{n+1}$.

Example 2.6

Prove that $23^n - 1$ *is divisible by 11 for all positive integers n.*

Solution

Clearly $23^1 - 1 = 22$ *is divisible by 11.Suppose* $11|23^k - 1$ *for some positive integer k . Then* $23^{k+1} - 1 = 23 \times 23^k - 1 = 11 \times 2 \times 23^k + (23^k - 1)$ *which is also divisible by 11. It follows that* $23^n - 1$ *is divisible by 11 for all positive integers n.*

2.3 Binomial Theorem

In mathematics the binomial theorem is an important formula giving the expansion of powers .Therefore we present some necessary things to prove this theorem.

Definition 2.7

Let m and k be non negative integers with $k \leq m$. The binomial coefficient $\binom{m}{k}$ is defined by $\binom{m}{k} = \frac{m!}{k!(m-k)}$. *When k and m are positive integers with $k > m$,* $\binom{m}{k} = 0$.

Example 2.8

We have a group of 4 people and you want to choose 2 of them to form a committee. Then the number is $\binom{4}{2} = \frac{4!}{2!(4-2)!} = \frac{4\times3\times2\times1}{2\times1} = 6$.

Theorem 2.9

Let n and k be non negative integers with $k \leq n$ then

$\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{k} = \binom{n}{n-k}$.

Proof

$\binom{n}{0} = \frac{n!}{0!(n!)} = 1$.

$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$.

Theorem 2.10 *(Pascal's identity)*

Let n and k be positive integers with $n \geq k$. Then $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$.

Proof

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k!)} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!(n-k+1)}{k!(n-k+1!)} + \frac{n!k}{k!(n-k+1)!)} \\ &= \frac{n!((n-k+1)+k)}{k!(n-k+1!)} \\ &= \frac{n!(n+1)}{k!(n-k+1)!} \\ &= \frac{n+1!}{k!(n-k+1)!} \\ &= \binom{n+1}{k}.\end{aligned}$$

Theorem 2.11 *(The Binomial Theorem)*

Let x and y be variable and n be a positive integer. Then

$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \ldots + \binom{n}{n-2} x^2 y^{n-2} + \binom{n}{n-1} x\, y^{n-1} + \binom{n}{n} y^n$ *or using summation notation*

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

Example 2.12

We have the cases $n = 5$

$$(x+y)^5 = \sum_{k=0}^{5} \binom{5}{k}\ x^{5-k}y^k$$

$$k = 0\ ,\ \binom{5}{0}x^{5-0}y^0 = x^5$$

$$k = 1\ ,\ \binom{5}{1}x^{5-1}y^1 = 5x^4y$$

$$k = 2\ ,\ \binom{5}{2}x^{5-2}y^2 = 10x^3y^2$$

$$k = 3\ ,\ \binom{5}{3}x^{5-3}y^3 = 10x^2y^3$$

$$k = 4\ ,\ \binom{5}{4}x^{5-4}y^4 = 5xy^4$$

$$k = 5\ ,\ \binom{5}{5}x^{5-5}y^5 = y^5.$$

$$\textit{Then } (x+y) = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + y^5.$$

Corollary 2.13

$2^n = (1+1)^n = \sum_{j=0}^{n}\binom{n}{j}\ 1^{n-j}\ 1^j = \sum_{j=1}^{n}\ \binom{n}{j}$.

2.4 Pigeonhole Principle

The Pigeonhole Principle is a simple combinatorial concept that we can use in a number of practical situations. states that if $n+1$ *pigeons fly to* n *holes there must be a pigeonhole containing at least two pigeons*

Theorem 2.14

Let $n, k \in \mathbb{N}$. *If at least* $nk + 1$ *objects are divided into* n *groups, then at least one of these groups contains at least* $k + 1$ *objects.*

Proof *We prove this by contradiction. For* $i = 1, 2, \ldots, n$ *we denote by* m_i *the number of objects in the* i*th group. Let us suppose that the conclusion does not hold, i.e each group contains no more than* k *objects. Then* $m_i \leq k$ *for all* $i = 1, 2, ..., n$, *which implies that* $nk + 1 \leq m_1 + m_2 + \cdots m_n \leq k + k + ... + k = nk$.

But this is a contradiction, since $nk + 1 > nk$.

Remark 2.15

We also find in many references the value of k *equal to 1.*

Example 2.16

Show that any set of ten two-digit numbers has two nonempty disjoint subsets such that the sums of their elements are the same.

Solution

A ten-element set has altogether $2^{10} - 1 = 1023$ *non empty subsets. The sum of at most ten two − digit numbers is less than 10* $\times 100 = 1000 < 1023$. *Hence there exist two different non empty subsets of the given set of ten numbers such that the sums of their elements are equal. By removing, if necessary any common elements, we obtain two disjoint non empty subsets with the desired property.*

Example 2.17 *[9] P269*

Show that there exists a number of the form 123456789123456789...123456789 *that is divisible by* 987654321.

Solution

We set $n = 123456789$, $m = 987654321$ *and* $a_i = \frac{(10^{9i}-1)n}{10^9-1}$

for $i = 1, 2, ..., m + 1$. *Then clearly, the* a_i *are exactly the numbers of the given form . Any integer has one of the m remainders* $0, 1, ...,$ *m -1 when divided by m.*

By pigeonhole principle at least two of the m+ 1 numbers $a_1 a_2$, ... , a_{m+1} *must have the same remainder, and thus there exist i, j ,* $1 \leq j < i \leq m + 1$ *such that* $m|a_i - a_j$. *Now* $a_i - a_j = ((10^{9i} - 1) - (10^{9j} - 1)).\frac{n}{10^9-1} = (10^{9i}10^{9j}).\frac{n}{10^9-1} = 10^{9j}a_{i-j}$

Since$(m, 10^{9i}) = 1$, *the number* a_{i-j} *is divisible by m which was to be shown.*

2.5 Inclusion-exclusion principle

The inclusion exclusion principle used to calculate the number of elements in the union of several sets by adjusting for element that my be counted multiple times.This principle used also in combinatorics and statistics.

Notation: For a set A, we note by $|A|$ *The cardinal of A .*

Theorem 2.18

Let A and B two finite sets we have $|A \cup B| = |A| + |B| - |A \cap B|$.

Example 2.19

At high school there are 28 students in algebre class and 30 students in biology class and 8 students in both classes. How many students are in either algebra or biology class ?

Solution

Let A denote the set of students in algebra class and B denote the set of student in biology class. To find the number of students in either class, we first add up the students in each class :

$|A \cup B| = |A| + |B| - |A \cap B| = 28 + 30 - 8 = 50$

so there are 50 students in at least one of the two classes.

Theorem 2.20

Let A , B and C three finite sets then :

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Example 2.21

Every student in some class takes at least one of three courses Mathematic , Philosophy and French.The number of Mathematic students is 30, The number of Philosophy students is 40 , The number of French students is 100, The number of Mathematic and Philosophy students is 10, The number of Mathematic and French students is 20, The number of Philosophy and French students is 20 there are 5 students who take all three courses mathematic, philosophy and french .How many students (N) are there in the class?

By inclusion exclusion principle we have N=30+40+100-10-20-20+5=125.

***Theorem 2.22** [4] P 504*

The principle of inclusion and exclusion states that for finite n sets $A_1, ..., A_n the following holds.Let $A_1, A_2, ...A_n$ be finite sets. Then

$|\bigcup A_{i1 \leq i \leq n}| = \sum_{1 \leq i_1 \leq n} |A_{i1}| - \sum_{1 \leq i_1 \leq i_2 \leq n} |A_{i1} \cap A_{i2}| + \sum_{1 \leq i_1 \leq i_2 \leq n} |A_{i1} \cap A_{i2} \cap A_{i3}| - ... + (-1)^{n-1} |\bigcap_{i=1}^{n} A_i|$

.

Proof

We will prove the formula by showing that an element in the union is counted exactly once by the right hand side of the equation . Suppose that a is a member of exactly r of the sets $A_1, A_2, ...A_n$ Where $1 \leq r \leq n$.This element is counted $C(r,1)$ times by $\sum |A_i|$ .It is counted $c(r,2)$ times by $\sum |A_i \cap A_j|$. In general it is counted $c(r,m)$ times by the summation involving m of the sets A_i . Thus , this element is counted exactly $c(r,1) - c(r,2) + c(r,3) - ... + (-1)^{r+1} c(r,r)$

times by the expression on the right hand side of this equation . Our goal is to evaluate this quantity .

We have $c(r,0) + c(r,1) - c(r,2) - ... + (-1)^{r+1} c(r,r) = 0$

Hence $1 = c(r,0) = c(r,1) - c(r,2) + ... + (-1)^{r+1} c(r,r)$.

Therefore , each element in the union is counted exactly once by the expression on the right hand side of the equation . This proves the principle of inclusion exclusion .

3 Some applications

In this section, we mainly used the following references [2], [3],[8], [9], [11].

3.1 The well ordering principle

3.1.1 Division Algorithm

Theorem 3.1

If a, b are positive integers, then there are unique integers q, r such that $a = bq + r$, $0 \leq r < b$.

Proof

By the Well-Ordering Principle. Consider the set $S = \{a - bk : k \in \mathbb{Z} \text{ and } a \geq bk\}$. Then S is a collection of nonnegative integers and $S \neq \emptyset$ as $a - b \cdot 0 \in S$. By the Well-Ordering Principle, S has a least element, say r. Now there must be some $q \in \mathbb{Z}$ such that $r = a - bq$ since $r \in S$. By construction, $r \geq 0$. Let us prove that $r < b$. For assume that $r \geq b$. Then $r > r - b = a - bq - b = a - (q + 1)b \geq 0$, since $r - b \geq 0$. But then $a - (q + 1)b \in S$ and $a - (q + 1)b < r$ which contradicts the fact that r is the smallest member of S. Thus we must have $0 \leq r < b$. To show that r and q are unique, assume that $bq_1 + r_1 = a = bq_2 + r_2$, $0 \leq r_1 < b$, $0 \leq r_2 < b$. Then $r_2 - r_1 = b(q_1 - q_2)$, that is $b \mid (r_2 - r_1)$. But $|r_2 - r_1| < b$, whence $r_2 = r_1$. From this it also follows that $q_1 = q_2$. This completes the proof.

Example 3.2

Show that if $p > 3$ is a prime, then $24 \mid (p^2 - 1)$.

Solution

By the Division Algorithm, integers come in one of six flavours: $6k$, $6k \pm 1$, $6k \pm 2$, or $6k + 3$. If $p > 3$ is a prime, then p is of the form $p = 6k \pm 1$ (the other choices are either divisible by 2 or 3). But

$$(6k \pm 1)^2 - 1 = 36k^2 \pm 12k = 12k(3k \pm 1).$$

Since either k or $3k \pm 1$ is even, $12k(3k \pm 1)$ is divisible by 24.

Theorem 3.3

The greatest common divisor of any two integers a, b can be written as a linear combination of a and b, i.e., there are integers x, y with

$$(a, b) = ax + by.$$

Proof

Let $A = \{ax + by \mid ax + by > 0, x, y \in \mathbb{Z}\}$. Clearly, one of $\pm a, \pm b$ is in A, as both a, b are not zero then $A \neq 0$, By the Well-Ordering Principle , A has a smallest element, say d. Therefore, there are x_0, y_0 such that $d = ax_0 + by_0$. We prove that $d = (a, b)$. To do this, we prove that $d \mid a$, $d \mid b$ and that if $t \mid a$, $t \mid b$, then $t \mid d$.

We first prove that $d \mid a$. By the Division Algorithm, we can find integers q, r, $0 \leq r < d$ such that $a = dq + r$. Then

$$r = a - dq = a(1 - qx_0) - by_0.$$

If $r > 0$, then $r \in A$ is smaller than the smallest element of A, namely d, a contradiction. Thus $r = 0$. This entails $dq = a$, i.e. $d \mid a$. We can similarly prove that $d \mid b$. Assume that $t \mid a$, $t \mid b$. Then $a = tm$, $b = tn$ for integers m, n. Hence

$$d = ax_0 + by_0 = t(mx_0 + ny_0),$$

that is, $t \mid d$. The theorem is thus proved.

Theorem 3.4

Let $n > 1$ be a positive integer. Then $a \in \mathbb{Z}$ has an order mod n if and only if $(a, n) = 1$.

Proof

If $(a, n) = 1$, then a has an order in view of Theorem d'euler and by the Well-Ordering Principle. Hence, assume that a has an order mod n. Clearly $a \neq 0$. The existence of an order entails the existence of a positive integer M such that $a^M \equiv 1 \mod n$. Hence, there is an integer s with $a^M + sn = 1$ or $a \cdot a^{M-1} + sn = 1$. This is a linear combination of a and n and hence divisible by (a, n). This entails that $(a, n) = 1$.

Example 3.5

Prove that the square of any integer is of the form $4k$ *or* $4k+1$.

Solution

By the Division Algorithm, any integer comes in one of two forms: $2a$ *or* $2a+1$. *Squaring these, we have:*

$$(2a)^2 = 4a^2,$$

$$(2a+1)^2 = 4(a^2+a)+1$$

and so the assertion follows.

Example 3.6

Prove that if $n > 1$, *then* n *is divisible by at least one prime.*

Proof

Since $n > 1$, *it has at least one divisor* > 1. *we use the Well Ordering Principle,* n *must have a least positive divisor greater than 1, say* q. *We claim that* q *is prime. For if not, then we can write* q *as* $q = ab$, *where* $1 < a \leq b < q$. *But then* a *is a divisor of* n *greater than 1 and smaller than* q, *which contradicts the minimality of* q.

Example 3.7

To prove that $\sqrt{2}$ *is irrational, let's suppose it's rational, i.e.,* $\sqrt{2} = \frac{a}{b}$ *for some integers* a *and* b, *where* $b \neq 0$ *and* a *and* b *have no common factors other than 1. This implies that the set*

$$A = \{n^2 : \text{both } n \text{ and } n^2 \text{ are positive integers}\}$$

is nonempty since it contains a. *By the Well-Ordering Principle,* A *has a smallest element, say* $j = k^2$. *As* $\sqrt{2} - 1 > 0$, $j(2-1) = j^2 - k^2 = (j-k)^2$ *is a positive integer. Since* $2 < 2^2$ *implies* $2 - 2 < 2^2 - 2$ *and also* $j^2 = 2k$, *we see that*

$$(j-k)^2 = k(2-2) < k(2) = j.$$

This leads to a contradiction, as j *was assumed to be the smallest positive element in* A. *Therefore,* $\sqrt{2}$ *cannot be rational, hence it must be irrational.*

3.2 Principle of Mathematical Induction

We will use the well-ordering principle to show that mathematical induction is a valid proof technique.

Theorem 3.8

A set S *of non-negative integers contains the integer* 0, *and also contains the integer* $n+1$ *whenever it contains the integer* n, *then* $S = \mathbb{N}$.

Proof

Assume this is not the case and so, by the Well-Ordering Principle there exists a least positive integer k not in S. Observe that $k > 0$, since $0 \in S$ and there is no positive integer smaller than 0. As $k - 1 < k$, we see that $k - 1 \in S$. But by assumption $k - 1 + 1$ is also in S, since the successor of each element in the set is also in the set. Hence $k = k - 1 + 1$ is also in the set, a contradiction. Thus $S = \mathbb{N}$.

Corollary 3.9 *If a set A of positive integers contains the integer m and also contains $n + 1$ whenever it contains n, where $n > m$, then A contains all the positive integers greate than or equal to m.*

Example 3.10

To prove that $n < 2^n$ for all positive integers n using mathematical induction, we follow these steps:

1. ***Base Case:*** *We prove the statement for the first positive integer $n = 1$.*

$$1 < 2^1$$

$$1 < 2 \quad \textit{which is true.}$$

2. ***Inductive Step:*** *Assume the statement is true for some positive integer k, i.e.,*

$$k < 2^k.$$

Now, we need to prove the statement for $k + 1$:

$$k + 1 < 2^{k+1}.$$

Using the induction hypothesis $k < 2^k$, we have:

$$k + 1 < 2^k + 1.$$

We know that:

$$2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}.$$

Thus:

$$k + 1 < 2^k + 1 \leq 2^{k+1}.$$

Hence

$$k + 1 < 2^{k+1}.$$

Therefore, by mathematical induction, $n < 2^n$ for all positive integers n.

Example 3.11

$2^{2n} - 1$ is divisible by 3.

Solution

Let the statement p(k) given as :

$p(n) = 2^{2n} - 1$ *is divisible by 3, for every natural number n . We observe that p(1) is true, since* $2^2 - 1 = 4 - 1 = 3$ *is divisible by 3 .*

Assume that p(n) is true for some naturel number k , i.e,

p(k)= $2^{2k} - 1$ *is divisible by 3 ,i.e.,* $2^{2k} - 1 = 3q$ *, Where* $q \in \mathbb{N}$*, Now to prove that p(k+1) is true we have*

$p(k+1) = 2^{2(k+1)} - 1 = = 2^{2k} \times 2^2 - 1 = 2^{2k} \times 4 - 1 = 3 \times 2^{2k} + (2^{2K} - 1) = 3 \times 2^{2k} + 3q = 3(2^{2k} + q) = 3m,$ *where* $m \in \mathbb{N}$*, thus p(k+1)is true, whenever p(k) is true.Then by the principle of Mathematical induction p(n) is true for all naturel numbers n .*

Example 3.12

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

Proof

Base case: First we start with the base case, here we shall show that the formula holds for $n = 1$*. We start with the left side:*

$$\sum_{i=1}^{1} i = 1$$

and then the right side,

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

We see that the left side is equal to the right side, so the formula holds for $n = 1$*. Induction step: Assume the formula holds for some arbitrary positive integer* $p \geq 1$*,*

$$\sum_{i=1}^{p} i = \frac{p(p+1)}{2}.$$

The next step is now to show that the formula also holds for the following integer $p + 1$*,*

$$\sum_{i=1}^{p+1} i = \frac{(p+1)(p+2)}{2}.$$

We start with the left side

$$\sum_{i=1}^{p+1} i = \sum_{i=1}^{p} i + (p+1),$$

and by the Induction hypothesis we see that we can rewrite $\sum_{i=1}^{p} i$ *and get*

$$\frac{p(p+1)}{2} + (p+1) = \frac{p(p+1) + 2(p+1)}{2} = \frac{p^2 + 3p + 2}{2} = \frac{(p+1)(p+2)}{2}.$$

We see that the formula also holds for $p + 1$*. By the Induction axiom the formula holds for all integers* $n \geq 1$*. The sum of* i^2

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof

For $n = 1$ we have

$$\sum_{i=1}^{1} i^2 = 1$$

and

$$\frac{1(1+1)(2\cdot 1+1)}{6} = \frac{6}{6} = 1.$$

We see that both left side and right side are equal to 1, so the formula holds for $n = 1$.

Suppose it holds for some arbitrary positive integer p, i.e.

$$\sum_{i=1}^{p} i^2 = \frac{p(p+1)(2p+1)}{6}.$$

Now we want to show that the formula also holds for $p+1$, i.e.

$$\sum_{i=1}^{p+1} i^2 = \frac{(p+1)(p+2)(2p+3)}{6}.$$

We start with the left side

$$\sum_{i=1}^{p+1} i^2 = \sum_{i=1}^{p} i^2 + (p+1)^2,$$

and using the Induction hypothesis, we get

$$\frac{p(p+1)(2p+1)}{6} + (p+1)^2 = \frac{(p+1)(p(2p+1)+6(p+1))}{6} = \frac{(p+1)(2p^2+7p+6)}{6} = \frac{(p+1)(p+2)(2p+3)}{6}.$$

We see that the formula also holds for $p+1$. By the Induction axiom the formula holds for all positive integers n.

Example 3.13 *We will use mathematical induction to show that*

$$\sum_{j=1}^{n}(2j-1) = 1 + 3 + \cdots + (2n-1) = n^2$$

for every positive integer n. (By the way, if our conjecture for the value of this sum was incorrect, mathematical induction would fail to produce a proof).

We begin with the basis step, which follows because

$$\sum_{j=1}^{1}(2j-1) = 2\cdot 1 - 1 = 1 = 1^2.$$

For the inductive step, we assume the inductive hypothesis that the formula holds for n; that is, we assume that

$$\sum_{j=1}^{n}(2j-1) = n^2.$$

Using the inductive hypothesis, we have

$$\sum_{j=1}^{n+1}(2j-1) = \sum_{j=1}^{n}(2j-1) + (2(n+1)-1) \quad \textit{(splitting off the term with } j = n+1)$$

$$= n^2 + 2(n+1) - 1 \quad \textit{(using the inductive hypothesis)}$$

$$= n^2 + 2n + 1$$

$$= (n+1)^2.$$

3.2.1 Strong Induction

Strong induction, also known as complete induction, is a type of mathematical induction. It involves an inductive hypothesis that assumes a statement is true for all positive integers less than or equal to a certain number, unlike weak induction previously mentioned, which assumes the statement is true for some positive integer. Both types are equivalent, but strong induction can sometimes be easier to use.

Theorem 3.14 *[3] p25*

A set of positive integers that contains the integer 1, and that has the property that, for every positive integer n, if it contains all the positive integers 1, 2, ... , n, then it also contains the integer n + 1, must be the set of all positive integers.

The second principle of mathematical induction is called strong induction.

Example 3.15 *[11] P38*

Prove that for all positive integers n, the equation

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

is solvable in positive integers.

Solution

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

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

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

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

for all $n \geq 1$. *Then*

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

hence $x_k^2 + y_k^2 + z_k^2 = 59^k$ *implies*

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

3.3 Binomial Theorem

Binomial theorem is used to solve many applications and these are some of them.

Example 3.16 *[8] p107*

Prove that the integers $[(1+\sqrt{2})^n]$

with n a non negative integer, are alternately even or odd.

Solution

By the Binomial Theorem

$(1+\sqrt{2})^n = (1-\sqrt{2})^n = 2\sum_{0\leq k\leq \frac{n}{2}} (2)^k \binom{n}{2k} = 2N$,

an even integer. Since $-1 < 1-\sqrt{2} < 0$ *it must be the case that (1-* $\sqrt{2})^n$ *is the fractional part of* $(1+\sqrt{2})^n$ *or* $(1+\sqrt{2})^n + 1$ *depending on whether n is odd or even respectively. Thus for odd n* $(1+\sqrt{2})^n - 1 < (1+\sqrt{2})^n = (1-\sqrt{2})^n + 1 < [(1+\sqrt{2})^n]$. *whence* $(1+\sqrt{2})^n + (1-\sqrt{2})^n = [(1+\sqrt{2})^n]$ *always even, and for n even*

$2N = (1+\sqrt{2})^n (1 - \sqrt{2})^n = [(1+\sqrt{2})^n] + 1$ *and so* $[(1+\sqrt{2})^n] = 2N - 1$ *always odd for even n.*

Example 3.17 *[9] p 175*

Show that there are infinitely many natural numbers n such that 2^{n+1} *is divisible by n.*

Solution

We will show that all numbers of the form $n = 3k$ *where* $k \in \mathbb{N}$ *have the desired property. We prove this by induction. If* $k = 1$ *then* $n = 3$ *and clearly* $3|2^3 + 1$. *Let us now assume that for some* $k \in \mathbb{N}$ *we have* $3^k|(2^3)^k + 1$. *Then there exists an integer m such that* $m.3^k = (2^3)^k + 1$. *The binomial theorem gives* $(2^3)^{k+1} = ((2^3)^k)^3 = (m.3^k - 1)^3 = m^3.3^{3k} - m^2.3^{2k+1} + m.3^{k+1} - 1 = t.3^{k+1} - 1$, *where* $t = m^3.3^{2k-1} - m^2.3^k + m$ *is an integer . Hence* $3^{k+1}|(2^3)^{k+1} + 1$.

Example 3.18 *[1] p 51*

Prove that the sum of any three consecutive cubes is a multiple of 9.

Solution

Let $N = (n-1)^3 + n^3 + (n+1)^3$, *use the Binomial Theorem to conclude that* $N = 3n^3 + 6n = 3n(n^2+2)$. *There are three cases to consider. If* $n \equiv 0 \pmod 3$ *then N contains two factors of 3 and so is divisible by 9. If* $n \equiv \pm 1 (mod 3)$, *then* $n^2 + 2 \equiv (\pm 1)^2 + 2 \equiv 0 mod\ (3)$, *and again N has a second factor of 3 .*

3.4 Pigeonhole Principle

We will us The Pigeonhole Principle in some examples states that if n + 1 pigeons fly into n holes, there must be a pigeonhole containing at least two pigeons. This Apparently trivial principle is very powerful.

Theorem 3.19

If α is a real number and n is a positive integer, then there exist integers a and b with $1 \leq a \leq n$ such that $|a\alpha - b| < 1/n$.

Proof

Consider the $n+1$ numbers $0, \{\alpha\}, \{2\alpha\}, ..., \{n\alpha\}$ .These $n+1$ numbers are the fractional parts of the numbers $j\alpha, j = 0, 1, ..., n$, so that $0 \leq j\alpha < 1$ for $j = 0, 1, ..., n$. Each of these $n+1$ numbers lies in one of the n disjoint intervals

$0 \leq x < 1/n, 1/n \leq x < 2/n, ..., (j-1)/n \leq x < j/n, ..., (n-1)/n \leq x < 1$. Because there are $n+1$ numbers under consideration, but only n intervals, the pigeonhole principle tells us that at least two of these numbers lies in the same interval. Because each of these intervals has length $1/n$ and does not include its right end point, we know that the distance between two numbers that lies in the same interval is less than $1/n$. It follows that there exist integers j and k with $0 \leq j < k \leq n$ so that $|k\alpha - |j\alpha|| < 1/n$, we will now show that when $a = k - j$, the product $a\alpha$ is with in $1/n$ of an integer, namely, the integer $b = [k\alpha] - [j\alpha]$. To see this, note that

$|a\alpha - b| = |(k-j)\alpha - ([k\alpha] - [j\alpha])| = |(k\alpha - [k\alpha]) - (ja\alpha - [j\alpha])| = |k\alpha - j\alpha| < 1/n$. Furthermore , note that because $0 \leq j < k \leq n$, we have $1 \leq a = k - j \leq n$. Consequently, we have found integers a and b with $1 \leq a \leq n$ and $|a\alpha - b| < 1/n$ as desired .

Example 3.20

Let A be any set of twenty integers chosen from the arithmetic progression $1, 4, \ldots, 100$. Prove that there must be two distinct integers in A whose sum is 104.

Solution

We partition the thirty-four elements of this progression into nineteen groups:

$$\{1\}, \{52\}, \{4, 100\}, \{7, 97\}, \{10, 94\}, \ldots, \{49, 55\}.$$

Since we are choosing twenty integers and we have nineteen sets, by the Pigeonhole Principle, there must be two integers that belong to one of the pairs, which add to 104.

Example 3.21

Consider an open interval of length $1/n$ on the real line, where n is a positive integer.

Prove that the number of irreducible fractions a/b, $1 \leq b \leq n$, contained in the given interval is at most

$(n+1)/2$.

Solution

Suppose to the contrary that we have at least $\lceil \frac{n+1}{2} \rceil + 1 = a$ *fractions. Let* $s_k, t_k, 1 \leq k \leq a$ *be the set of numerators and denominators. The set of denominators is a subset of* $\{1, 2, \ldots, 2(a-1)\}$. *By the Pigeonhole Principle,* $t_i \mid t_k$ *for some* i, k, *say* $t_k = mt_i$. *But then*

$$\left| \frac{s_k}{t_k} - \frac{s_i}{t_i} \right| = \left| \frac{ms_i - s_k}{t_k} \right| \geq \frac{1}{n},$$

contradicting the hypothesis that the open interval is of length $1/n$.

Lemma 3.22 *[3] p150*

A set of m incongruent integers modulo m forms a complete set of residues modulo m .

Proof

Suppose that a set of m incongruent integers modulo m does not form a complete set of residues modulo m. This implies that at least one integer a is not congruent to any of the integers in the set. Hence , there is no integer in the set congruent modulo m to the remainder of a when it is divided by m . Hence, there can be at most $m-1$ *different remainders of the integers when they are divided by m. It follows (by the pigeonhole principle, which says that if more than n objects are distributed into n boxes, at least two objects are in the same box) that at least two integers in the set have the same remainder modulo m. This is impossible, because these integers are incongruent modulo m. Hence, any m incongruent integers modulo m form a complete system of residues modulo m .*

3.5 Principle of inclusion and exclusion

Example 3.23 *[8] P 70*

How many positive integers ≤ 1260 *are relatively prime to* 1260 *?*

Solution

As $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$*, the problem amounts to finding those numbers less than* 1260 *which are not divisible by* 2, 3, 5, *or* 7. *Let* A *denote the set of integers* ≤ 1260 *which are multiples of* 2, B *the set of multiples of* 3, *etc. By the Inclusion-Exclusion Principle,*

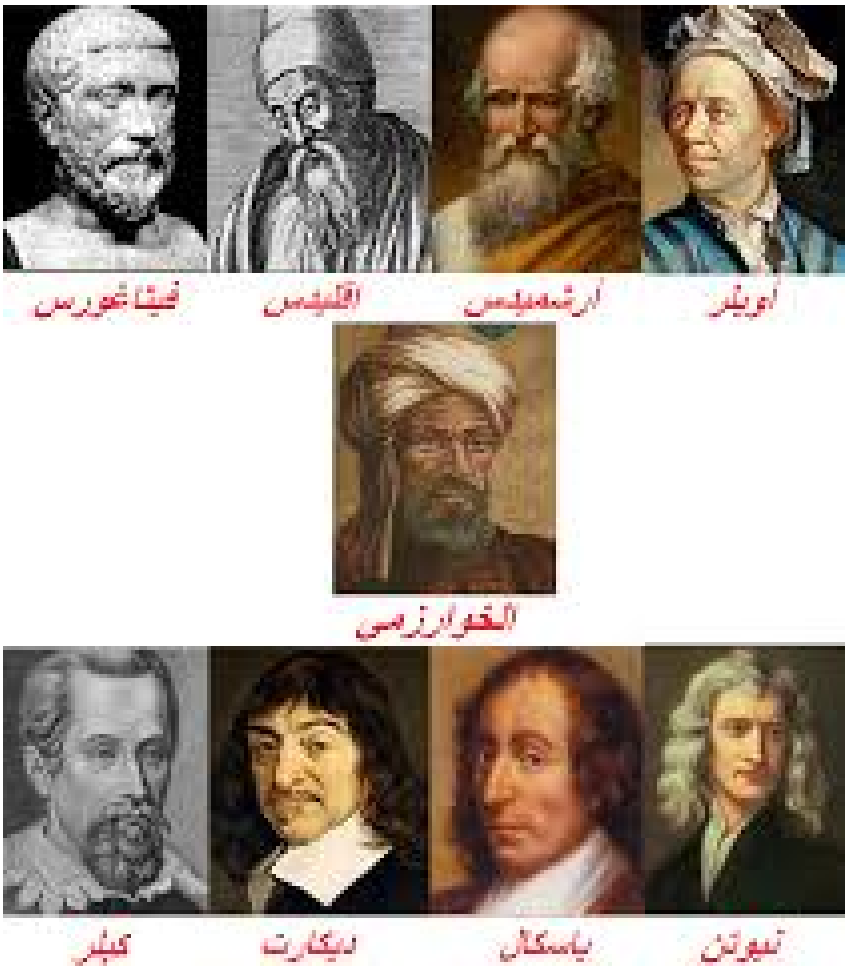
$$\begin{aligned}
|A \cup B \cup C \cup D| &= |A| + |B| + |C| + |D| \\
&\quad - |A \cap B| - |A \cap C| - |A \cap D| \\
&\quad - |B \cap C| - |B \cap D| - |C \cap D| \\
&\quad + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| \\
&\quad + |B \cap C \cap D| - |A \cap B \cap C \cap D| \\
&= 630 + 420 + 252 + 180 \\
&\quad - 210 - 126 - 90 - 84 \\
&\quad - 60 - 36 + 42 + 30 + 18 + 12 - 6 \\
&= 972.
\end{aligned}$$

The number of integers sought is then $1260 - 972 = 288$.

3.6 Conclusion

In this memory, we have studied some principles of elementary number theory. In fact, these principles are also, under certain conditions, principles in other mathematics disciplines. The work in this memory consisted of listing each of these principles on the one hand and then listing some of its applications on the other hand. We see as a horizon for this study the search for other applications that further enrich the mathematical universe.

Annexe


أويلر
أرشميدس
اقليدس
فيثاغورس
الخوارزمي
تيوتن
باسكال
ديكارت
كبلر

Bibliography

[1] Andrew Adler, John E. ClouryThe Theory of Numbers, Library of congress cataloging in publication data ,1995 .

[2] A.Boudaoud, cour théorie de nombre 1 er anne master algebre et mathématique discret, Université Mohamed Boudiaf M'sila, 2021 - 2022.

[3] Kenneth H. Rosen, Elementary Number Theory, London Pearson Education.2011

[4] Kenneth H. Rosen Discrete Mathematics and Its Application,Library of congress cataloging in publication data ,2007.

[5] Kenneth H. Rosen, Instructor's Solutions Manual,2011

[6] Ivan. Niven, An Introduction to the Theory of Numbers FIFTH EDITION University of Oregon Herbert S. Zuckerman University of Washington Hugh L. Montgomery University of Michigan ,1915.

[7] Kenneth H. Rosen, Elementary Number Theory and lts Applications ATT Informotion Systems Laboratories (formerly part of Bell Laborotories),2011.

[8] Santos.David A , Elementary Number Theory Notes ,Preprint,internet 9 (2002) (January 15, 2004).

[9] Herman, Jiri Radan Kucera, and Jaromir Simsa Equations and Inequalities Elementary Problems and Theorems in Algebra and Number Theory, Spring Sciznce and Buisness Media, 2012.

[10] Leonard,Dickson's history of the theory of numbers, an historical study with Mathimatical implication Delld fenster (*), societ e Mathimatic de france , 1999.

[11] *Titu Andreescu Ion Cucurezeanu ,An Introduction Dorin Andrica to Diophantine Equations A Problem-Based Approac,New yorkk Dordrecht Heidelberg London Library of Congress Control Number: 2010934856,2010*

ملخص

هدف هذا العمل هو تتبع تاريخ هذه النظريات، أي المبادئ المذكورة في هذه المذكرة، في مجال نظرية الأعداد، وإظهار أن لها تطبيقات عديدة ومتنوعة، مما يسمح لها بأن تُسمى مبادئ. لتوضيح أهمية هذه النظريات بشكل أفضل، قمنا بتضمين بعض التطبيقات لكل مبدأ.

كلمات مفتاحية

مبدأ الترتيب الجيد، مبادئ الاستقراء، مبدأاقفاص الحمام، مبدأ الإدراج والإقصاء، نظرية فيرمات ونظرية ويلسون .

Abstract

The aim of this work is to retrace the history of these theorems, namely the principles mentioned in this memoir, in the the field of number theory, and to show that they have numerous and varied applications, which allows them to be called principles. To better demonstrate the importance of these theorems, we include some applications of each principle.

Key words

Principle of well-ordering, Principle of induction, Pigeonhole lemma, Principle of inclusion-exclusion, Fermat's Theorem, Wilson theorem.

Résumé

Le but de ce travail est de retracer l'historique de ces théorèmes, a savoir les principes èvoquès dans ce mèmoire, dans le domaine de la théorie des nombres, et de montrer qu'ils ont des applications nombreuses et variées, ce qui leur permet d'être appelés principes. Pour mieux démontrer L'importance de ces théorèmes, nous incluons quelques applications de chaque principe.

Mot-clés

Principe du bon ordre, Principe d'induction, Lemme des tiroirs, Principe d'exclusion inclusion, théorèm de Fermat ,théorèm de wilson.