

Introduction to
**Number
Theory**

WOLFRAM  eTEXTBOOK SERIES

Introduction to Number Theory

A COMPUTATIONAL APPROACH

Lusine Sukiasyan | Charles Pooh

Introduction to Number Theory: A Computational Approach
by Lusine Sukiasyan and Charles Pooh
Copyright © 2026 by Wolfram Media, Inc.

Wolfram Media, Inc. | wolfram-media.com

ISBN 978-1-57955-115-5 (paperback)
ISBN 978-1-57955-114-8 (Wolfram Notebooks)
ISBN 978-1-57955-116-2 (Kindle)

Library of Congress Control Number: 2026944860

For information about permission to reproduce selections from this book, write to
permissions@wolfram.com. Sources for images that are not from the author's collection or in the
public domain:

p. 12: Trinity College, Cambridge^{*}. *p. 13: Diacritica*[†]. *p. 16: Nick Hillier, unsplash.com/license*. *p. 16: Trinity College, Cambridge*^{*}.
p. 23: Kmhkmh[†]. *p. 99: Max Ronnersjö*[†]. *p. 120: Emmanuel Garces Medina*. *p. 128: Rob Morris, Stephen Wolfram*. *p. 136: Luringen*[†].
p. 136: Alessandro Nassiri^{*}. *p. 137: Sonicdrewdriver*^{*}. *p. 138: Duncan.Hull*[†]. *p. 138: Alexander Sigachov*[†]. *p. 142: Ronald L. Rivest*^{*}.
p. 142: Duncan.Hull[†]. *p. 142: len adlmen*[†]. *p. 142: Royal Society uploader*[†]. *p. 154: David Eppstein*[†]. *p. 154: Erlangen Konrad
Jacobs*[†]. *p. 165: David Monniaux*[†]. *p. 165: WikiPedant, creativecommons.org/licenses/by-sa/2.5/deed.en*. *p. 165: George
Bergman*^{*}. *p. 173: Erlangen Konrad Jacobs*[†]. *p. 179: Mike Cowlshaw*[†].

^{*} creativecommons.org/licenses/by/4.0/deed.en

[†] creativecommons.org/licenses/by-sa/3.0/deed.en

[‡] creativecommons.org/licenses/by-sa/2.0/deed.en

Typeset with Wolfram Notebooks: wolfram.com/notebooks

Access the interactive Wolfram
Notebook edition of this textbook:



wolfr.am/eTextbook-NumberTheory

Opening these notebooks will require
Mathematica, Wolfram|One or Wolfram Player.

Most organizations have a site license for Mathematica.
To find out if you have access, visit wolfr.am/siteinfo.

If you don't have access through your organization,
visit wolfr.am/downloads.

Contents

Preface.....ix

Introduction

1 | What Is Number Theory?.....3

2 | Integers: The Basics.....15

3 | Primes and Composites.....23

Part 1 Exercises.....31

Primes and Divisibility

4 | Prime Factorization.....37

5 | Multiples and Divisors.....45

6 | Greatest Common Divisor.....51

Part 2 Exercises.....57

Modular Arithmetic

7 | Congruences.....61

8 | Modular Arithmetic.....67

9 | Chinese Remainder Theorem.....73

Part 3 Exercises.....77

Continued Fractions

10 | Real Number Representations.....83

11 | Continued Fractions.....91

12 | Best Rational Approximations.....99

Part 4 Exercises.....105

Diophantine Equations

13	Diophantine Equations.....	111
14	Linear Diophantine Equations.....	117
15	Diophantine Equations of Degree 2.....	123
	Part 5 Exercises.....	129

Cryptography

16	Cryptography.....	135
17	The RSA Algorithm.....	141
	Part 6 Exercises.....	147

Additional Topics

18	Primality Testing: Miller–Rabin.....	153
19	Factorization: Pollard’s Rho.....	159
20	Diophantine Equations: Hilbert’s Tenth Problem.....	163
21	The Riemann Zeta Function.....	167
22	Special Numbers.....	173
23	Numerical Systems.....	179
	Part 7 Exercises.....	187

Preface

Number theory has captivated the minds of mathematicians for centuries. Its origins are as ancient as mathematics itself, tracing back to the Babylonians and Greeks, yet it continues to be a thriving field of study in the present day. The simplicity and beauty of number theory lie in its fundamental questions about integers—questions that are easy to state but often difficult to answer.

Designed as an introduction, this book opens the door to the captivating field of number theory. The primary intention of the book is to serve all those who are embarking on their mathematical journey. The text is structured to guide readers through basic concepts, making it accessible to beginners. The joy of discovering unexpected patterns, the satisfaction of solving a tricky problem and the appreciation for the profound theorems that have shaped the field—these are experiences we hope to share with our readers.

The first chapters introduce the essential building blocks of number theory, such as divisibility, prime numbers and congruences. As the book progresses, we explore deeper topics of number theory, including continued fractions, Diophantine equations and its most important application in the modern world, cryptography. Each chapter is crafted to build on previous material, ensuring a smooth and logical progression of ideas.

While the main text provides the theoretical framework, the exercises play a crucial role in reinforcing understanding. They encourage readers to apply the concepts they have learned and to explore new ideas independently. The exercises will help you discover the potential of Wolfram Language. The otherwise tedious computations can be elegantly executed with blinding speed using Wolfram Language. Its outstanding functionality makes it effortless to illustrate, visualize and actively explore mathematical concepts. With a vast array of sophisticated algorithms—many of which are recent and original—it offers a powerful collection of functions that leverages nearly every major result in number theory. Wolfram Language has been an indispensable tool for over three decades. Its symbolic architecture and efficient algorithms create a distinct platform for conducting number theoretic experiments, making discoveries and providing proofs.

We hope that *Introduction to Number Theory: A Computational Approach* will serve as a valuable resource on your mathematical journey and that it will inspire a lifelong appreciation for the beauty and depth of number theory.

Acknowledgements

We would like to thank the R&D team of Wolfram Research, and particularly the Discrete Computation group, for their dedicated work on various aspects of this book.



Introduction

1 | What Is Number Theory?

Number theory studies numbers and their properties. The properties can range from very natural and easy ones to the most sophisticated.

Mathematicians use different methods and tools to study numbers. Hence, number theory has different subdivisions, which we'll address in this lesson.

The story of number theory begins over two millennia ago, and yet, it is a living subject. Newer and newer aspects and sides are discovered in number theory as mathematics and the world progresses. Number theory gets a new boost with each new era in science.

The latest discoveries in number theory and its importance are connected with electronic computers. Because modern computers can handle incredibly large numbers, we're now doing what our ancestors couldn't even dream about!

The Study of Numbers

Number theory is one of the oldest and most intuitive fields of mathematics. It studies numbers ... -3 , -2 , -1 , 0 , 1 , 2 , 3 , Number theory is also referred to as *higher arithmetic*.



Carl Friedrich Gauss

The great mathematician Carl Friedrich Gauss said:

“Mathematics is the queen of sciences and arithmetic the queen of mathematics.”

Number theory aims to discover fascinating and unexpected patterns in numbers.

One of the oldest and best-known unsolved problems in number theory is Goldbach's conjecture. It states that all even numbers greater than 2 are the sum of two prime numbers.

Fermat's last theorem is another very famous problem in number theory. It states that it is not possible to have the sum of two positive numbers taken to a power greater than 2 equal to a third positive number taken to the same power. It was solved in 1995 by English mathematician Andrew Wiles, who had been interested in it since the age of 10.

Number theory problems have fascinated generations of math enthusiasts.

The Subdivisions of Number Theory

In number theory, different methods and techniques are used to work with numbers. Based on that, the main subdivisions in number theory are:

1. Elementary number theory
2. Algebraic number theory
3. Diophantine geometry
4. Analytic number theory

Elementary Number Theory

How many ways are there to make \$2.00 from only nickels and quarters?

If x is the number of nickels and a nickel is 5 cents, and if y is the number of quarters and a quarter is 25 cents, and \$2.00 is 200 cents, then a solution to this problem satisfies the equation

$$5x + 25y = 200$$

This is not a simple equation because

- › The equation has two unknowns: x and y .
- › The solutions must be numbers 0, 1, 2, 3, ... because they represent the number of nickels and quarters (0 means no nickel or quarter is used).

Divide both sides of the equation by 5:

$$x + 5y = 40$$

Since solutions can be numbers 0, 1, 2, 3, ..., y can change from 0 to 8 (if you take $y = 9$, then no such x in numbers 0, 1, 2, 3, ... exists so that $x + 45 = 40$).

So the solutions to the equation are (40, 0), (35, 1), (30, 2), (25, 3), (20, 4), (15, 5), (10, 6), (5, 7) and (0, 8). Therefore, there are 9 ways to make \$2.00 from only nickels and quarters.

Elementary use of divisibility solves this problem. *Elementary number theory* is the subdivision of number theory that uses only elementary methods.

Algebraic Number Theory

Now consider the equation $x^2 + y^2 = 5$. The problem is to find solutions to the equation in numbers $0, \pm 1, \pm 2, \pm 3, \dots$

Subtract y^2 from both sides of the equation:

$$x^2 = 5 - y^2$$

Now substitute the values of y into the previous equation:

- If $y = 0$, then $x^2 = 5$ (no such x in numbers $0, \pm 1, \pm 2, \pm 3, \dots$ exists).
- If $y = 1$, then $x^2 = 4$ and $x = \pm 2$. Thus $(-2, 1)$ and $(2, 1)$ are solutions.
- If $y = 2$, then $x^2 = 1$ and $x = \pm 1$. Thus $(-1, 2)$ and $(1, 2)$ are solutions.

y cannot be greater than 2, because $5 - y^2$ must be non-negative.

Therefore, the solutions of the equation are $(-2, 1)$, $(2, 1)$, $(-1, 2)$ and $(1, 2)$.

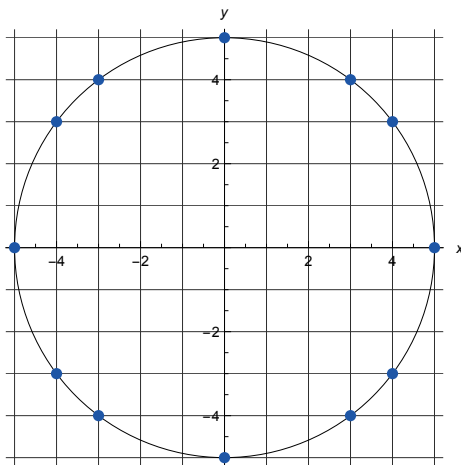
Algebraic methods were used to solve this problem. *Algebraic number theory* is the subdivision of number theory that uses algebraic methods.

Diophantine Geometry

Let's take a similar example, $x^2 + y^2 = 25$, and find its solutions geometrically.

Equations with two variables, like $x^2 + y^2 = 25$, define curves in a plane. The solutions of the equation are the integral points on the curve defined by the equation. Integral points are those with coordinates that are numbers $0, \pm 1, \pm 2, \pm 3, \dots$

The equation $x^2 + y^2 = 25$ is a circle with a radius of 5 around the origin. Its integral points are plotted in blue here:



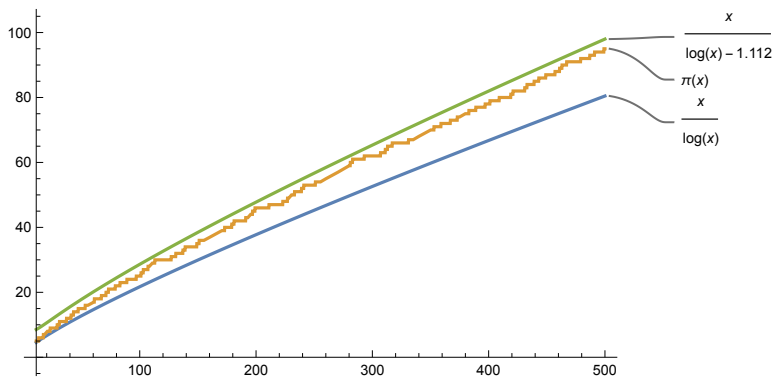
Therefore, the solutions are $(\pm 5, 0)$, $(\pm 4, \pm 3)$, $(\pm 3, \pm 4)$ and $(0, \pm 5)$.

Diophantine geometry is the subdivision of number theory that seeks to determine if such equations have solutions and how many solutions there are.

Analytic Number Theory

Prime numbers are those numbers that have two divisors: 1 and themselves. Examples of prime numbers are 2, 3, 5, 7, 11, How many prime numbers are there less than a certain limit, say x ?

Number theory can answer that question. The number of primes less than or equal to x , denoted as $\pi(x)$, is bounded below by $\frac{x}{\log x}$ and above by $\frac{x}{\log x - 1.112}$:



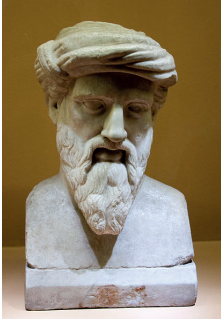
This problem has been solved using advanced mathematics. *Analytic number theory* is the subdivision of number theory that uses calculus to solve such problems.

Early Development

Based on archaeological artifacts, people have been able to count since prehistoric times. One of the earliest known counting artifacts is a 10,000-year-old bone with tally marks scratched into it that was found in the Congo region of Africa.

In the early stages of civilization, people had already developed a sense of studying numbers. Surviving tablets, papyri and temple carvings show that ancient Mesopotamian, Egyptian, Chinese and Indian cultures understood numbers. A fragment of a clay tablet called *Plimpton 322* is the oldest known artifact related to arithmetic. Carved into *Plimpton 322* is a list of numbers that satisfy the Pythagorean theorem, $a^2 + b^2 = c^2$. There are too many and the numbers are too big to be merely an accident.

Even though there is evidence of ancient people studying numbers, there was no general number theory. The classical Greeks were the first to develop many mathematical theories, and number theory is among those achievements. The Greeks merged the unusual and vaguely mystical teachings of the *Pythagoreans* with the harsh logic present in Euclid's *Elements* (c. 300 BC).



Pythagoras

Across southern Italy, devoted followers of *Pythagoras* promoted his theory that numbers united everything and could be used to understand concepts and theories ranging from the motion of planets to harmonies in music. Based on his philosophy, Pythagoreans also believed certain numbers had quasi-rational properties. As an example, they believed perfect numbers had special significance.



Euclid

On the opposite end of the spectrum was *Euclid*. He presented a more practical number theory, one without embellishments. Book VII of Euclid's *Elements* defined each number as “a multitude composed of units,” each prime number as being “measured by a unit alone,” composite numbers as those that are not prime and perfect numbers as those that equal the sum of their “parts.” Euclid used these definitions to prove a sequence of theorems that led to number theory being considered a mathematical pursuit rather than a numerological endeavor.



Diophantus of Alexandria

Diophantus of Alexandria was an especially famous Greek mathematician. He wrote *Arithmetica*, a book featuring many significant equations, including some so important that people have named them Diophantine equations.

After Rome fell, there were no significant advances in Europe for a millennium, but there were great strides in number theory being made by Chinese and Indian mathematicians. *Sun Zi*, a Chinese mathematician, solved many Diophantine equations in his quest to understand astronomy and calendars.

During this period, Indian scholars were also working on number theory. *Brahmagupta* worked on the Pell equation (which was named incorrectly) in the seventh century. Other Indian mathematicians developed a base-10 notation system that was later adopted by mathematicians and societies all over the world; it is now known as the Hindu-Arabic numerals. People still use these numerals today because they are simple and easy to use.

Because it was between East and West trade routes, the Islamic world soaked up the mathematical achievements in other parts of the world and added its own accomplishments. It became an influential center for mathematical knowledge. *Thābit ibn Qurrah* was one of the prominent figures in Islamic mathematics; he was active in ninth-century Baghdad. His focus was amicable numbers, a Greek problem. Thābit ibn Qurrah found a second pair of these amicable numbers: 17 296 and 18 416.

Later Developments

When Renaissance-era Europe was first exposed to the mathematics developed in the Islamic world, they did not consider number theory a serious subject. Between 1400 and 1650, there were significant advancements in the fields of geometry, algebra and probability, as well as logarithms and analytic geometry being discovered. Despite these advancements, people still perceived number theory as a recreational hobby.



Pierre de Fermat

Number theory remained a recreational hobby until a French magistrate who loved numbers and had too much recreational time, *Pierre de Fermat*, asked the questions and identified problems that would shape number theory. Of the few works he published, his most notable are Fermat's little theorem, an instrumental tool for modern number theorists, and Fermat's last theorem, one of mathematics' most famous statements.

Fermat rarely supplied proofs, so many did not see the value in number theory. The invention of calculus near the end of the seventeenth century was an additional hurdle for mainstream acceptance of the field of number theory. Given the practicality of calculus, scholars in many disciplines rushed to solve real-world problems with calculus. They viewed number theory as too pure and divorced from practical problems in physics, astronomy and engineering.



Leonhard Euler

Leonhard Euler, a prominent Swiss mathematician in the eighteenth century, was one of the most prolific and influential mathematicians ever, and he eventually popularized number theory and Fermat's works. When Euler began to work on number theory, he was initially indifferent to it, as most mathematicians were, but his correspondence with *Christian Goldbach* changed his mind. Goldbach was so enthusiastic about number theory and Fermat's work that it started to rub off on Euler. After Euler's conversion to number theory, the wider mathematical community finally started taking the field seriously.

In contrast to Fermat rarely publishing proofs of his work, Euler spent 50 years publishing over a thousand pages of research and proofs. Many of his proofs proved Fermat's theorems. He published his proof of Fermat's little theorem in 1736. There were only three pairs of amicable numbers known when Euler started working on them, but he found 58 new pairs through his work.

Once Euler had legitimized the field of number theory, progress was fast.



Joseph – Louis Lagrange

Joseph-Louis Lagrange published a proof that every number can be defined as the sum of fewer than five squares in 1770. This was another one of Fermat's theorems. Lagrange then proved Wilson's theorem.



Carl Friedrich Gauss

Carl Friedrich Gauss published *Disquisitiones Arithmeticae* in 1801, a book that became a foundational work in number theory. The book organized and summarized the work of previous mathematicians, as well as contained Gauss's fresh proofs and theories. Gauss observed that "one of the most important and useful" problems was finding prime factors for composite numbers. He published the first proof of the unique factorization theorem in modern mathematics.



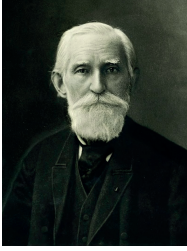
Peter Gustav Lejeune Dirichlet

Among *Peter Gustav Lejeune Dirichlet's* important contributions to the field of number theory is a proof that the arithmetic progression $a, a + b, a + 2b, a + 3b, \dots$ must have an unlimited number of primes if the integers a and b have no common divisor other than 1. This proof was exceptional because Dirichlet used calculus techniques to solve the problem. The combination of calculus and number theory was surprising but ingenious and paved the way for analytic number theory, a new branch of number theory.

The prime number theorem was one of the greatest advancements in nineteenth-century mathematics. Gauss was one of the first to work on this theorem; his work was based on examining log tables and prime numbers.



Bernhard Riemann



Pafnuty Chebyshev



Jacques Hadamard



Charles Jean de la Vallée – Poussin

There were several other important advancements in nineteenth-century mathematics after Dirichlet developed analytic number theory from the combination of calculus and number theory. In 1896, *Jacques Hadamard* and *Charles Jean de la Vallée-Poussin* finally proved the prime number theorem, and their work was based on the dramatic progress made by *Bernhard Riemann* and *Pafnuty Chebyshev* before them.

Number theory research expanded even more in the next century. Mathematicians began to specialize in subfields like geometric number theory, algebraic number theory and combinatorial number theory, complements to classic and analytic number theory. These new subfields developed the subject beyond anything Fermat could have dreamed of, with new abstract concepts and sophisticated techniques.



Srinivasa Ramanujan

Srinivasa Ramanujan was an influential mathematician in the early twentieth century. Ramanujan had limited formal training, but he made several important discoveries in his brief life.

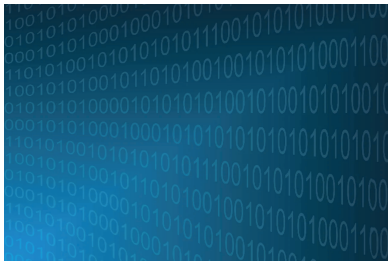
Later in the twentieth century, the invention of electronic computers gave number theorists the ability to answer questions faster. After this, number theory became a practical field. It was used to design encryption systems for governments and businesses. Number theory helped to factor very large numbers into primes, a process the code user knows and the code breakers do not.

Number Theory in Today's World

Number theory is no longer considered as the purest of pure math.

The number theorist Leonard Dickson once said, “Thank God that number theory is unsullied by any application.”

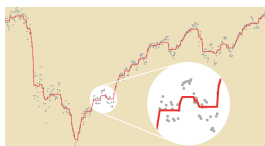
But such a view is not true now. In 1974, Donald Knuth said, “...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations.”



Cryptography depends heavily on number theory.



The security of information transfers depends on number theory.

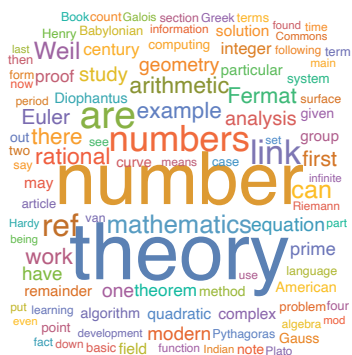


Number theory has applications in numerical analysis.



Number theory is used in random and quasi – random number generation.

Why Study Number Theory?



This lesson has already covered the main advantages of number theory in fields such as computer science and mathematics. However, not every student wants to be a computer scientist or mathematician!

Pythagoras's dictum that "all is number" is well known. So knowing the fundamentals of number theory is to know a bit more about the world surrounding us.

In some areas, like calculus, a person needs to start learning from first principles. Some other areas are best mastered by diving right in. Number theory is one of the latter. It is the most natural of all mathematical disciplines, and the introductory parts of it do not need many prerequisites.

Above all else, it is important to study number theory because it is a major milestone in any student's career. A solid grasp of number theory is essential for senior undergraduates in STEM fields to excel in their studies.

Knowing how to solve problems that baffled even the Greeks, as well as the greatest minds in mathematics, is sure to boost one's ego and self-confidence.

Summary

- *Number theory* studies properties of numbers.
- Number theory is one of the earliest branches in mathematics.
- The main subdivisions in the field of number theory are *elementary number theory*, *algebraic number theory*, *Diophantine geometry* and *analytic number theory*.
- Number theory was once considered the purest of pure math. However, it has important applications in the modern world.

2 | Integers: The Basics



“God made the integers, all else is the work of man.” — Leopold Kronecker

Number theory is a branch of mathematics that primarily studies *integers* and their properties.

Whole numbers, or integers, are the first mathematical objects humans created. They used them to count objects and do other simple things, like keeping records or doing commercial transactions.

You might think that the numbers 1, 2, 3, ... can only have a few simple properties. If that was true, then number theory would have finished many centuries ago.

In the twenty-first century, there are still many properties being discovered. Many questions got their answers, and many more questions are arising.

This chapter introduces integers and basic operations on them, along with one of the key notions in number theory: *divisibility*.

Interesting Number Paradox



The interesting number paradox is a humorous paradox that states:

Every natural number is interesting!

This paradox is proved by using the method of contradiction:

- › Assume there exists a non-empty set of uninteresting natural numbers.
- › This set would contain the smallest uninteresting number.
- › But that number would possess a rather interesting quality—it would be the smallest uninteresting number, and thus it would be an interesting number!

Hence, the result is a contradiction.

1729



Godfrey Hardy Srinivasa Ramanujan

Have a look at the number 1729.

It doesn't look special at first glance. That's certainly what British mathematician Godfrey Hardy was thinking when once, in a taxi from London, he noticed its number. He was on his way to visit Indian mathematician Srinivasa Ramanujan in the hospital.

“As he entered the room where Ramanujan lay in bed, he declared it ‘rather a dull number,’ adding that he hoped that was not a bad omen. ‘No, Hardy,’ said Ramanujan, ‘it is a very interesting number.’ It is the smallest number expressible as the sum of two cubes in two different ways.” —Hofstadter (1989)

The two different ways are

$$1729 = 1^3 + 12^3$$

$$1729 = 9^3 + 10^3$$

Integers

An *integer* is a number that can be written without a fractional component.

For example,

$$-25, 6, 0, 7887$$

are all integers.

The set of integers is often denoted by a doublestruck $\mathbb{Z}$ standing for the German word *Zahlen* (numbers).

The set $\mathbb{Z}$ of all integers consists of:

› *Positive integers:*

$$1, 2, 3, 4, \dots$$

› *Negative integers:*

$$-1, -2, -3, -4, \dots$$

› *Zero:*

$$0$$

Thus, the set $\mathbb{Z}$ is

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Positive integers are sometimes called natural numbers and are denoted by $\mathbb{N}$.

Lowercase, italicized Latin letters usually represent integers:

$$a, b, c, d, \dots$$

Some Basic Properties

› The *sum* of two integers is an integer:

$$10 + 15 = 25$$

$$58 - 36 = 22$$

$$-14 + 5 = -9$$

› The *product* of two integers is an integer:

$$15 * 87 = 1305$$

$$-96 * 2 = -192$$

$$(-89) * (-8) = 712$$

› If a is an integer, there is no such integer x that:

$$a < x < a + 1$$

In other words, there is no integer between two consecutive integers. For example, there is no integer between 1 and 2, 2 and 3, 3 and 4, etc.

- › If a and b are integers and $a * b = 1$, then

$$a = b = 1 \text{ or } a = b = -1$$

- › Note that the *quotient* of two integers need not be an integer:

$$20 / 4 = 5$$

$$15 / 4 = 3.75$$

Laws of Exponents

For natural numbers n and m and real numbers a and b , all the following are true:

- › $(a^n)^m = a^{n*m}$:

$$(3^2)^3 = 3^6$$

- › $(a * b)^n = a^n * b^n$:

$$(5 * 12)^2 = 5^2 * 12^2$$

- › $a^n * a^m = a^{n+m}$:

$$4^3 * 4^5 = 4^8$$

Properties of Inequalities

If a , b and c are integers, then the following inequalities hold:

- › $a < b$ and $b < c \Rightarrow a < c$:

$$4 < 6 \text{ and } 6 < 10 \Rightarrow 4 < 10$$

- › $a < b \Rightarrow a + c < b + c$:

$$8 < 11 \Rightarrow 8 + 2 < 11 + 2$$

- › $a < b$ and $0 < c \Rightarrow a * c < b * c$:

$$7 < 9 \Rightarrow 7 * 3 < 9 * 3$$

- › $a < b$ and $c < 0 \Rightarrow a * c > b * c$:

$$7 < 9 \Rightarrow 7 * (-3) > 9 * (-3)$$

- › Given two numbers a and b , only one of the following holds: $a = b$, $a < b$, $a > b$:

$$8, 4 : 8 > 4$$

$$14, 20 : 14 < 20$$

$$9, 9 : 9 = 9$$

Divisibility of Integers

The number d *divides* the number n if there is an integer k such that

$$n = d * k$$

$n | d$ expresses the fact that n divides d , or d is divisible by n .

Also, n is a *divisor* of d and d is a *multiple* of n .

For example, 12 is divisible by 3 as

$$12 = 3 * 4$$

However, 12 is not divisible by 5 as no integer k exists such that $12 = 5 * k$.

The table here shows numbers up to 100 that are divisible by 3:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Divisibility Properties

If n , m and d are integers, then the following statements hold:

- › A number is divisible by itself (*reflective property*):

$$n = n * 1$$

- › If d divides n and n divides m , then d divides m (*transitive property*):

$$3 \text{ divides } 9 \text{ and } 9 \text{ divides } 81 \Rightarrow 3 \text{ divides } 81$$

- › If d divides n and m , then d divides $a * n + b * m$ (*linearity property*):

$$4 \text{ divides } 8 \text{ and } 4 \text{ divides } 12 \Rightarrow 4 \text{ divides } a * 8 + b * 12$$

- › If d divides n , then $a * d$ divides $a * n$ (*multiplication property*):

$$5 \text{ divides } 15 \Rightarrow 5 * a \text{ divides } 15 * a$$

- › If $a * d$ divides $a * n$ and $a \neq 0$, then d divides n (*cancellation property*):

$$5 * a \text{ divides } 15 * a \Rightarrow 5 \text{ divides } 15$$

- › 1 divides every integer:

$$n = 1 * n$$

- › Every integer divides 0:

$$0 = n * 0$$

- › If d and n are positive and d divides n , then $d \leq n$:

$$4 \text{ divides } 24 \Rightarrow 4 \leq 24$$

One can easily prove these properties using only the definition of divisibility.

Parity

An integer is *even* if it is divisible by 2 and is *odd* otherwise.

For example, the number 14 is even:

$$14 = 7 * 2$$

On the contrary, the number 17 is odd:

$$17 / 2 = 8.5$$

Even numbers leave a remainder of 0 when divided by 2:

$$14 = 7 * 2 + 0$$

So the set of even numbers can be defined as:

$$\{2k, k \in \mathbb{Z}\}$$

Odd numbers leave a remainder of 1 when divided by 2:

$$17 = 2 * 8 + 1$$

The set of odd numbers can be defined as:

$$\{2k + 1, k \in \mathbb{Z}\}$$

Divisors of a Number

This lesson already covered what a divisor of a number is.

The divisors of 40, for example, are:

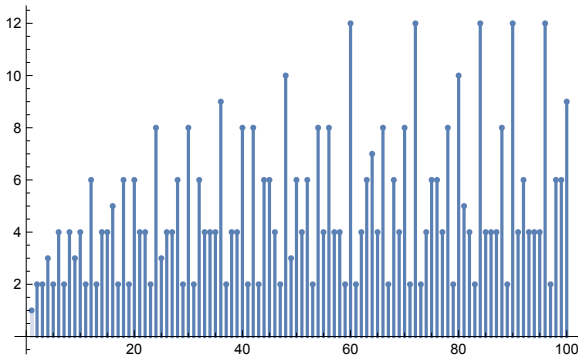
$$\{1, 2, 4, 5, 8, 10, 20, 40\}$$

The divisors of 17 are

$$\{1, 17\}$$

A number is always divisible by 1 and itself. With 17, these are its only divisors, whereas 40 has other divisors as well.

Here is a plot of the number of divisors of numbers up to 100:



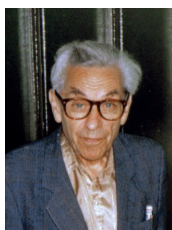
Some numbers have only two divisors, and others have over two.

This difference leads to the following subdivision of integers: *prime* and *composite* numbers.

Summary

- Number theory is a branch of mathematics that primarily studies integers.
- An *integer* is a number that can be written without a fractional component.
- The set of integers consists of zero, positive integers and negative integers.
- The number d *divides* the number n if there is an integer k such that $n = d * k$.
- An integer is *even* if it is divisible by 2 and is *odd* otherwise.

3 | Primes and Composites



“God may not play dice with the universe, but something strange is going on with the prime numbers.” — Paul Erdos

There are so many types of integers based on their properties. The simplest classification among the integers is dividing integers into even and odd numbers.

The most important and peculiar subgroup of integers is *prime numbers*. Prime numbers serve as the building blocks of integers.

Prime numbers have fascinated generations of math enthusiasts. What are the primes like? Where can one find prime numbers? How can the prime factors of an integer be computed?

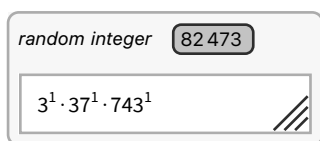
Some of these questions were the cause of whole new fields of mathematics. Some of them are still unanswered, and who knows, maybe you’ll be the one to find the answers!

This lesson is about prime and composite numbers, as well as about their properties.

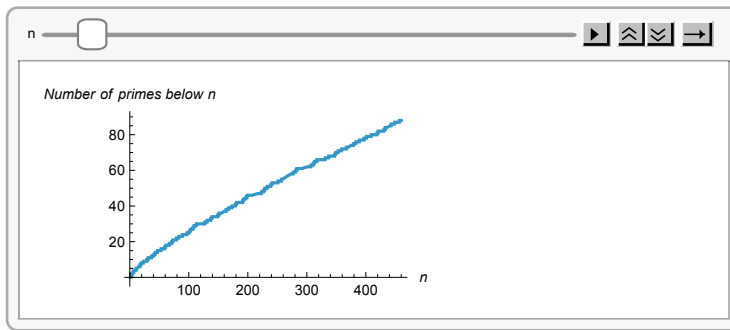
Peculiar Prime Numbers

Here are some peculiar facts about prime numbers:

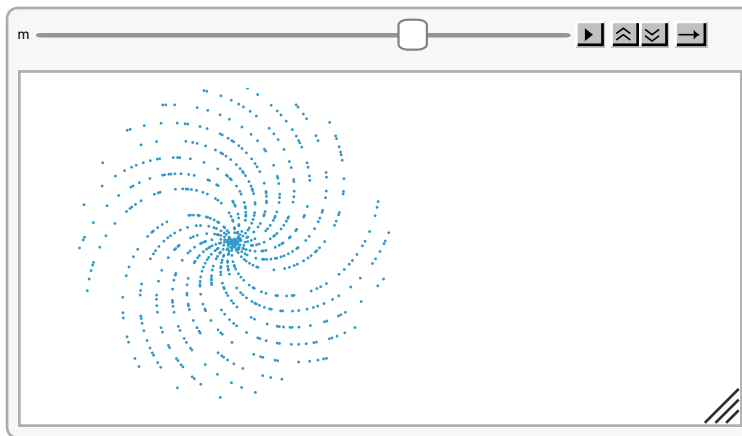
- › Every integer is a prime or a product of primes:



- › There are infinitely many prime numbers:



- › Prime numbers make a spiral when plotted in polar coordinates:



- › As of September 2025, the largest known prime number is $2^{136\,279\,841} - 1$. It has over 41 million digits. It was found on October 12, 2024.
- › The organization the *Great Internet Mersenne Prime Number Search* (GIMPS) is dedicated to finding larger and larger primes. GIMPS is responsible for finding the 51 most recently discovered largest prime numbers. George Woltman founded the organization in 1996.
- › Prime numbers prevent cybercrime. RSA encryption systems keep information transfers (like digital credit card transactions) secure by combining simple and well-known principles of prime numbers.
- › In his 1985 book, *Contact*, the famous astronomer *Carl Sagan* postulates that prime numbers could feature in signals from aliens.

Prime and Composite Numbers

An integer $p > 1$ is said to be *prime* if the only positive divisors of p are 1 and p .

For example, the only positive divisors of 19 are

$$\{1, 19\}$$

So 19 is a prime number.

A number that is greater than 1 and not prime is called *composite*.

The divisors of 24 are

$$\{1, 2, 3, 4, 6, 8, 12, 24\}$$

So 24 is a composite number.

The number 1 is considered neither prime nor composite. Mathematicians used to think 1 was a prime number, but since so many definitions and applications do not apply to the number 1, it is now considered to be in a separate class.

The number 2 is the only even prime number. All the other even numbers are divisible by 2, so they are composite.

Composite Numbers and Prime Divisors

If n is composite, then it has a prime divisor p such that $p^2 \leq n$.

Consider the number 97.

The theorem says that if 97 is composite, then it has a prime divisor less than 10 because

› $9^2 = 81$ is less than 97

› $10^2 = 100$ is greater than 97

So it has one of these primes as a divisor:

$$\{2, 3, 5, 7\}$$

Since none of these primes divides 97, it is a prime number.

Euclid's First Theorem

Euclid's first theorem states:

If p is prime and p divides $a * b$, then p divides a or p divides b .

For example, take $p = 3$.

72 is divisible by 3. On the other hand,

$$72 = 8 * 9$$

The theorem states that either 8 or 9 is divisible by 3. Of course, it is 9 that is divisible by 3.

72 can also be represented as

$$72 = 4 * 18$$

In this case, it is 18 that's divisible by 3.

More generally, if a prime p divides the product $a_1 * a_2 * \dots * a_n$, then p divides at least one of the factors.

Sequence of Primes



The set of all primes is often denoted by a doublestruck $\mathbb{P}$.

The prime numbers up to 100 are

{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}

It is easy to presuppose that prime numbers can end only in 1, 3, 7 and 9, except for 2 and 5.

Sieve of Eratosthenes

“Sift the Two’s and Sift the Three’s,
The Sieve of Eratosthenes.
When the multiples sublime,
The numbers that remain are Prime.”

Civilizations as early as the ancient Greeks had a simple algorithm to find all the prime numbers below a certain limit. It was called the *Sieve of Eratosthenes*.

The Sieve of Eratosthenes starts by marking the multiples of primes as composites.

Using this method, let’s find all the prime numbers less than or equal to 100.

› Create a table of consecutive integers from 2 to 100:

2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67
68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100

- The first prime number is 2. Cross out all the multiples of 2 (except for 2 itself):

2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67
68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100

2	3		5		7		9		11	
13		15		17		19		21		23
	25		27		29		31		33	
35		37		39		41		43		45
	47		49		51		53		55	
57		59		61		63		65		67
	69		71		73		75		77	
79		81		83		85		87		89
	91		93		95		97		99	

- The second prime number is 3. Cross out all the multiples of 3 (except for 3 itself):

2	3		5		7		9		11	
13		15		17		19		21		23
	25		27		29		31		33	
35		37		39		41		43		45
	47		49		51		53		55	
57		59		61		63		65		67
	69		71		73		75		77	
79		81		83		85		87		89
	91		93		95		97		99	

2	3		5		7				11	
13				17		19				23
	25				29		31			
35		37				41		43		
	47		49				53		55	
		59		61				65		67
			71		73				77	
79				83		85				89
	91				95		97			

➤ The next prime number is 5. Cross out all the multiples of 5 (except for 5 itself):

2	3		5		7				11	
13				17		19				23
	25				29		31			
35		37				41		43		
	47		49				53		55	
		59		61				65		67
			71		73				77	
79				83		85				89
	91				95		97			

2	3		5		7				11	
13				17		19				23
					29		31			
		37				41		43		
	47		49				53			
		59		61						67
			71		73				77	
79				83						89
	91						97			

- › The next prime number is 7. Cross out all the multiples of 7 (except for 7 itself):

2	3		5		7				11	
13				17		19				23
					29		31			
		37				41		43		
	47		49				53			
		59		61						67
			71		73				77	
79				83						89
	91						97			

2	3		5		7				11	
13				17		19				23
					29		31			
		37				41		43		
	47						53			
		59		61						67
			71		73					
79				83						89
							97			

- › The next step would be to cross out every 11th number in the list after 11, but they are all already crossed out because these numbers (22, 33, 44, 55, 66, 77, 88, 99) are also multiples of smaller primes:

2	3		5		7				11	
13				17		19				23
					29		31			
		37				41		43		
	47						53			
		59		61						67
			71		73					
79				83						89
							97			

The remaining numbers are all primes below 100.

Infinitude of Primes

Are there infinitely many primes?

- › The number of primes below 1 000 000 is 78 498.
- › The number of primes below 10 000 000 is 664 579.
- › The number of primes below 100 000 000 is 5 761 455.
- › ...

All of this data suggests the following theorem, which is known as *Euclid's theorem*:

The number of primes is infinite.

Euclid offered a proof published in his work *Elements*. Several variations on Euclid's proof exist.

Formula for Primes

Another natural question to ask about the sequence of primes is the following:

Is there a simple general formula for the n^{th} prime? A formula by which you can calculate the value of the n^{th} prime for any n without any prior information about its value?

Certain formulas do produce many primes:

- › The expression $x^2 + x + 41$ gives primes for all of the first 39 natural numbers.
- › The expression $x^2 - 79x + 1601$ gives primes for all of the first 79 natural numbers.

However, no such simple formula exists that yields a prime number for every x , regardless of the use of cubes or higher powers.

In fact, in 1752, Goldbach showed that no polynomial in x with integer coefficients can be prime for all x .

Summary

- An integer is said to be *prime* if its only positive divisors are 1 and itself.
- A number greater than 1 and not prime is called *composite*.
- If n is composite, then it has a prime divisor p such that $p^2 \leq n$.
- *Euclid's first theorem* states that if p is prime and p divides $a * b$, then p divides a or p divides b .
- The number of primes is infinite.
- There is no known simple, general formula for determining the n^{th} prime.

Part 1 Exercises

1.1 What are main the subdivisions in number theory?

Solution

The main subdivisions in number theory are:

- 1) Elementary number theory
- 2) Algebraic number theory
- 3) Diophantine geometry
- 4) Analytic number theory

1.2 Which of the following numbers are integers?

4, 1.5, -3, $\frac{6}{11}$, 19, 0.6

Solution

Use the function IntegerQ in Wolfram Language:

```
In[ ]:= IntegerQ [ 4 ]
```

```
Out[ ]= True
```

```
In[ ]:= IntegerQ [ 1.5 ]
```

```
Out[ ]= False
```

```
In[ ]:= IntegerQ [ -3 ]
```

```
Out[ ]= True
```

```
In[ ]:= IntegerQ [  $\frac{6}{11}$  ]
```

```
Out[ ]= False
```

```
In[ ]:= IntegerQ [ 19 ]
```

```
Out[ ]= True
```

```
In[ ]:= IntegerQ [ 0.6 ]
```

```
Out[ ]= False
```

So the integers are {4, -3, 19}.

1.3 Divide the following group of integers into even and odd integers:

26, 18, 70, 21, 68, 15, 30, 52, 44, 7

Solution

Use the functions EvenQ and OddQ in Wolfram Language:

```
In[ ]:= Select [ {26, 18, 70, 21, 68, 15, 30, 52, 44, 7}, EvenQ]
```

```
Out[ ]:= {26, 18, 70, 68, 30, 52, 44}
```

```
In[ ]:= Select [ {26, 18, 70, 21, 68, 15, 30, 52, 44, 7}, OddQ]
```

```
Out[ ]:= {21, 15, 7}
```

1.4 Using the theorem about composite numbers and prime divisors, show that 53 is a prime number.

Solution

Suppose 53 is composite. The theorem says it has a prime divisor p such that $p^2 \leq 53$, or $p \leq \sqrt{53}$:

```
In[ ]:= Sqrt [53] // N
```

```
Out[ ]:= 7.28011
```

So the potential prime divisors are {2, 3, 5, 7}.

But none of these divide 53:

```
In[ ]:= Divisible [53, {2, 3, 5, 7}]
```

```
Out[ ]:= {False, False, False, False}
```

We arrive at a contradiction, and 53 is, in fact, prime.

1.5 Using the sieve of Eratosthenes method, find all prime numbers less than or equal to 25.

Solution

Create a table of consecutive integers from 2 to 25:

```
In[ ]:= p = Range [2, 25]
```

```
Out[ ]:= {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25}
```

The first prime number is 2. Cross out all the multiples of 2 (except for 2 itself):

```
In[ ]:= p2 = Select [p, (! Divisible [ #, 2] || # == 2) &]
```

```
Out[ ]:= {2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25}
```

The second prime number is 3. Cross out all the multiples of 3 (except for 3 itself):

```
In[ ]:= p3 = Select [p2, (! Divisible [ #, 3] || # == 3) &]
```

```
Out[ ]:= {2, 3, 5, 7, 11, 13, 17, 19, 23, 25}
```

The next prime number is 5. Cross out all the multiples of 5 (except for 5 itself):

```
In[ ]:= p5 = Select [p3, (! Divisible [ #, 5] || # == 5) &]
```

```
Out[ ]:= {2, 3, 5, 7, 11, 13, 17, 19, 23}
```


The next prime number is 7. Notice that there aren't any multiples of 7 left on our list (except for 7 itself):

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$$

These remaining numbers are all the primes below 25.

Now, let's use the function PrimeQ in Wolfram Language to see if all the numbers are indeed prime:

```
In[*]:= PrimeQ[ {2, 3, 5, 7, 11, 13, 17, 19, 23} ]
```

```
out[*]= {True, True, True, True, True, True, True, True, True}
```

What if there are primes less than or equal to 25 that didn't end up in the final list? Use the function `CompositeQ` in Wolfram Language to check:

$$\text{In}[\bullet] := \text{Complement}[p, p5]$$

```
Out[*]= {4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25}
```

```
In[*]:= CompositeQ [ { 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25 } ]
```

[illegible]

Primes and Divisibility

4 | Prime Factorization

“The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers.” — Bill Gates

Can you imagine representing integers in a canonical, systematic way? As a sum or a product of specific numbers? If we could do it, we then could generalize so many things about numbers. We could just examine those little bricks that make up the number we want to examine.

Well, it is quite the reality! It turns out, every number can be represented as a product of primes. We call it prime factorization.

The *prime factorization* of integers is one of the most important results in number theory. It says that every natural number can be written uniquely as a product of primes.

Much of what follows depends on *unique factorization*. It gives an alternative, conceptually simpler way to find a lot of numerical characteristics of a number.

It turns out, factoring large numbers is a hard task. In fact, secure transfers of information (like digital credit card transactions) rely on that very fact. Returning to the Bill Gates quote, if we could find an easy way to factor large numbers, then the entire system of secure transactions would fail.

This lesson will be about prime factorization and some things derived from it.

Prime Factorization

Prime numbers are the building blocks of integers.

Intuitively, that means that every integer is built out of prime numbers.

Particularly, every integer is a product of primes.

Look at these examples:

$$6 = 2 * 3$$

$$99 = 3 * 3 * 11$$

$$600 = 2 * 2 * 2 * 3 * 5 * 5$$

$$17 = 17$$

As seen, the primes in the product are neither distinct nor arranged in any order; for example,

$$600 = 2 * 2 * 2 * 3 * 5 * 5$$

$$600 = 2 * 3 * 2 * 5 * 2 * 5$$

$$600 = 3 * 5 * 2 * 2 * 2 * 5$$

A nice representation of prime factorization would be achieved by arranging primes in increasing order and associating sets of equal primes into single factors:

$$600 = 2^3 * 3 * 5^2$$

Unique Factorization

Up until now, there has been no discussion about the uniqueness of such a representation, but a quick examination of special cases immediately indicates that this is true.

The *fundamental theorem of arithmetic* states that every integer greater than 1 can be represented as a product of prime factors in only one way, apart from the order of the factors.

Formally, one can represent the factorization of n as

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

where all the p_i are distinct.

Unique factorization is one of the main reasons 1 is not considered a prime number. If 1 were considered a prime number, the factorization into primes would no longer be unique:

$$7 = 7 * 1 = 7 * 1 * 1 = \dots$$

Examples

Let's play with the factorization of certain integers.

Obviously, the prime factorization of primes is just themselves because they are already prime:

$$23 = 23$$

$$127 = 127$$

Here are some other examples of prime factorization:

$$8 = 2^3$$

$$18 = 2 * 3^2$$

$$40 = 2^3 * 5$$

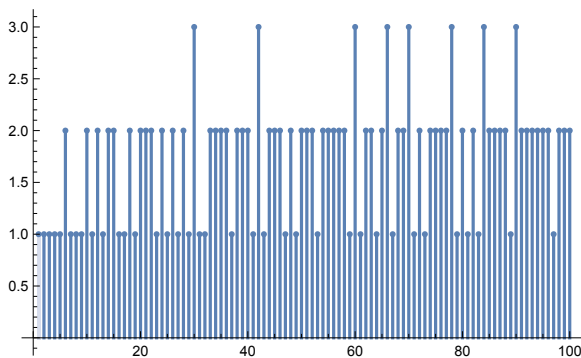
$$875 = 5^3 * 7$$

$$1200 = 2^4 * 3 * 5^2$$

$$2310 = 2 * 3 * 5 * 7 * 11$$

Number of Distinct Prime Factors

The plot below shows the number of distinct prime factors of the first 100 numbers:



That number cannot be greater than three in the first 100 integers because the product of the first four primes is 210 ($2 * 3 * 5 * 7 = 210$), which is greater than 100.

The first number that has three distinct prime factors is 30 since $2 * 3 * 5 = 30$.

Numerical Characteristics of a Number

Have a look at the prime factorization of 1200:

$$1200 = 2^4 * 3 * 5^2$$

In terms of numbers, it says:

- › 1200 has three distinct prime factors.
- › The exponents of primes in the factorization are {4, 1, 2}.
- › The sum of the exponents of primes in the factorization is 7.

This all is not just for fun. There are very important functions in number theory that represent all these characteristics.

Liouville Function

The first function of that kind is the *Liouville function* λ , which is defined as follows:

If $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, then

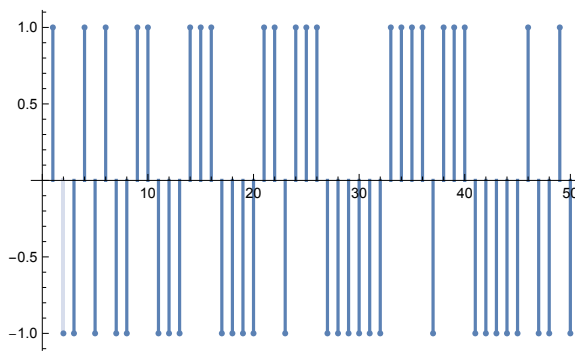
$$\lambda(n) = (-1)^{k_1 + \dots + k_m}$$

The value of $\lambda(1)$ is 1 by definition.

So it only takes two values, -1 and 1 :

n	1	2	3	4	5	6	7	8	9	10
$\lambda(n)$	1	-1	-1	1	-1	1	-1	-1	1	1

Here is the plot of the Liouville function for numbers up to 50:



Moebius Function

The next very important function is the *Moebius function* μ , which is defined as follows:

If $n > 1$, write $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. Then

$$\mu(n) = (-1)^m, \text{ if } k_1 = k_2 = \dots = k_m = 1$$

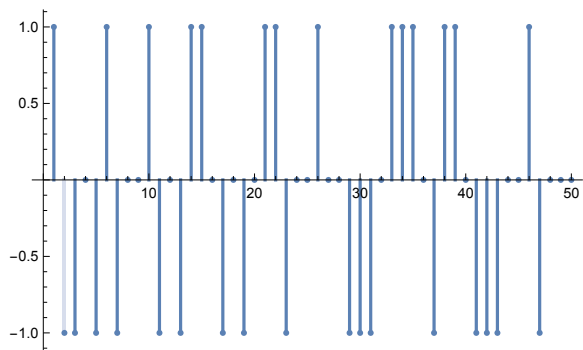
$$\mu(n) = 0 \text{ otherwise}$$

The value of $\mu(1)$ is 1 by definition.

So it takes three values, -1 , 0 and 1 :

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Here is the plot of the Moebius function for numbers up to 50:



Mangoldt's Function

The next function is *Mangoldt's function* Λ . It plays a central role in the distribution of primes. It is defined as follows:

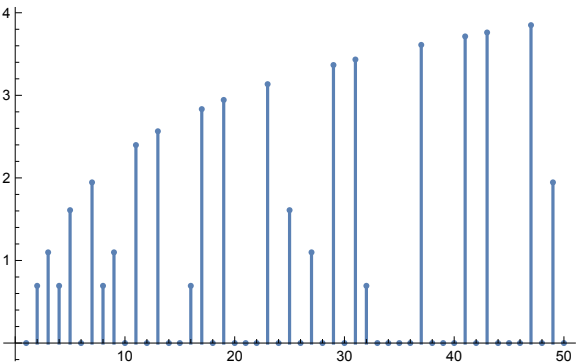
$$\Lambda(n) = \log(p), \text{ if } n = p^m \text{ for some prime } p \text{ and } m \geq 1$$

$$\Lambda(n) = 0 \text{ otherwise}$$

Here is a short table of values of $\Lambda(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$	0	$\log(2)$	$\log(3)$	$\log(2)$	$\log(5)$	0	$\log(7)$	$\log(2)$	$\log(3)$	0

Here is the plot of Mangoldt's function for numbers up to 50:



Prime Omega Functions

The *prime omega functions* $\omega(n)$ and $\Omega(n)$ count the number of prime factors of a natural number n .

Prime Omega Function $\omega(n)$

The *prime omega function* $\omega(n)$ counts the number of distinct primes of n .

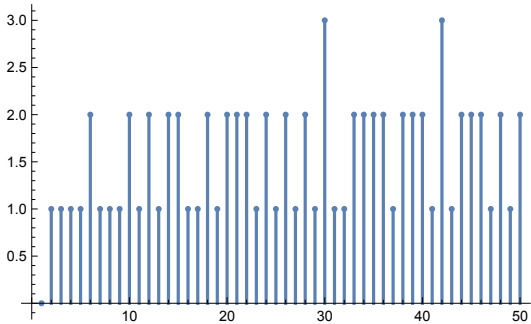
If $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, then

$$\omega(n) = m$$

Here is a short table of values of $\omega(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\omega(n)$	0	1	1	1	1	2	1	1	1	2

Here is the plot of $\omega(n)$ for all numbers up to 50:



Prime Omega Function $\Omega(n)$

The *prime omega function* $\Omega(n)$ counts the total number of prime factors of n , considering their multiplicity:

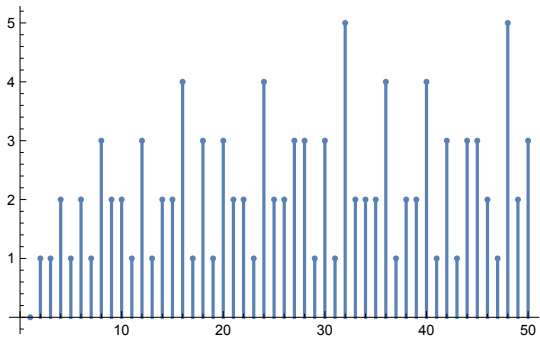
If $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, then

$$\Omega(n) = k_1 + \dots + k_m$$

Here is a short table of values of $\Omega(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\Omega(n)$	0	1	1	2	1	2	1	3	2	2

Here is the plot of $\Omega(n)$ for all numbers up to 50:



Summary

- Every integer is a product of primes.
- The primes in the product are neither distinct nor arranged in any specific order.
- The *fundamental theorem of arithmetic* states that every integer greater than 1 can be represented as a product of prime factors in only one way, apart from the order of the factors.
- There are some very important functions connected with *prime factorization*.

5 | Multiples and Divisors

The divisibility property is one of the most important notions of number theory.

So far, we talked about primes and prime factorization of numbers. These deal with divisors and multiples of numbers. By only adding and subtracting numbers, we won't get anywhere in both daily life and science.

The book has already partially covered the divisibility of integers and the classification of numbers based on their number of divisors.

This lesson will introduce the *multiples* and *divisors* of a number, as well as other notions derived from them.

Multiples

Take a certain integer, for example, 7, and multiply it by all natural numbers:

$$7 * 2 = 14$$

$$7 * 3 = 21$$

$$7 * 4 = 28$$

...

All those numbers have the form $7 * k$, where k is an arbitrary integer.

Those numbers are the multiples of 7.

It is said that b is a *multiple* of a if $b = k * a$ for some integer k .

The integer k is called the *multiplier*.

Therefore, the number of multiples of an integer is infinite.

You can represent the set of multiples of 6 as:

$$\{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, \dots, 6 * k, \dots\}$$

where k is an arbitrary integer.

Divisors

Consider the number 6. What are its divisors? Check by dividing 6 by all the numbers below 6:

$$6 \div 1 = 6$$

$$6 \div 2 = 3$$

$$6 \div 3 = 2$$

$$6 \div 4 = 4 * 1 + 2$$

$$6 \div 5 = 5 * 1 + 1$$

$$6 \div 6 = 1$$

The divisors of 6 are numbers that leave a remainder of 0 when divided by 6, so they are

$$\{1, 2, 3, 6\}$$

It is said that b is a *divisor* of a if there is an integer k such that $a = k * b$.

For example, the divisors of 180 are

$$\{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180\}$$

Since no divisor can be greater than the number, the number of divisors of an integer is finite.

It is very easy to see that all numbers have 1 and themselves as divisors:

$$a = a * 1$$

$$a = 1 * a$$

Number of Divisors

- › The only number with just one divisor is 1.
- › Numbers with two divisors are prime numbers.

Therefore, the smallest number with just two divisors is 2.

Which numbers have exactly three divisors?

Look at the numbers

$$4, 9, 25, 49$$

They have three divisors each.

For example, the divisors of 4 are 1, 2 and 4.

They have one more thing in common. They are all squares of a prime number:

$$4 = 2^2, \quad 9 = 3^2, \quad 25 = 5^2, \quad 49 = 7^2$$

Actually, a number has exactly three divisors if and only if it is a square of a prime. You will find out why shortly.

Formula for the Number of Divisors

Prime factorization gives a simple way of finding some numerical characteristics of a number.

Once you know the prime factorization of the number, you can answer certain questions about the number right away.

Consider the number 1480. Its prime factorization is

$$1480 = 2^3 * 5 * 37$$

Suppose d is one of its divisors.

The prime factorization shows that the only primes that can occur as factors of d are 2, 5 and 37.

Furthermore, 2 can occur as a factor at most three times, while 5 and 37 can each occur at most once. So, the possible divisors of 1480 are

$$d = 2^a * 5^b * 37^c$$

where the choices are

$$a = 0, 1, 2, 3$$

$$b = 0, 1$$

$$c = 0, 1$$

That means that the number of divisors of 1480 is

$$(3 + 1) * (1 + 1) * (1 + 1) = 4 * 2 * 2 = 16$$

because these choices can be combined in all possible ways.

So, the number of divisors of $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ is

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1)$$

Knowing this, let's now prove that a number has exactly three divisors if and only if it is a square of a prime.

➤ Squares of primes have three divisors.

Consider a square of a prime number p^2 . Its prime factorization is

$$p^2 = p^2$$

The formula says it has $2 + 1 = 3$ divisors.

So squares of primes have three divisors.

➤ Only squares of primes have three divisors.

Suppose number $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ has three divisors. That means

$$(k_1 + 1)(k_2 + 1) \dots (k_m + 1) = 3$$

3 can be represented as a product of integers in only one way: $3 = 3 * 1 * 1 * \dots * 1$.

So in the previous formula, only one factor is 3, say

$$k_1 + 1 = 3$$

$$k_2 = 2$$

The other factors are 1, so all the other $k_i = 0$.

So n has the representation $n = p_1^2$, and therefore is a square of a prime.

The Divisor Function

$d(n)$ or $\tau(n)$ usually denotes the number of divisors of n .

Another natural thing to do with a finite set of numbers, like the divisors of a number, is to consider their sum. For example, the sum of the divisors of 36 is 91:

$$1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 + 36 = 91$$

The sum of the divisors of a number is, again, very important in mathematics and is usually denoted by $\sigma(n)$.

These two functions are actually special cases of a more general function, the divisor function.

The *divisor function* is denoted by $\sigma_k(n)$ and are defined as sums of the k^{th} powers of the integer n .

For example, $\sigma_2(36)$ and $\sigma_3(36)$ are 1911 and 55 261, respectively:

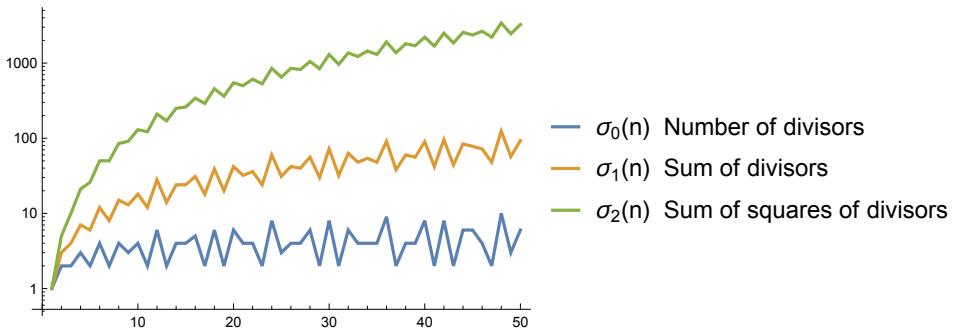
$$1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 9^2 + 12^2 + 18^2 + 36^2 = 1911$$

$$1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 + 36 = 55\,261$$

Now, take $n = 1, 2, \dots, 10$ and change the value of $k = 0, 1, 2, 3, 4$:

n	$\sigma_0(n)$	$\sigma_1(n)$	$\sigma_2(n)$	$\sigma_3(n)$	$\sigma_4(n)$
1	1	1	1	1	1
2	2	3	5	9	17
3	2	4	10	28	82
4	3	7	21	73	273
5	2	6	26	126	626
6	4	12	50	252	1394
7	2	8	50	344	2402
8	4	15	85	585	4369
9	3	13	91	757	6643
10	4	18	130	1134	10642

Compare the following plots:



Summary

- b is a *multiple* of a if $b = k * a$ for some integer k . The integer k is called the *multiplier*.
- The number of multiples of an integer is infinite.
- b is a *divisor* of a if there is an integer k such that $a = k * b$.
- The number of divisors of an integer is finite.
- The *divisor function* is denoted by $\sigma_k(n)$ and are defined as sums of the k^{th} powers of the integer n .

6 | Greatest Common Divisor

We believe that you already have a familiarity with the concepts we will discuss in this lesson.

Let us take the fraction $\frac{8}{12}$. Usually we try to reduce it to its lowest terms by canceling out factors common to 8 and 12. This operation does not change the value of the fraction. First, we cancel out by 2:

$$\frac{8}{12} = \frac{4}{6}$$

We can now see that we can do it again:

$$\frac{4}{6} = \frac{2}{3}$$

So we canceled 4 out of both 8 and 12. Why 4? Because 4 is the greatest common divisor of 8 and 12.

The notions of the *greatest common divisor (GCD)* and the *least common multiple (LCM)* are basic yet important in elementary number theory.

These are straight consequences of divisors and multiples.

This lesson will give theoretical knowledge about them, as well as the logic behind them.

Greatest Common Divisor

Take two numbers, for example, 8 and 12. They are both divisible by 4, so they have a common divisor.

Actually, 4 is not the only number that divides both 8 and 12. Their common divisors are

$$(1, 2, 4)$$

The set of common divisors of two numbers always contains 1 and is a finite set.

Because of the latter, it is natural to ask for the greatest common divisor of two numbers.

Formally, the *greatest common divisor (GCD)* of two or more integers is the largest positive integer that can divide all of the integers.

Usually, the greatest common divisor of the numbers m and n is denoted by $\gcd(m, n)$.

Here are some examples:

$$\gcd(8, 28) = 4$$

$$\gcd(5, 15) = 5$$

$$\gcd(9, 30) = 3$$

The following is a table of the greatest common divisors of the first 100 pairs of integers:

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1	2	1	2
3	1	1	3	1	1	3	1	1	3	1
4	1	2	1	4	1	2	1	4	1	2
5	1	1	1	1	5	1	1	1	1	5
6	1	2	3	2	1	6	1	2	3	2
7	1	1	1	1	1	1	7	1	1	1
8	1	2	1	4	1	2	1	8	1	2
9	1	1	3	1	1	3	1	1	9	1
10	1	2	1	2	5	2	1	2	1	10

Relatively Prime Numbers

The term relatively prime numbers intuitively prompts one to guess the relationship between those numbers: they do not have any common divisors except for 1.

Two integers are called *relatively prime* (mutually prime, coprime) when the only positive integer that can divide both of them is 1.

For example, the numbers 4 and 18 are not relatively prime as they both have 2 as a divisor:

$$4 \div 2 = 2$$

$$18 \div 2 = 9$$

However, the numbers 3 and 8 are relatively prime as their only common divisor is 1.

The definition of relatively prime numbers is equivalent to their greatest common divisor being 1.

As in the previous examples:

$$\gcd(4, 18) = 2$$

So they are not relatively prime.

On the contrary, 3 and 8 are relatively prime:

$$\gcd(3, 8) = 1$$

Bézout's Identity

Bézout's identity is a basic theorem in number theory.

Let a and b be integers with greatest common divisor d . Then, there exist integers x and y such that

$$a * x + b * y = d$$

In general, integers of the form $a * x + b * y$ are exactly the multiples of d .

The integers x and y are called *Bézout coefficients*. They are not unique.

Bézout coefficients can be determined using the extended Euclidean algorithm.

For example, take $a = 12$ and $b = 15$. The greatest common divisor of these numbers is 3. Find x and y such that

$$12x + 15y = 3$$

Even without computing, one can see that $x = -1$ and $y = 1$ as

$$-12 + 15 = 3$$

Least Common Multiple

Now take the numbers 6 and 9. They can both be used to divide 18. So they have a common multiple.

But 18 is not the only number that can be divided by both 6 and 9. Their common multiples are

$$\{18, 36, 72, \dots\}$$

Any number of the form $18 * k$, where k is a natural number, is a common multiple of 6 and 9.

More generally, two numbers a and b always divide at least $a * b$, and consequently, $a * b * k$.

18 is less than $6 * 9$ and is still divisible by both.

Since the set of common multiples of a number is infinite, it is very natural to ask for the least common multiple of two numbers, which can be smaller than their product, as you saw.

Formally, the *least common multiple (LCM)* of two or more integers is the smallest positive integer divisible by all of the integers.

Usually, the least common multiple of the numbers m and n is denoted by $\text{lcm}(m, n)$.

Here are some examples:

$$\text{lcm}(8, 12) = 24$$

$$\text{lcm}(5, 15) = 15$$

$$\text{lcm}(3, 7) = 21$$

There is an interesting relationship between the greatest common divisor and the least common multiple:

$$\text{gcd}(a, b) * \text{lcm}(a, b) = a * b$$

If the greatest common multiple of two numbers is 1, then and only then does the least common multiple equal the product.

The following is a table of the least common multiples of the first 100 pairs of integers:

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	2	6	4	10	6	14	8	18	10
3	3	6	3	12	15	6	21	24	9	30
4	4	4	12	4	20	12	28	8	36	20
5	5	10	15	20	5	30	35	40	45	10
6	6	6	6	12	30	6	42	24	18	30
7	7	14	21	28	35	42	7	56	63	70
8	8	8	24	8	40	24	56	8	72	40
9	9	18	9	36	45	18	63	72	9	90
10	10	10	30	20	10	30	70	40	90	10

GCD, LCM and Prime Factorization

Prime factorization also allows one to easily find the greatest common divisor and the least common multiple of numbers.

Take two numbers, for example, 600 and 252. Their prime factorization is

$$600 = 2^3 * 3 * 5^2$$

$$252 = 2^2 * 3^2 * 7$$

Rewrite it in a way that the prime factors are present in both factorizations:

$$600 = 2^3 * 3^1 * 5^2 * 7^0$$

$$252 = 2^2 * 3^2 * 5^0 * 7^1$$

The greatest common divisor of 600 and 252 is then

$$2^{\min(3,2)} * 3^{\min(1,2)} * 5^{\min(2,0)} * 7^{\min(0,7)} = 2^2 * 3^1 * 5^0 * 7^0 = 12$$

And the least common multiple of 600 and 252 is

$$2^{\max(3,2)} * 3^{\max(1,2)} * 5^{\max(2,0)} * 7^{\max(0,7)} = 2^3 * 3^2 * 5^2 * 7^1 = 12\,600$$

Summary

- The *greatest common divisor (GCD)* of two or more integers is the largest positive integer that can divide all of the integers.
- *Bézout's identity* says that for a given a, b , there exist integers x and y such that $a * x + b * y = d$. In this equation, d represents the greatest common divisor of the integers a and b .
- Two integers are *relatively prime* (mutually prime, coprime) when the only positive integer that can divide both of them is 1.
- The *least common multiple (LCM)* of two or more integers is the smallest positive integer divisible by all of the integers.

Part 2 Exercises

2.1 Which is the smallest number that has five distinct prime factors?

Solution

That number is the product of the first five primes. You can use the function `Prime` in Wolfram Language to find first five primes:

```
In[•]:= Prime [ { 1, 2, 3, 4, 5 } ]
```

```
Out[•]= { 2, 3, 5, 7, 11 }
```

So that number is 2310:

```
In[•]:= 2 * 3 * 5 * 7 * 11
```

```
Out[•]= 2310
```

`FactorInteger` is a function in Wolfram Language that gives a list of the prime factors of the integer together with their exponents. For example:

```
In[•]:= FactorInteger [ 60 ]
```

```
Out[•]= { { 2, 2 }, { 3, 1 }, { 5, 1 } }
```

The prime factorization of 2310 is:

```
In[•]:= FactorInteger [ 2310 ]
```

```
Out[•]= { { 2, 1 }, { 3, 1 }, { 5, 1 }, { 7, 1 }, { 11, 1 } }
```

The resulted table has length 5, and since the powers are 1, it is indeed the smallest number that has five distinct prime factors.

2.2 Which of the following numbers has a repeated prime factor?

10, 88, 145

Solution

A repeated prime factor means that the Moebius function value is 0. You can use the function `MoebiusMu` in Wolfram Language to identify the required number:

```
In[•]:= MoebiusMu [ 10 ]
```

```
Out[•]= 1
```

In[$\ast$]:= **MoebiusMu [88]**

Out[$\ast$]= 0

In[$\ast$]:= **MoebiusMu [145]**

Out[$\ast$]= 1

So the answer is 88.

- 2.3** Suppose there is 72 dollars worth of cash in the form of one-dollar bills. List all the numbers such that the money can be distributed equally among a group of that many people.

Solution

It's easy to realize that the numbers among which the money can be distributed equally are the factors of 72.

You can find these using the function `Divisors` in Wolfram Language:

In[$\ast$]:= **Divisors [72]**

Out[$\ast$]= { 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72 }

So that sum of money can be distributed equally among a group of 1, 2, 3, 4, 6, 8, 9, 12, 18, 36 or 72 people.

- 2.4** A tortoise jumps 3 cm for each jump. A hare jumps 11 cm for each jump. A kangaroo jumps 1232 cm for each jump. If there is a mark for every centimeter, which is the first mark that all three of them will cross?

Solution

The problem is asking for the least common multiple (LCM) of 3, 11 and 1232.

You can calculate it by using the function `LCM` in Wolfram Language:

In[$\ast$]:= **LCM [3, 11, 1232]**

Out[$\ast$]= 3696

So the first mark that all three of them will cross is at 3696 cm.

Modular Arithmetic

7 | Congruences



Carl Friedrich Gauss

Congruences are of great practical importance both in number theory and everyday life.

Gauss introduced the theory of congruences and created a new branch of number theory by introducing a remarkable notation. However, traces of congruence theory predate Gauss, appearing in ancient arithmetic check rules for arithmetical computations.

Congruences have several important properties, making them highly useful in number theory.

This lesson is about congruences. Let's dive in!

Congruency Relation

A congruence is simply a statement about divisibility.

It is said that the numbers a and b are *congruent* modulo m if a and b leave the same remainder when divided by m .

For example, both 17 and 22 leave the remainder 2 when divided by 5. Thus, they are congruent modulo 5.

In mathematical terms, it is said that a is congruent to b modulo m if

$$m \mid (a - b)$$

That is to say, m divides the difference $a - b$.

That a and b are congruent modulo m is denoted as

$$a \equiv b \pmod{m}$$

The number m is the *modulus* of the congruence.

$a \not\equiv b \pmod{m}$ means a is not congruent to b .

Congruency Relation and Modulo Operation

Students very often confuse congruences with the modulo operation because of the similar notation.

The *modulo operation* gives the remainder of the division of a by n . The notation is a modulo n , which is often abbreviated as $a \bmod n$.

For example,

$$5 \bmod 2 = 1$$

The parentheses in the case of *congruences* $\bmod(m)$ indicate that it applies to the entire equation, not just the right-hand side.

More precisely, what the statement $a \equiv b \pmod{m}$ asserts is that a and b have the same remainder when divided by m :

$$a \bmod m = b \bmod m$$

In short, congruence is a relation between two numbers, whereas the modulo operation is a binary operation.

Examples

Some example of congruency relation:

$$25 \equiv 1 \pmod{4}$$

$$19 \equiv 7 \pmod{12}$$

$$22 \equiv 10 \pmod{6}$$

$$50 \equiv 20 \pmod{15}$$

Some general examples:

$$n \equiv 1 \pmod{2}, \text{ if } n \text{ is odd}$$

$$a \equiv b \pmod{1}, \text{ for every } a \text{ and } b$$

The case $m = 1$ is not interesting at all and generally it is considered that $m \geq 2$.

Properties of Congruences

First of all, congruence is an equivalence relation, which means that for all a, b, c and m , the following statements are true:

› Reflexivity:

$$a \equiv a \pmod{m}$$

Proof: $a - a = 0, m \mid 0 \Rightarrow m \mid a - a$

› Symmetry:

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

Proof: $m \mid a - b \Rightarrow m \mid b - a$

› Transitivity:

$$a \equiv b \pmod{m} \text{ and } b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

Proof: $m \mid a - b, m \mid b - c, (a - b) + (b - c) = a - c \Rightarrow$ (linearity property of division) $m \mid a - c$

Residue Class

Consider a fixed modulus m . The set of all integers x such that

$$x \equiv a \pmod{m}$$

is called the *residue class* of a modulo m .

For example, take $m = 5$ and $a = 2$. The question is to find such x that $x \equiv 2 \pmod{5}$ or $5 \mid (x - 2)$. From this, it follows that

$$x - 2 = 5k \text{ for some number } k$$

All of those numbers have the form

$$x = 2 + 5k$$

where k is an integer.

So the residue class of 2 modulo 5 is

$$\{..., -18, -13, -8, -3, 2, 7, 12, 17, 22, 27, ...\}$$

Residue Classes of 5

In the same way, it's easy to find other residue classes of modulo 5.

The residue class of 0 modulo 5 is

$$\{..., -15, -10, -5, 0, 5, 10, 15, 20, 25, 30, ...\}$$

The residue class of 1 modulo 5 is

$$\{..., -14, -9, -4, 1, 6, 11, 16, 21, 26, 31, ...\}$$

The residue class of 3 modulo 5 is

$$\{\dots, -17, -12, -7, -2, 3, 8, 13, 18, 23, 28, \dots\}$$

The residue class of 4 modulo 5 is

$$\{\dots, -16, -11, -6, -1, 4, 9, 14, 19, 24, 29, \dots\}$$

Is it any use to continue and consider the residue class of 5 modulo 5? No, because that will be the same as the residue class of 0 modulo 5 and so on.

It is easy to notice that the union of the previous five sets is the set of all integers, so no integer is missed.

Complete Residue System

A *complete residue system* is a set of integers containing one element from each class (the modulo is fixed).

For example, complete residue systems modulo 5 are

$$\{20, 16, 37, 18, 24\}$$

$$\{-5, 21, 102, -17, 4\}$$

There are endlessly many complete residue systems, so it is interesting and important to consider the *least residue system modulo n* , which is the following set of integers:

$$\{0, 1, 2, \dots, n-1\}$$

For example, the least residue system modulo 5 is

$$\{0, 1, 2, 3, 4\}$$

Linear Congruences

In ordinary algebra, an equation of the form

$$a * x = b$$

is called a linear equation.

As congruences are, in a way, analogues to equations, it is very natural that there are analogues to linear equations as well.

A congruence of the form

$$a * x \equiv b \pmod{m}$$

where x is an unknown integer is called a *linear congruence*.

Some examples of linear congruences:

$$2x \equiv 8 \pmod{10}$$

$$11x \equiv 20 \pmod{6}$$

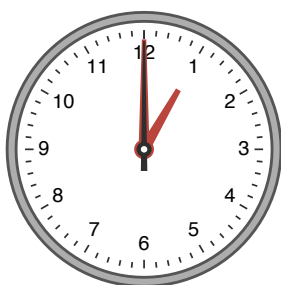
$$2x \equiv 5 \pmod{8}$$

It's easy to see that the latter has no solutions since $2x - 5$ is odd and therefore not divisible by 8.

Summary

- Numbers a and b are *congruent modulo m* if a and b leave the same remainder when divided by m .
- The number m is the *modulus* of the congruence.
- The set of all integers x such that $x \equiv a \pmod{m}$ is called the *residue class* of a modulo m .
- A *complete residue system* is a set of integers containing one element from each class.
- The least residue system modulo n is the set $\{0, 1, 2, \dots, n - 1\}$.
- A congruence of the form $a * x \equiv b \pmod{m}$ where x is an unknown integer is called a *linear congruence*.

8 | Modular Arithmetic



Number theory has an algebra of its own, known as *modular arithmetic*.

A significant number of astronomical and chronological problems related to periodicity may be framed within a number theoretical context. A prominent example is determining the day of the week corresponding to a given date. To simplify things, instead of using the names for the days of the week, we can number them 1–7, reflecting their recurring seven-day cycle.

Congruence theory also helps create round-robin schedules for various competitions, from chess to baseball.

Algebra initially served as a concise notation for arithmetic operations. Likewise, congruences serve as a symbolic representation of divisibility.

In this lesson, you will see that modular arithmetic is a strictly finite science, and you will grasp the intuition behind periodic events in life, the most basic of which is the 12-hour clock.

The Idea Behind Modular Arithmetic

Modular arithmetic is the basis for so many things in our daily life.

All of the things that are periodic can be interpreted as a modular arithmetic.

The periodic things in our lives are countless:

- › A minute has 60 seconds
- › An hour has 60 minutes
- › A week has seven days
- › ...

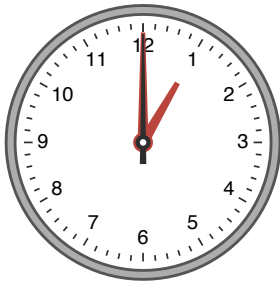
For instance, the statement “today is Thursday” reflects the congruence property modulo 7 of the days passed since a fixed date.

This property is typically more significant than the actual number of days that have passed since creation.

Clock Arithmetic

Modular arithmetic is perhaps most familiar as a generalization of the arithmetic of the clock.

Picture the face of a clock:



The numbers go from 1 to 12:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

When you get to 13 o'clock, it becomes 1 o'clock again. When you get to 14 o'clock, it becomes 2 o'clock and so on.

So in this clock-based system, you only care where you are in relation to the numbers 1 to 12. In this world, 1, 13, 25, 37, ... are all thought of as the same thing, as are 2, 14, 26, 38, ... and so on.

Mathematically speaking, “ $13=1+$ some multiple of 12”, or “the remainder when 13 is divided by 12 is 1.”

Modular Arithmetic: Addition

It's not a coincidence that the congruence symbol $\equiv$ looks like the equal sign. Congruences indeed possess many properties of equations.

If

$$a \equiv b \pmod{m}$$

$$c \equiv d \pmod{m}$$

Then

$$a \pm c \equiv b \pm d \pmod{m}$$

This is quite easy to prove.

For example,

$$7 \equiv 43 \pmod{6}$$

$$4 \equiv 28 \pmod{6}$$

The property says that

$$7 + 4 \equiv 43 + 28 \pmod{6}$$

$$11 \equiv 71 \pmod{6}$$

and

$$7 - 4 \equiv 43 - 28 \pmod{6}$$

$$3 \equiv 15 \pmod{6}$$

Modular Arithmetic: Multiplication

There is a similar property about the product.

If

$$a \equiv b \pmod{m}$$

$$c \equiv d \pmod{m}$$

Then

$$a * c \equiv b * d \pmod{m}$$

This is again easily provable. For example,

$$9 \equiv 25 \pmod{4}$$

$$10 \equiv 2 \pmod{4}$$

The property says that

$$9 * 10 \equiv 25 * 2 \pmod{4}$$

$$90 \equiv 50 \pmod{4}$$

Modular Arithmetic: Exponentiation

The next property is about powers.

If

$$a \equiv b \pmod{m}$$

Then

$$a^n \equiv b^n \pmod{m}$$

For example,

$$2 \equiv 7 \pmod{5}$$

The property says that

$$2^2 \equiv 7^2 \pmod{5}$$

$$2^3 \equiv 7^3 \pmod{5}$$

$$2^4 \equiv 7^4 \pmod{5}$$

and so on.

Notice that in all these cases the modulus is fixed.

Arithmetic Modulo 12

In modular arithmetic, numbers “wrap around” when reaching a certain value, which is the modulus.

A good example, as already mentioned, can be arithmetic modulo 12, which is known as *clock arithmetic*.

If it is 10 o'clock now, then in 5 hours, the clock will show 3 o'clock instead of 15 as

$$15 \equiv 3 \pmod{12}$$

Here, it is more preferable to write $15 \equiv 3 \pmod{12}$ rather than $3 \equiv 15 \pmod{12}$, although both are correct:

- All there is are numbers from 1 to 12, and they are usually written on the right of the congruence relation.
- 15 gives the remainder of 3 when divided by 12.

In arithmetic modulo 12, it is common to use the numbers from 0 to 11:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Think of it this way: In this arithmetic, there is a finite set of numbers and all we have are these numbers. All other numbers are interesting in their relation to the modulus, what remainder they leave when divided by the modulus. So usually the least residue system modulo m is taken as the set of numbers:

$$\{0, 1, 2, \dots, m-1\}$$

But since the usual clock numbers range from 1 to 12, the set

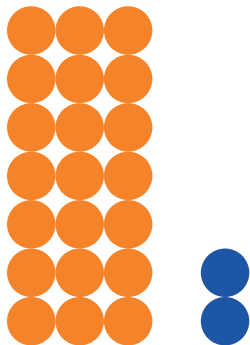
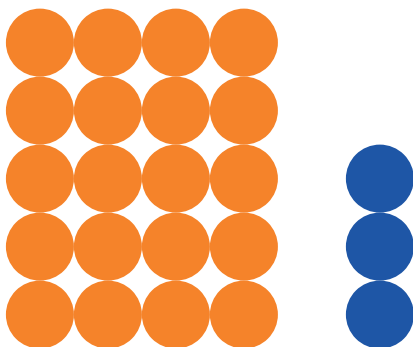
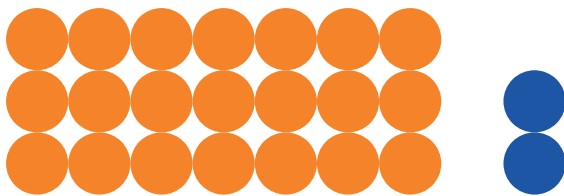
$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

is considered.

Summary

- Number theory has an algebra of its own known as *modular arithmetic*.
- Congruences possess many properties of equations.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$, $a * c \equiv b * d \pmod{m}$ and $a^n \equiv b^n \pmod{m}$.
- In modular arithmetic, numbers “wrap around” when reaching a certain value, which is the modulus.
- Arithmetic modulo 12 is also known as *clock arithmetic*.

9 | Chinese Remainder Theorem



The *Chinese remainder theorem* says you can uniquely solve every pair of congruences having relatively prime moduli.

The earliest known statement of the theorem says:

“There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?”

History

The theorem, as a problem using specific numbers, quoted in the previous section is found in the Chinese mathematician Sun Zi's third-century book *Sunzi Suanjing* (*Master Sun's Mathematical Manual*).

Sun Zi's work, however, does not contain a proof or a full algorithm. *Aryabhata* described an algorithm for solving this problem in the sixth century. *Brahmagupta* (seventh century) knew special cases of the Chinese remainder theorem, and they also appear in *Fibonacci's Liber Abaci* (1202). *Qin Jiushao's* 1247 *Shushu Jiuzhang* (*Mathematical Treatise in Nine Sections*) offered a complete solution called Ta-yan-shu, generalizing the result. British missionary *Alexander Wylie* translated it into English in the early 1800s.



Carl Friedrich Gauss

In his *Disquisitiones Arithmeticae* (1801), *Carl Friedrich Gauss* introduced the notion of congruence. Gauss demonstrates the Chinese remainder theorem on a problem involving calendars “to find the years that have a certain period number with respect to the solar and lunar cycle and the Roman indiction” and introduces a procedure for solving the problem that had already been used by Euler but was actually an ancient method that had shown up multiple times.

The Chinese remainder theorem is one of the few theorems named for an Asian person or place because of the closed development of mathematics in the Western world.

Chinese Remainder Theorem

The *Chinese remainder theorem* says you can uniquely solve every pair of congruences having relatively prime moduli.

Formally stated, the Chinese remainder theorem says that the system of congruences

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv b_k \pmod{m_k}$$

has a unique solution modulo $m = m_1 * m_2 * \dots * m_k$ if $m_1, m_2, \dots, m_k$ are pairwise relatively prime integers.

The unique solution modulo m means that there is a solution x with $0 < x < m$, and all other solutions are congruent modulo m to this solution.

Examples

Let's return to the earliest statement of the theorem.

Basically, it asks for the solution to the following system of linear congruences:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

The theorem says it has a unique solution modulo 105, which is $3 * 5 * 7$. That means there is a solution x with $0 < x < 105$, and all other solutions are congruent modulo 105 to this solution.

You can easily check that 23 is a solution:

$$23 \equiv 2 \pmod{3}$$

$$23 \equiv 3 \pmod{5}$$

$$23 \equiv 2 \pmod{7}$$

All the other solutions are congruent to 23 modulo 105. Therefore, we can express all the other solutions as $23 + 105k$, where k is an integer.

Applications

The Chinese remainder theorem has many uses, particularly in advanced computing algorithms.

It enables replacing a computation by several similar computations on small integers.

Its applications include:

› Cryptography and encryption

The widely used RSA public-key cryptosystem uses the Chinese remainder theorem for secure data transmission. The optimization for decryption is based on the

theorem. In particular, it produces and stores values as part of a private key. The theorem also ensures that the secret can't be recovered from an insufficient number of shares in secret sharing schemes.

› Fourier transforms

The Fourier transform is a well-known function used in many areas. It takes a signal, which is a function of time, and breaks it down into the individual frequencies that compose it. The Chinese remainder theorem helps simplify the computations of the problems that the Fourier transform solves.

› Radar range ambiguity resolution

Medium pulse repetition frequency radar uses techniques for range ambiguity resolution that implement the Chinese remainder theorem. It helps them to get information over significant distances that are even longer than the gap between the transmit pulses.

Summary

- The *Chinese remainder theorem* says you can uniquely solve every pair of congruences having relatively prime moduli.
- The earliest known statement of the theorem is by the Chinese mathematician *Sun Zi* in the *Sunzi Suanjing* (*Master Sun's Mathematical Manual*) in the third century AD.
- The Chinese remainder theorem has many uses, particularly in advanced computing algorithms.

Part 3 Exercises

3.1 If 17 781 234 coins are distributed equally among 17 people, how many coins remain?

Solution

The solution is essentially asking for the remainder of the division of 17 781 234 by 17.

You can calculate this by using the function Mod in Wolfram Language:

```
In[ ]:= Mod [ 17 781 234, 17 ]
```

```
Out[ ]= 16
```

So 16 coins remain after distributing our coins equally among 17 people.

3.2 Using the properties of congruences, compute the remainder when 23^{129} is divided by 3.

Solution

It's not an easy task to do at first sight. 23^{129} has 176 digits:

```
In[ ]:= IntegerDigits [ 23^129 ] // Length
```

```
Out[ ]= 176
```

Instead, you can use modular arithmetic. You have the following congruency relation:

$$23 \equiv -1 \pmod{3}.$$

The exponentiation property says that $23^{129} \equiv (-1)^{129} \pmod{3}$. Since 129 is odd, then $(-1)^{129} = -1$. So

$$23^{129} \equiv -1 \pmod{3}$$

Now since $-1 \equiv 2 \pmod{3}$, you can rewrite the congruency relation as

$$23^{129} \equiv 2 \pmod{3}$$

That means 23^{129} has remainder 2 when divided by 3. You can check it using Wolfram Language:

```
In[ ]:= Mod [ 23^129, 3 ]
```

```
Out[ ]= 2
```

3.3 A group of fishermen find some fish. If they distribute the fish equally among 4 of them, 3 fish remain. If they distribute the fish equally among 5 of them, 4 fish remain. What is the least number of fish they could have found?

Solution

You can use the Chinese remainder theorem to solve this problem.

Basically, the goal is to find the solution to the following system of linear congruences:

$$x \equiv 3 \pmod{4}$$

$$x \equiv 4 \pmod{5}$$

It has a unique solution modulo 20 since 4 and 5 are relatively prime. You can check it using the function `CoprimeQ` in Wolfram Language:

```
In[ ]:= CoprimeQ [ 4, 5 ]
```

```
Out[ ]:= True
```

Now, just use the function `ChineseRemainder` in Wolfram Language:

```
In[ ]:= ChineseRemainder [ { 3, 4 }, { 4, 5 } ]
```

```
Out[ ]:= 19
```

So the least number of fish they could have found is 19.

- 3.4** There is a classical result in number theory, which follows as: Let p be a prime number and k an integer such that $0 < k < p$. Then, $(k-1)! * (p-k)!$ is congruent to $(-1)^k$ modulo p . Verify this result for any three primes of your choice. Be sure to use suitable, small numbers to prevent large computations and overloading of the kernel.

The *factorial* of a non-negative integer n , denoted by $n!$, is the product of all positive integers less than or equal to n .

Solution

Let $p = 7$. Choose $k = 6$:

```
In[ ]:= p = 7;
        k = 6;
```

```
In[ ]:= Mod [ Factorial [ k - 1 ] * Factorial [ p - k ], p ]
```

```
Out[ ]:= 1
```

```
In[ ]:= Mod [ ( -1 ) ^ k, p ]
```

```
Out[ ]:= 1
```

Let $p = 11$. Choose $k = 4$:

```
In[ ]:= p = 11;
        k = 4;
```

```
In[ ]:= Mod [ Factorial [ k - 1 ] * Factorial [ p - k ], p ]
```

```
Out[ ]:= 1
```

```
In[ ]:= Mod [ ( -1 ) ^ k, p ]
```

```
Out[ ]:= 1
```

Let $p = 13$. Choose $k = 9$:

```
In[*]:= p = 13;
k = 9;

In[*]:= Mod [ Factorial [ k - 1 ] * Factorial [ p - k ] , p ]

Out[*]= 12

In[*]:= Mod [ ( - 1 ) ^ k , p ]

Out[*]= 12
```

3.5 A prime number is called a Wilson prime if $(p - 1)!$ is congruent to -1 modulo p^2 . Find all the Wilson primes up to 100.

Solution

You can use a standard loop Do in Wolfram Language with the following conditions:

- 1) p is prime.
- 2) $(p - 1)!$ is congruent to -1 modulo p^2 .

```
In[*]:= Do [
  If [ PrimeQ [ p ] && ( Mod [ Factorial [ p - 1 ] , p^2 ] == Mod [ - 1 , p^2 ] ) , Print [ p ] ,
  { p , 1 , 100 }
]

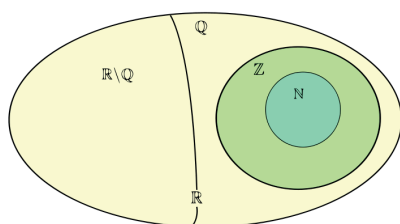
Out[*]= 5

Out[*]= 13
```

So the Wilson primes up to 100 are 5 and 13.

Continued Fractions

10 | Real Number Representations



Look up the “most important numbers in mathematics” or “most famous numbers in the world” on the web, and you’ll look at lists of all kinds of different numbers.

We guarantee that the following numbers will be on most of the lists:

› $\pi = 3.1415 \dots$ (the ratio of the circumference of a circle to the diameter and so much more)

The constant π is fundamental to any equation describing circular or harmonic motion. It is a fundamental relationship in mathematics.

› $e = 2.7182 \dots$ (Euler’s number, also known as the exponential growth constant)

Euler’s number is critical in finance for calculating compound interest, a fundamental concept in understanding the time value of money.

› $\phi = 1.6180 \dots$ (the golden ratio)

In technical analysis, the golden ratio helps some financial analysts predict whether a market will continue its path or reverse. It’s also commonly seen in nature; for instance, naturally occurring spirals that expand outward in a geometric pattern can be found in seashells, pinecones and sunflower seeds.

These numbers are not integers. In fact, integers are rather a small group of numbers on the number line.

There are other numbers as well: rational and irrational numbers. Their union is *real numbers*.

In this lesson, we will primarily discuss how to represent rational numbers and touch on the topic of irrational numbers. The representation of integers is trivial.

Numbers on the Number Line

An *integer* is a number that can be written without a fractional component. The set of integers is denoted by $\mathbb{Z}$:

$$1, -3, 5, 19, \dots$$

Positive integers are called *natural numbers* and are denoted by $\mathbb{N}$:

$$2, 7, 10, 158, \dots$$

So integers include natural numbers:

$$\mathbb{N} \subset \mathbb{Z}$$

A *rational number* is a number that can be expressed in the form a/b , where a and b are integers and b is not zero. The set of rational numbers is represented by the symbol $\mathbb{Q}$:

$$\frac{1}{2}, \frac{3}{10}, \frac{20}{3}, \frac{5}{1}, \dots$$

So integers are included in rational numbers:

$$\mathbb{Z} \subset \mathbb{Q}$$

Rational numbers are included in *real numbers*. The latter are denoted by $\mathbb{R}$:

$$\mathbb{Q} \subset \mathbb{R}$$

All the numbers on the number line are real numbers.

Real numbers that are not rational are called *irrational numbers*:

$$\sqrt{2}, \pi, \sqrt{10}, \dots$$

Decimal Numeral System

First, all the numbers you will examine are in decimal numeral system.

The *decimal numeral system* is the standard system for representing integers and nonintegers.

The way of denoting numbers in the decimal system is frequently called *decimal notation*.

A *decimal number*, or just a *decimal*, refers to the notation of a number in the decimal numeral system.

For example, all of the following integer and noninteger numbers are decimal numbers:

$$14, 0.75, -9$$

For writing integers, the decimal system uses:

- › Ten digits: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
- › The minus sign “-” for negative integers

For writing noninteger numbers, it uses:

- › A decimal separator “.”

Decimals

The *integer part* of a decimal is the integer written to the left of the decimal separator. The part from the decimal separator to the right is the *fractional part*.

For example, the integer part of the decimal 18.75 is 18, and the fractional part is .75 or 0.75.

The fractional part equals the difference between the decimal and its integer part:

$$18.75 - 18 = 0.75$$

You can have one or more 0s on the left. This does not change the decimal’s value. For example,

$$4.15 = 04.15 = 004.15$$

In the same way, adding trailing zeros doesn’t change the represented number. For example,

$$19 = 19.0 = 19.00$$

$$7.8 = 7.80 = 7.800$$

The integral part of a numeral may be left out if it is zero. Like in the previous example, instead of 0.75, you can write .75.

Decimals as the Sum of Digits

Any number in the decimal numeral system can be decomposed as the sum of its digits multiplied by the power of 10 depending on their position.

For example, the number 48 967 is represented as

$$48\,967 = 7 * 10^0 + 6 * 10^1 + 9 * 10^2 + 8 * 10^3 + 4 * 10^4$$

The rule is quite the same with nonintegers in a way that the contribution of each digit to the value of a number depends on its position in the numeral.

For example, the decimal 14.254 is represented as

$$14.254 = 1 * 10^1 + 4 * 10^0 + 2 * 10^{-1} + 5 * 10^{-2} + 4 * 10^{-3}$$

You see, the digits after the decimal point are multiplied with the negative powers of 10.

A couple more examples are

$$23.8 = 2 * 10^1 + 3 * 10^0 + 8 * 10^{-1}$$

$$0.75 = 0 * 10^0 + 7 * 10^{-1} + 5 * 10^{-2} = 7 * 10^{-1} + 5 * 10^{-2}$$

Types of Decimals

There are two types of decimals, *terminating* and *non-terminating*.

Terminating decimal numbers have a finite number of digits after the decimal point.

These types of decimal numbers are also known as *exact decimal numbers*. Examples are

1.89

15.7

Terminating decimal numbers represent rational numbers.

The digits after the decimal point of *non-terminating* decimals repeat endlessly, so these decimal numbers have an infinite number of digits after the decimal point.

These decimal numbers are further divided into *recurring* and *non-recurring* decimal numbers.

Recurring decimal numbers have an infinite number of digits after the decimal point.

These digits, however, repeat regularly:

2.3333333 ...

14.15151515 ...

By putting a bar sign over the repeating digits, you can indicate that they go on to infinity:

2. $\overline{3}$

14. $\overline{15}$

Non-recurring decimal numbers have not only an infinite number of digits at their decimal places, but their decimal place digits do not follow a specific order. For example,

41.487414585 ...

78.586248 ...

You can't put a bar sign over the decimal numbers as the digits don't follow any order.

Recurring decimal numbers represent rational numbers, whereas non-recurring numbers represent irrational numbers.

Fractions

A *fraction* represents a part of a whole, or any number of equal parts.

For example,

$$\frac{5}{4}, \frac{1}{2}, \frac{11}{145}$$

are all fractions.

A common fraction consists of a *numerator* displayed above a line and a nonzero *denominator* displayed below that line. So for the fraction

$$\frac{3}{4}$$

3 is the numerator and 4 is the denominator.

The numerator represents the number of equal parts, and the denominator indicates how many of those parts make up a unit or a whole.

In the previous example, the numerator, 3, tells you that the fraction represents 3 equal parts, and the denominator, 4, tells you that 4 parts make up a whole:



You already know the definition of rational numbers. So, you can conclude that fractions actually represent rational numbers.

Types of Fractions

A *simple fraction* is a rational number written as $\frac{a}{b}$, where a and b are both integers.

The denominator b cannot be zero. For example,

$$\frac{8}{7}, \frac{3}{14}, \frac{9}{1}$$

A *unit fraction* is a common fraction with a numerator of 1. For example,

$$\frac{1}{3}, \frac{1}{4}, \frac{1}{250}$$

Common fractions can be classified as either *proper* or *improper*.

When the numerator and the denominator are both positive, the fraction is called *proper* if the numerator is less than the denominator:

$$\frac{15}{64}, \frac{2}{5}$$

Otherwise, the fraction is called *improper*:

$$\frac{100}{7}, \frac{56}{12}$$

Reciprocal of a Fraction

The *reciprocal* of a fraction is another fraction with the numerator and denominator exchanged. The reciprocal of $\frac{4}{5}$ is $\frac{5}{4}$.

The product of a fraction and its reciprocal is 1.

It's very easy to see that the reciprocal of a proper fraction is improper, and the reciprocal of an improper fraction not equal to 1 is a proper fraction.

When the numerator and denominator of a fraction are equal, its value is 1, and the fraction therefore is improper. Its reciprocal also has the value 1, and is improper, too:

$$\frac{2}{2} = \frac{3}{3} = \frac{10}{10} = 1$$

Any integer can be written as a fraction with the number 1 as the denominator. For example,

$$20 = \frac{20}{1}$$

1 is sometimes referred to as the invisible denominator.

Decimal Fractions

It's easy to see that the decimal 0.8 is the fraction

$$\frac{8}{10}$$

as 0.8 represents the number

$$0.8 = 0 + 8 * 10^{-1} = \frac{8}{10}$$

0.8 is a fraction too, as it is a part of a whole. It is called a *decimal fraction*.

It's understood that the denominator for a decimal fraction is an integer power of 10, even if it's not given explicitly. Decimal fractions are expressed using decimal notation in which the implied denominator is determined by the number of digits to the right of a decimal separator.

So, for 1.25, the numerator is 125 and the implied denominator is 10 to the power of 2, as there are two digits to the right of the decimal point:

$$1.25 = \frac{125}{100}$$

A few more examples are

$$0.2 = \frac{2}{10}$$

$$1.4 = \frac{14}{10}$$

$$0.75 = \frac{75}{100}$$

$$1.2589 = \frac{12\,589}{10\,000}$$

Decimals and Fractions

Converting terminating decimals to simple fractions has already been discussed, but there are other types of decimals as well, so let's generalize that.

Every simple fraction represents a rational number and thus it corresponds to a certain terminating or recurring decimal number:

$$\frac{256}{10} = 25.6$$

$$\frac{1}{3} = 0.\overline{3}$$

In the same way, every terminating and recurring decimal number represents a rational number too and corresponds to a certain simple fraction:

$$128.4 = \frac{1284}{10}$$

$$0.\overline{62} = \frac{62}{99}$$

There are quite easy algorithms for every one of these cases, but this book will not cover them.

Summary

- The *integer part* of a decimal is the integer written to the left of the decimal separator. The part from the decimal separator to the right is the *fractional part*.
- There are two types of decimals: *terminating* and *non-terminating*.
- *Non-terminating* decimal numbers are further divided into *recurring* and *non-recurring*.

- *Terminating* decimal numbers represent rational numbers.
- *Recurring* decimal numbers represent rational numbers, whereas *non-recurring* numbers represent irrational numbers.
- A *fraction* represents a part of a whole, or any number of equal parts.
- A common fraction consists of a *numerator* displayed above a line, and a nonzero *denominator* displayed below that line.
- A *simple fraction* is a rational number written as $\frac{a}{b}$, where a and b are both integers and b is not zero.

11 | Continued Fractions



A *continued fraction* is an expression obtained through iteratively representing a number as the sum of its integer part and the reciprocal of another number, then writing this other number as the sum of its integer part and another reciprocal and so on.

Continued fractions, a very natural object, appear unexpectedly in many mathematical areas.



Christian Huygens

The Dutch mathematician and astronomer *Christian Huygens* wrote a paper explaining how to use convergents to find the best rational approximations for gear ratios. He was able to select the best gears based on these approximate values.

Continued fractions can also approximate irrational numbers, for example, $\sqrt{2}$.

Continued fractions further captivated the attention of most prominent mathematicians. Many mathematicians, including Euler, Jacobi, Cauchy and Gauss, explored this subject. Continued fractions are applied in certain areas of modern mathematics as well.

In certain aspects, continued fractions are a more natural mathematical representation of real numbers than, say, decimals, and they offer several useful properties.

Logic behind Continued Fractions

Consider, for example, the fraction $\frac{238}{37}$. It's a rational number and the goal is to approximate it as well as possible:

$$\frac{238}{37} \approx 6.43243$$

The first approximation will be 6, but it's very rough. So you go on. Notice that

$$\frac{238}{37} = 6 + \frac{16}{37}$$

As a second approximation, you would want to represent $\frac{238}{37}$ as $6 + \frac{1}{x}$, where x is yet unknown. So consider the reciprocal of $\frac{16}{37}$, which will be $\frac{37}{16}$, and represent it as

$$\frac{37}{16} = 2 + \frac{5}{16}$$

As a result, the first approximation for $\frac{37}{16}$ will be 2, and the second approximation for $\frac{238}{37}$ will be

$$\frac{238}{37} = 6 + \frac{1}{2}$$

The goal now is to represent $\frac{238}{37}$ as $6 + \frac{1}{2 + \frac{1}{x}}$, which is the same as to represent $\frac{37}{16}$ as $2 + \frac{1}{x}$. That means you should do the same steps with $\frac{5}{16}$ as you did with $\frac{238}{37}$:

$$\frac{16}{5} = 3 + \frac{1}{5}$$

And the third approximation will be

$$\frac{238}{37} = 6 + \frac{1}{2 + \frac{1}{3}}$$

Finally, what remains is $\frac{1}{5}$, which has a reciprocal of 5 and $5 = 5 + 0$, so

$$\frac{238}{37} = 6 + \frac{1}{2 + \frac{1}{3 + \frac{1}{5}}}$$

which is precise, as there is no other place to go.

So you're left with the following representation for the fraction $\frac{238}{37}$:

$$\frac{238}{37} = 6 + \frac{1}{2 + \frac{1}{3 + \frac{1}{5}}}$$

The approximations are

$$6, \quad 6 + \frac{1}{2} = 6.5, \quad 6 + \frac{1}{2 + \frac{1}{3}} \approx 6.4285, \quad 6 + \frac{1}{2 + \frac{1}{3 + \frac{1}{5}}} \approx 6.4324$$

Definition

A *continued fraction* is an expression of the form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

In this book, it is assumed that all a_i are integers. Such continued fractions are called *simple continued fractions*. The expression can contain a finite or infinite number of terms.

The previous continued fraction is denoted by

$$[a_0; a_1, a_2, \dots]$$

Examples

$$[1; 2, 3] = 1 + \frac{1}{2 + \frac{1}{3}} = \frac{10}{7} = 1.42 \dots$$

$$[1; 3, 2, 4] = 1 + \frac{1}{3 + \frac{1}{2 + \frac{1}{4}}} = \frac{40}{31} = 1.29 \dots$$

The first integer may be negative:

$$[-3; 6, 1, 4] = -3 + \frac{1}{6 + \frac{1}{1 + \frac{1}{4}}} = -\frac{97}{34} = -2.85 \dots$$

The first integer may be zero:

$$[0; 7, 2, 5] = 0 + \frac{1}{7 + \frac{1}{2 + \frac{1}{5}}} = \frac{11}{82} = 0.13 \dots$$

The integers $a_0, a_1, a_2, \dots$ are called the *coefficients*, or *terms*, of the continued fraction.

Finite Continued Fractions

A *finite continued fraction* is a continued fraction with a finite number of terms:

$$a_0 + \frac{1}{a_1 + \frac{1}{\dots + \frac{1}{a_n}}}$$

It is denoted by $[a_0; a_1, a_2, \dots, a_n]$.

Here are some examples:

$$[0; 1, 4, 1, 3] = \frac{19}{23}$$

$$[4; 6] = \frac{25}{6}$$

Every finite continued fraction represents a rational number:

$$[3; 4, 8] = 3 + \frac{1}{4 + \frac{1}{8}} = \frac{107}{33}$$

And every rational number can be represented by a finite continued fraction in exactly two ways:

$$\begin{aligned} \frac{10}{27} &= [0; 2, 1, 2, 3] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}}} \\ \frac{10}{27} &= [0; 2, 1, 2, 2, 1] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1}}}}} \end{aligned}$$

Only the last term of the representations differ. The last term in the continued fraction is 1 in the longer representation, whereas the shorter one drops the last 1 and adds 1 to the new last term.

Consider the continued fraction representation of $\frac{9}{4}$:

$$\frac{9}{4} = [2; 4] = 2 + \frac{1}{4}$$

Now represent its reciprocal, which is $\frac{4}{9}$, as a continued fraction:

$$\frac{4}{9} = [0; 2, 4] = 0 + \frac{1}{2 + \frac{1}{4}}$$

They are the same except for a one-position shift left or right depending on whether the number is less than or greater than 1, respectively.

The Sequence of Convergents

Consider a continued fraction representation of $\frac{272}{105}$:

$$\frac{272}{105} = [2; 1, 1, 2, 3, 1, 4] = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}}}} = 2.590476190 \dots$$

Keep only a limited number of terms. Start with one term and add one each time:

$$[2;] = 2$$

$$[2; 1] = 3$$

$$[2; 1, 1] = \frac{5}{2}$$

$$[2; 1, 1, 2] = \frac{13}{5}$$

$$[2; 1, 1, 2, 3] = \frac{44}{17}$$

$$[2; 1, 1, 2, 3, 1] = \frac{57}{22}$$

$$[2; 1, 1, 2, 3, 1, 4] = \frac{272}{105}$$

You get a sequence of rational numbers:

$$2, 3, \frac{5}{2}, \frac{13}{5}, \frac{44}{17}, \frac{57}{22}, \frac{272}{105}$$

They are actually approximations of $\frac{272}{105}$. It will become clear if you approximate those numbers using decimals:

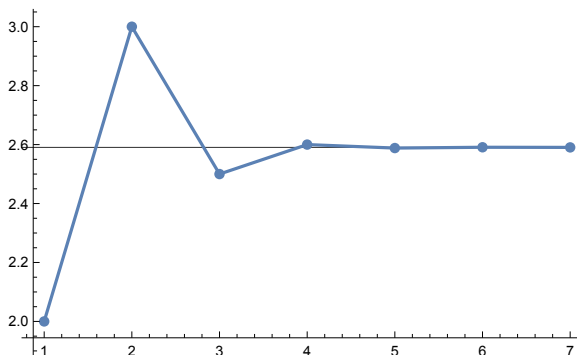
$$2, 3, 2.5, 2.6, 2.588, 2.5909, 2.59047$$

The first thing to notice is that by taking more terms, they get closer to the exact value of the continued fraction.

Then you can notice that the odd-numbered numbers are smaller than the value of the continued fraction and their sequence is increasing. While the even-numbered numbers are greater than the value of the continued fraction and their sequence is decreasing.

These numbers are called *convergents*.

You can see that they tend to the number (the gray line is $\frac{272}{105}$ and the blue markers are its convergents):



Infinite Continued Fractions

An *infinite continued fraction* is a continued fraction with an infinite number of terms:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

It is denoted by $[a_0; a_1, a_2, \dots]$.

Here are some examples:

$$[3; 7, 15, 1, \dots] = \pi$$

$$[1; 2, 2, 2, \dots] = \sqrt{2}$$

Consider the number $\frac{1+\sqrt{5}}{2} = 1.61803 \dots$ and represent it as a continued fraction.

Remember the steps done previously:

$$\frac{1 + \sqrt{5}}{2} = 1 + \frac{-1 + \sqrt{5}}{2}$$

The reciprocal of $\frac{-1+\sqrt{5}}{2}$ is again $\frac{1+\sqrt{5}}{2}$, as

$$\frac{2}{-1 + \sqrt{5}} = \frac{2(-1 - \sqrt{5})}{(-1 + \sqrt{5})(-1 - \sqrt{5})} = \frac{1 + \sqrt{5}}{2}$$

That means that you will get the continued fraction

$$1 + \frac{1}{1 + \frac{1}{1 + \dots}}$$

So you'll get the continued fraction $[1; 1, 1, \dots]$. This is actually the continued fraction of the *golden ratio*.

Every infinite continued fraction is irrational, and every irrational number can be uniquely represented as an infinite continued fraction. For example,

$$[4; 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, \dots] = \sqrt{19}$$

$$\frac{1 + 5\sqrt{3}}{4} = [2; 2, 2, 2, 3, 1, 10, 1, 3, 2, \dots]$$

Only real quadratic irrationals have periodic continued fraction forms:

$$\sqrt{5} = [2; 4, 4, 4, \dots]$$

$$\sqrt{27} = [5; 5, 10, 5, 10, \dots]$$

Khinchin's Constant

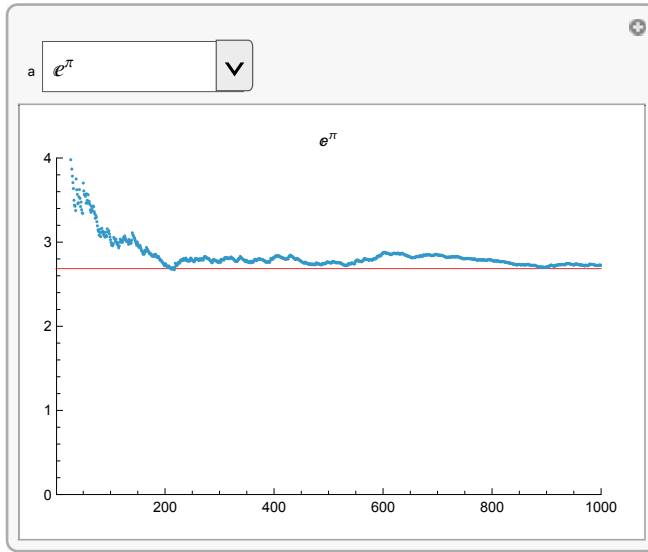
There is a peculiar property that is common with all real numbers, independent of the number.

Aleksandr Khinchin proved that for almost all real numbers x , terms a_i of the continued fraction expansion of x have a finite geometric mean that is independent of the value of x and is known as *Khinchin's constant*.

That means, it is almost always true that

$$\lim_{n \rightarrow \infty} (a_0 a_1 \dots a_n)^{\frac{1}{n}} = K_0 \approx 2.6854520010 \dots$$

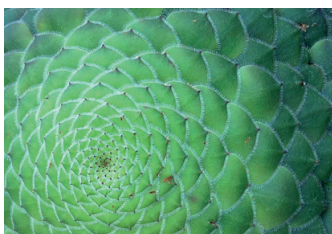
In the following plot, Khinchin's constant is the red line, and you can see that $(a_0 a_1 \dots a_n)^{\frac{1}{n}}$ for almost all the numbers tends to the red line:



Summary

- A *continued fraction* is an expression of the form $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$.
- The integers a_i are called the *terms*, or *coefficients*.
- A *finite continued fraction* is a continued fraction with a finite number of terms.
- An *infinite continued fraction* is a continued fraction with an infinite number of terms.
- For almost all real numbers x , terms a_i of the continued fraction expansion of x have a finite geometric mean that is independent of the value of x and is known as *Khinchin's constant*.

12 | Best Rational Approximations



$\frac{22}{7} = 3.142857143 \dots$ is a well-known rational approximation to π . The error in the approximation is 0.00126.

Another rational approximation to π is $\frac{355}{113} = 3.141592920 \dots$. Now the error is 0.000000266.

Now take $\sqrt{2}$. The best rational approximation to $\sqrt{2}$ is $\frac{7}{5} = 1.4$. The error in the approximation is 0.0142.

The best rational approximation to $\sqrt{2}$ with a denominator less than 200 is $\frac{239}{169} = 1.414201183 \dots$. The error now is 0.0000124.

This is far less satisfying than the rational approximations of π . This has led mathematicians to classify irrational numbers by how well they can be approximated by rational numbers.

It is in this sense that one irrational is more irrational than another.

In this lesson, we will explore *rational approximation* and the concept of why some numbers are better approximated by rationals than others.

Rational Approximations to π

Look at the sequence of rational approximations to the irrational number $\pi = 3.14159 \dots$:

$$r_0 = 3$$

$$r_1 = 3.1 = \frac{31}{10}$$

$$r_2 = 3.14 = \frac{314}{100}$$

$$r_3 = 3.141 = \frac{3141}{1000}$$

...

The rational numbers r_k are the approximations to π . As you can see, they get closer and closer to π .

You can measure the quality of these approximations by observing that

$$\pi - r_k < \frac{1}{10^k}$$

The error is less than 1 over the denominator of the fraction.

Rational Approximations to $\sqrt{2}$

Now look at the sequence of rational approximations to the irrational number $\sqrt{2} = 1.41421 \dots$:

$$r_0 = 1$$

$$r_1 = 1.4 = \frac{14}{10}$$

$$r_2 = 1.41 = \frac{141}{100}$$

$$r_3 = 1.414 = \frac{1414}{1000}$$

...

Similarly, the rational numbers r_k are the approximations to $\sqrt{2}$. Again, they get closer and closer to $\sqrt{2}$.

The accuracy is the same as the approximations to π :

$$\sqrt{2} - r_k < \frac{1}{10^k}$$

The error is less than 1 over the denominator of the fraction.

Better Rational Approximations to π

So far, the denominators of the approximations have been powers of 10.

Suppose the denominators of the approximations can be other integers as well.

For example,

$$\frac{22}{7} = 3.142857143 \dots$$

is a well-known rational approximation to π .

The error in the approximation is 0.00126.

Another rational approximation to π is

$$\frac{355}{113} = 3.141592920 \dots$$

Now the error is 0.000000266.

Better Rational Approximations to $\sqrt{2}$

Now take $\sqrt{2}$.

The best rational approximation to $\sqrt{2}$ with a denominator less than 10 is

$$\frac{7}{5} = 1.4$$

The error in the approximation is 0.0142.

The best rational approximation to $\sqrt{2}$ with a denominator less than 200 is

$$\frac{239}{169} = 1.414201183 \dots$$

The error now is 0.0000124.

Logic behind the Best Rational Approximations

The *best rational approximations* come from continued fraction expansions of a number.

As you already know, a *continued fraction* is an expression of the form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

An infinite continued fraction is a continued fraction with an infinite number of terms.

Every irrational number can be represented in one way as an infinite continued fraction.

The numbers $c_1, c_2, \dots$ are called *convergents*:

$$c_1 = a_1$$

$$c_2 = a_1 + \frac{1}{a_2}$$

$$c_3 = a_1 + \frac{1}{a_2 + \frac{1}{a_3}}$$

...

The convergents of a number tend to it.

The best rational approximations to an irrational number always lie among its convergents.

The Most Irrational Number

What do you think is the most irrational number, the one for which rational approximations perform the worst?

The most irrational number is, in fact, a widely recognized number.

It is the *golden ratio*.

The *golden ratio*, also known as the divine proportion, golden mean or golden section, is the irrational number:

$$\frac{\sqrt{5} + 1}{2} = 1.618033989 \dots$$

It is often denoted by ϕ .

The continued fraction expansion of the golden ratio is the simplest of all:

$$\phi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\dots}}}$$

The golden ratio appears in an array of mathematical contexts. You can find it when calculating the ratios of distances in basic geometric shapes, like pentagons.

The golden ratio also occurs in nature. For example, it is often used for the arrangement of leaves or flowers.

You can see the first 10 convergents of the golden ratio and their numerical values in the following table:

c_1	1	1.000000000
c_2	2	2.000000000
c_3	$\frac{3}{2}$	1.500000000
c_4	$\frac{5}{3}$	1.666666667
c_5	$\frac{8}{5}$	1.600000000
c_6	$\frac{13}{8}$	1.625000000
c_7	$\frac{21}{13}$	1.615384615
c_8	$\frac{34}{21}$	1.619047619
c_9	$\frac{55}{34}$	1.617647059
c_{10}	$\frac{89}{55}$	1.618181818

Fibonacci Numbers

The convergents of the golden ratio are connected to Fibonacci numbers.

The *Fibonacci sequence* is a sequence in which each number is the sum of the two preceding ones.

The numbers in the Fibonacci sequence are called *Fibonacci numbers*.

The n^{th} Fibonacci number is denoted by F_n .

Here are the first few Fibonacci numbers:

F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	...
1	1	2	3	5	8	13	21	34	55	89	144	233	377	...

The convergents of the golden ratio are the ratios of consecutive Fibonacci numbers:

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	...
1	2	$\frac{3}{2}$	$\frac{5}{3}$	$\frac{8}{5}$	$\frac{13}{8}$	$\frac{21}{13}$	$\frac{34}{21}$	$\frac{55}{34}$	$\frac{89}{55}$	$\frac{144}{89}$	$\frac{233}{144}$	$\frac{377}{233}$	...

Summary

- There is a classification among irrational numbers based on how well they can be approximated by rational numbers.
- Some irrational numbers are more irrational than others.
- The *best rational approximations*, as well as most of the theory of rational approximation, come from continued fraction expansions.
- The best rational approximations to an irrational number are always found among its *convergents*.
- The most irrational number is the *golden ratio*.
- The *Fibonacci sequence* is a sequence in which each number is the sum of the two preceding ones.
- The numbers in the Fibonacci sequence are called *Fibonacci numbers*.
- The convergents of the golden ratio are the ratios of consecutive Fibonacci numbers.

Part 4 Exercises

- 4.1** There's a set of numbers $\{-\frac{1}{3}, -7, \pi, e^\pi, 0, \sqrt{2}, 12, -45, \sqrt{17}, \frac{34}{3}, 87, -70, \frac{4}{5}, 123\}$. Divide that set of numbers into rational and irrational numbers. Then select integers from the rational numbers. Finally, from the set of integers, select natural numbers.

Solution

You are given a set of numbers:

$$\text{In[]:= numbers} = \left\{-\frac{1}{3}, -7, \pi, e^\pi, 0, \sqrt{2}, 12, -45, \sqrt{17}, \frac{34}{3}, 87, -70, \frac{4}{5}, 123\right\};$$

Use the function `Element` and the domain `Rationals` in Wolfram Language to select rational numbers from the list:

$$\text{In[]:= rationals} = \text{Select}[\text{numbers}, \text{Element}[\#, \text{Rationals}] \&]$$

$$\text{Out[]:=} \left\{-\frac{1}{3}, -7, 0, 12, -45, \frac{34}{3}, 87, -70, \frac{4}{5}, 123\right\}$$

The rest of the functions are apparently irrational numbers:

$$\text{In[]:= irrationals} = \text{Complement}[\text{numbers}, \text{rationals}]$$

$$\text{Out[]:=} \left\{\sqrt{2}, \sqrt{17}, e^\pi, \pi\right\}$$

From the rational numbers, select integers by using the domain `Integers` in Wolfram Language:

$$\text{In[]:= integers} = \text{Select}[\text{rationals}, \text{Element}[\#, \text{Integers}] \&]$$

$$\text{Out[]:=} \{-7, 0, 12, -45, 87, -70, 123\}$$

From the integers, select the natural numbers:

$$\text{In[]:= naturals} = \text{Select}[\text{integers}, \# > 0 \&]$$

$$\text{Out[]:=} \{12, 87, 123\}$$

- 4.2** Find the value of the digit x so that the four-digit number $137x$ is divisible by 9.

Solution

The number $137x$ is represented as

$$137x = x \cdot 10^0 + 7 \cdot 10^1 + 3 \cdot 10^2 + 1 \cdot 10^3 = x + 7 \cdot 10 + 3 \cdot 100 + 1 \cdot 1000$$

You can rewrite it as

$$137x = x + 7 \cdot (9 + 1) + 3 \cdot (99 + 1) + 1 \cdot (999 + 1) = (7 \cdot 9 + 3 \cdot 99 + 1 \cdot 999) + (x + 7 + 3 + 1)$$

The first sum ($7 \cdot 9 + 3 \cdot 99 + 1 \cdot 999$) is divisible by 9. If the second sum ($x + 7 + 3 + 1$) is divisible by 9, then $137x$ is divisible by 9.

Now the goal is to find x such that $11 + x$ is divisible by 9. Note that x is a digit and can only be 0, 1, 2, 3, 4, 5, 6, 7, 8 or 9. It's easy to see that $x = 7$:

In[]:= **Divisible [11 + 7, 9]**

Out[]:= True

So the number is 1377. Check:

In[]:= **Divisible [1377, 9]**

Out[]:= True

This is actually the divisibility rule for 9, which states if the sum of the digits are divisible by 9, then the number is divisible by 9.

4.3 Find the convergents for $\sqrt{19}$. To get a feel for how closely the convergents approximate the number, find and plot the difference between $\sqrt{19}$ and the value of each convergent.

Solution

You can find the first 10 convergents of $\sqrt{19}$ using the function `Convergents` in Wolfram Language:

In[]:= **convergents = Convergents [$\sqrt{19}$, 10]**

Out[]:= $\left\{ 4, \frac{9}{2}, \frac{13}{3}, \frac{48}{11}, \frac{61}{14}, \frac{170}{39}, \frac{1421}{326}, \frac{3012}{691}, \frac{4433}{1017}, \frac{16311}{3742} \right\}$

The convergents get closer and closer to the number:

In[]:= **N [$\sqrt{19}$ - convergents]**

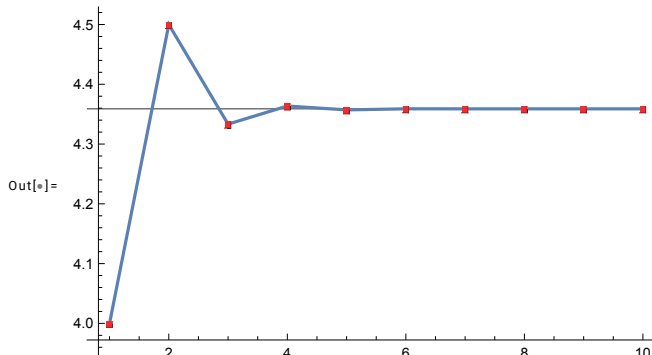
Out[]:= $\{ 0.358899, -0.141101, 0.0255656, -0.00473742, 0.00175609, -0.0000754154, 3.23802 \times 10^{-6}, -1.20118 \times 10^{-6}, 2.2181 \times 10^{-7}, -4.09596 \times 10^{-8} \}$

Plot the difference using `ListLinePlot`:

In[]:= **ListLinePlot [convergents,**

Prolog $\rightarrow$ { Gray, N [Line [{ { 0, $\sqrt{19}$ }, { 10, $\sqrt{19}$ } }] }],

PlotRange $\rightarrow$ All, PlotMarkers $\rightarrow$ { Red, 4 }]



4.4 Calculate the geometric mean of the first 100 terms in the continued fractional representation of π .

For a set of numbers $a_1, a_2, \dots, a_n$ the geometric mean is defined as $(a_1 * a_2 * \dots * a_n)^{\frac{1}{n}}$.

Solution

Use the function `ContinuedFraction` in Wolfram Language to find the first 100 terms in the continued fraction representation of π :

```
In[ ]:= terms = ContinuedFraction [ Pi, 100 ]
```

```
Out[ ]= { 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6,
          99, 1, 2, 2, 6, 3, 5, 1, 1, 6, 8, 1, 7, 1, 2, 3, 7, 1, 2, 1, 1, 12, 1, 1, 1, 3, 1, 1, 8, 1, 1, 2, 1, 6, 1,
          1, 5, 2, 2, 3, 1, 2, 4, 4, 16, 1, 161, 45, 1, 22, 1, 2, 2, 1, 4, 1, 2, 24, 1, 2, 1, 3, 1, 2, 1, 1, 10 }
```

Then the geometric mean would be:

```
In[ ]:= Power [ Apply [ Times, ContinuedFraction [ Pi, 100 ] ], 1 / 100 ] / / N
```

```
Out[ ]= 2.69405
```

Compare it to Khinchin's constant:

```
In[ ]:= Khinchin / / N
```

```
Out[ ]= 2.68545
```

4.5 In Mathematica, if `Rationalize` returns a rational number $\frac{p}{q}$, then $|\frac{p}{q} - x| < \frac{10^{-4}}{q^2}$. You can show this for an arbitrary x between 0 and 1.

Solution

Choose an arbitrary x between 0 and 1:

```
In[ ]:= x = 0.202898;
```

Apply the function `Rationalize` to it:

```
In[ ]:= r = Rationalize [ x ]
```

```
Out[ ]=  $\frac{101449}{500000}$ 
```

Show the inequality. Use the functions `Numerator` and `Denominator` in Wolfram Language:

```
In[ ]:= p = Numerator [ r ];
        q = Denominator [ r ];
```

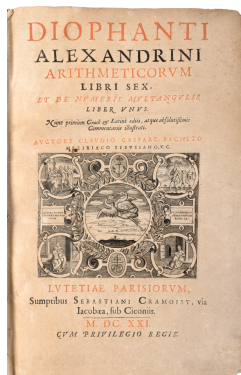
```
In[ ]:=
```

$$\text{Abs} [r - x] < \frac{10^{-4}}{q^2}$$

```
Out[ ]= True
```


Diophantine Equations

13 | Diophantine Equations



Imagine a problem: how many ways are there to make \$2.00 from only nickels and quarters?

In your mind, you must be looking for some sort of equation with the number of nickels and quarter, and all of that would add up to 2.

Imagine you have that equation. For now, it does not matter which equation exactly. The unknowns in that equation would logically be the number of nickels and quarters.

What does the word number say to you? Can 0.5 or $\frac{3}{4}$ be a number? Of course, no.

So, you put a restraint on the unknowns: the unknowns must be natural numbers. Your problem now is to solve that equation in natural numbers.

This is so different from solving equations with no restrictions. As a matter of fact, there's a huge and very important subdivision in number theory dedicated to finding solutions to Diophantine equations.

A *Diophantine equation* is a polynomial equation, usually in two or more unknowns, such that only the integer solutions are sought or studied.

Diophantine problems have fewer equations than unknown variables and involve finding integers that work correctly for all equations.

Historically, individual Diophantine equations have been studied as puzzles, but the development of comprehensive theories to address them is a twentieth-century breakthrough.

History



Diophantus of Alexandria

The word Diophantine refers to the Hellenistic mathematician of the third century, *Diophantus of Alexandria*, who was a Greek mathematician and studied such equations. He pioneered the use of symbolism in algebra.

He was the author of a series of books called *Arithmetica*. It is a collection of 130 algebraic problems giving numerical solutions of equations. Equations in the book are Diophantine equations. Most of the *Arithmetica* problems lead to quadratic equations.



Pierre de Fermat

Reading Diophantus's *Arithmetica*, *Pierre de Fermat* concluded a particular equation considered by Diophantus had no solutions, and added a brief, unexplained note in the margin that he had found “a truly marvelous proof of this proposition,” now known as *Fermat's Last Theorem*. This resulted in significant breakthroughs in the field of Diophantine equations.

Introduction to Diophantine Equations

Think back to the problem that was already posed: how many ways are there to make \$2.00 from only nickels and quarters?

If x is the number of nickels and a nickel is 5 cents, y is the number of quarters and a quarter is 25 cents, and \$2.00 is 200 cents, then a solution to this problem satisfies the equation:

$$5x + 25y = 200$$

Mathematically speaking, the problem is: how many integer solutions does this equation have?

However, this is different from simply solving an equation because:

- › There is one equation and two unknowns.
- › There is more than one solution to account for.
- › The solutions are restricted because they must be non-negative integers.

This is a classic example of a Diophantine equation.

Definition

A *Diophantine equation* is a polynomial equation, usually in two or more unknowns, such that only the integer solutions are studied.

Here are some examples of Diophantine equations:

$$6x + 19y = 1$$

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

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

Here, x , y and z are unknowns. As you can see, in all these cases, we have one equation and yet two or more unknowns.

The typical questions concerning a Diophantine equation are:

- › Are there any solutions?
- › Are there any solutions beyond some that are easily found by inspection?
- › Are there finitely or infinitely many solutions?
- › Can all solutions be found in theory?
- › Can a full list of solutions be computed?

These classic problems remained unsolved for hundreds of years until mathematicians started appreciating their complexity instead of viewing them as mere puzzles.

Example

First, you cannot solve any given Diophantine equation. Moreover, a general algorithm for solving all Diophantine equations cannot exist.

Apart from the simplest cases of Diophantine equations, there isn't a general method for solving them. Outside a certain class of equations, each Diophantine equation is treated individually.

Now let's solve a simple Diophantine equation with no knowledge about such equations:

- › The father's age is 1 less than twice that of his son.
- › The digits AB making up the father's age are reversed in the son's age (BA).

This leads to the equation

$$10A + B = 2(10B + A) - 1$$

Thus,

$$19B - 8A = 1$$

By inspecting, you get to the result $A = 7$ and $B = 3$. Thus the father's age is 73 and the son's age is 37.

Of course, the fact that A and B are positive integers less than 10 helps a great deal. It also helps to show that there is no other solution with such A and B .

There is a general algorithm by which you can solve such equations, but you just solved it without any prior knowledge!

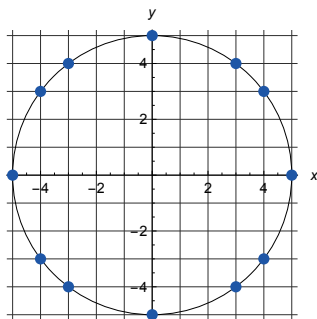
Geometric Interpretation

The most interesting thing about Diophantine equations is that we can describe them geometrically.

Equations with two variables define curves in a plane. The solutions of the equation are the *integral points* on the curve defined by the equation. Integral points are those points that have integer coordinates. They are also called lattice points.

Consider, for example, the Diophantine equation $x^2 + y^2 = 25$. What are its integer solutions? Let's solve it geometrically.

The curve $x^2 + y^2 = 25$ is a circle of radius 5 around the origin. The goal is to know whether there are any integral points on the circle:



There indeed are points with integer coefficients.

Cases $\{5, 0\}$, $\{-5, 0\}$, $\{0, 5\}$ and $\{0, -5\}$ are trivial.

Apart from them, the desired points are $\{3, 4\}$ and $\{4, 3\}$ and their negative versions, as the unknowns in our equation are squared: $\{-3, 4\}$, $\{-4, 3\}$, $\{3, -4\}$, $\{4, -3\}$, $\{-3, -4\}$ and $\{-4, -3\}$.

Therefore, the solutions are $(\pm 5, 0)$, $(\pm 4, \pm 3)$, $(\pm 3, \pm 4)$ and $(0, \pm 5)$.

Summary

- A *Diophantine equation* is a polynomial equation, usually in two or more unknowns, such that only the integer solutions are studied.
- The word Diophantine refers to the Hellenistic mathematician of the third century *Diophantus of Alexandria*, who was a Greek mathematician and studied such equations.
- A general algorithm for solving all Diophantine equations cannot even exist.
- Geometrically, a Diophantine equation with two variables defines a curve in a plane, and the goal is to find the integral points on it.

14 | Linear Diophantine Equations

Diophantine equations are a very broad subject of study. It would be rational to narrow the subject of study by examining the very simple equations first.

The simplest Diophantine equation is the *linear Diophantine equation*.

In abstract, it can have as many unknowns as you want. The book will cover linear Diophantine equations with two unknowns. Linear Diophantine equations are completely solved.

In this lesson, you are going to learn about such equations, their solutions and their geometric interpretation.

Linear Diophantine Equations

A *linear Diophantine equation* in two variables is an equation of the form

$$a * x + b * y = c$$

where a , b and c are integers. The goal is to find the integer solutions x and y .

Here are some examples:

$$3x + 8y = 22$$

$$x - 10y = 1$$

Such equations can be solved completely, and *Brahmagupta* constructed the first known solution.

Example about Coins

Do you remember the problem about coins?

$$5x + 25y = 200$$

This is a linear Diophantine equation.

Let's try to solve it.

The important thing is that in this problem, x and y cannot be negative since they are a number of coins.

You can divide each side of the equation by 5:

$$x + 5y = 40$$

From this, you get

$$x = 40 - 5y$$

Since x takes non-negative values, then y can change from 0 to 8 (if you take $y = 9$, then no such non-negative integer x exists so that $x + 45 = 40$). So the solutions to the equation are

$$(40, 0), (35, 1), (30, 2), (25, 3), (20, 4), (15, 5), (10, 6), (5, 7), (0, 8)$$

So there are 9 ways to make \$2.00 from only nickels and quarters.

Such equations, if they do have solutions, have infinitely many of them. But in this case, there is a condition on the set of solutions to being non-negative. That's why there are finitely many of them.

Examples

Linear Diophantine equations can have infinitely many solutions, or they can have no solutions at all.

Consider the equation

$$14x + 34y = 90$$

Check that $x = 4$ and $y = 1$ is a solution:

$$14 * 4 + 34 * 1 = 90$$

Other solutions are $(21, -6)$, $(38, -13)$, $(55, -20)$, In fact, this goes on infinitely. All solutions have the form $\{4 + 21k, 1 - 7k\}$, where k is an integer.

Now consider the equation

$$12x + 18y = 35$$

With this one, you can easily see that it has no solutions at all. No matter what x and y , the left-hand side of the equation is an even number, while the right-hand side is odd.

Logic behind the Solution

The greatest thing about linear Diophantine equations is that they can be solved completely.

The complete algorithmic method for finding all the integer solutions requires the extended Euclidean algorithm. But you should concentrate on two questions:

- › When does $a * x + b * y = c$ have integer solutions (x, y) ?
- › If there exists a solution at all, how many solutions are there altogether?

Let's work out a few examples. The first equation is

$$12x + 16y = 21$$

The left-hand side is always divisible by 4, which is the greatest common divisor of 12 and 16, but the right-hand side is not. Therefore, this equation has no solution. Hence:

If $a * x + b * y = c$ has an integer solution, then c must be an integer multiple of $\gcd(a, b)$.

With that in mind, let's try an example that has a chance of having solutions:

$$12x + 16y = 24$$

You can divide through by 4 to get $3x + 4y = 6$. The extended Euclidean algorithm produces a solution $3 * (-1) + 4 * 1 = 1$. You can multiply everything by 6 to get

$$3 * (-6) + 4 * 6 = 6$$

You just found a solution: $(-6, 4)$.

Solutions of Linear Diophantine Equations

Now you can completely answer the previous two questions.

The equation

$$a * x + b * y = c$$

has a solution if and only if c is a multiple of the greatest common divisor of a and b .

Moreover, if (x, y) is a solution, then the other solutions have the form $(x + k * v, y - k * u)$, where k is an arbitrary integer and u and v are the quotients of a and b (respectively) by the greatest common divisor of a and b .

For example, the Diophantine equation

$$6x + 21y = 30$$

has infinitely many solutions since 30 is a multiple of 3 and the greatest common divisor of 6 and 21.

On the other hand, the equation

$$6x + 21y = 10$$

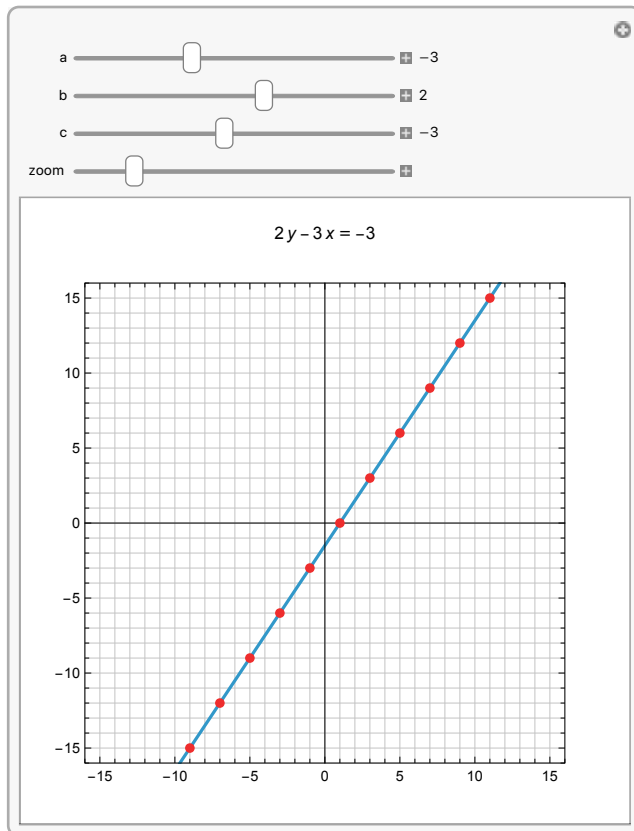
has no solutions at all.

Geometric Interpretation

Let's describe linear Diophantine equations geometrically.

The equation $a * x + b * y = c$ gives a line.

The solutions to this equation are the integer points that are on the line:



Garces Medina, Emmanuel. 2010. "Linear Diophantine Equations." Wolfram Demonstrations Project. demonstrations.wolfram.com/LinearDiophantineEquations.

Summary

- A *linear Diophantine equation* in two variables is an equation of the general form $a * x + b * y = c$, where a , b and c are integers. The goal is to find the integer solutions x and y .

- The equation $a * x + b * y = c$ has a solution if and only if c is a multiple of the greatest common divisor of a and b . If this is the case, then there are infinitely many solutions.
- Geometrically, a linear Diophantine equation gives a line. The solutions to these equations are the integer points that are on the line.

15 | Diophantine Equations of Degree 2

You already know about Diophantine equations and how difficult they are to solve.

After examining linear Diophantine equations, it would be very natural to consider *Diophantine equations of degree 2* or *quadratic Diophantine equations*.

How to solve a general Diophantine equation of degree 2 is a hard task and lies outside the scope of our book, but there are special cases worth knowing.

In this lesson, you will learn about two very famous special cases of the Diophantine equations of degree 2.

Diophantine Equations of Degree 2

A general *Diophantine equation of degree 2* in two variables x and y is given by

$$a * x^2 + b * x * y + c * y^2 = k$$

where a , b , c and k are integers. The goal is to find the integer solutions x and y .

They are also called *quadratic Diophantine equations*.

The slightly less general degree 2 equation is

$$a * x^2 + c * y^2 = k$$

where a , c and k are integers and the goal is to find the integer solutions x and y .

Here are a couple of examples:

$$2 x^2 + 6 y^2 = 74$$

$$3 x^2 - 6 x y + 7 y^2 = 15$$

Quadratic Diophantine equations in two variables can be completely solved. For equations in more than two variables, there are additional deep results.

Pell's Equation

Consider an equation of the form

$$x^2 - n y^2 = 1$$

where n is a nonsquare natural number and the integer solutions are sought for x and y .

It's a very special type of equation. It is called *Pell's equation* or the *Pell–Fermat equation*.

As you can see, it is a quadratic Diophantine equation in two variables.

Pell's equation has infinitely many distinct integer solutions.

For example, the equation

$$x^2 - 2 y^2 = 1$$

is Pell's equation for $n = 2$. Among its solutions are

$$(-1, 0), (1, 0), (3, 2), (3, -2), (-3, 2), (-3, -2) \dots$$

The solutions of Pell's equation can be used to approximate the square root of n by rational numbers of the form $\frac{x}{y}$.

The History of Pell's Equation

Solutions to specific examples of Pell's equation had been known for much longer, since the time of Pythagoras in Greece and a similar timeframe in India.

As early as 400 BC, mathematicians studied the numbers arising from Pell's equation $x^2 - 2 y^2 = 1$ and from the closely related equation $x^2 - 2 y^2 = -1$.

Brahmagupta found an integer solution to $92 x^2 + 1 = y^2$ circa 628.

Pell's equation was also solved by the Indian mathematicians *Bhaskara* in the twelfth century and *Narayana Pandit* in the fourteenth century. Both found general solutions for Pell's equation.



William Brouncker

William Brouncker was the first European to solve Pell's equation.



Pierre de Fermat

The first extensive study of this equation is credited to *Pierre de Fermat*.

The incorrect attribution of the work to Pell was actually the doing of *Leonard Euler*. He wrongly credited *John Pell* with Brouncker's solution to the equation.



Joseph – Louis Lagrange

The general theory of Pell's equation was developed by *Joseph-Louis Lagrange* in 1766–1769.

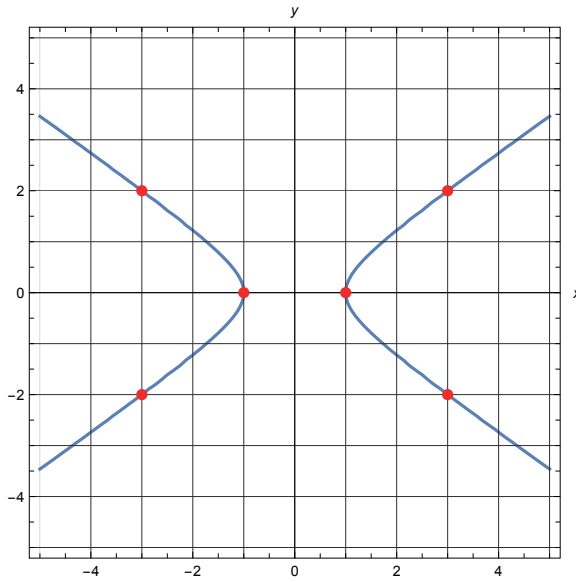
Geometric Interpretation of Pell's Equation

Let's describe Pell's equation geometrically.

The equation $x^2 - n \cdot y^2 = 1$ defines a curve in a plane, more specifically, it defines a *hyperbola*.

The solutions to this equation are the integer points that are on the curve.

Look at the plot of Pell's equation $x^2 - 2y^2 = 1$:



The solutions (x, y) in the range $-5 \leq x \leq 5$ and $-5 \leq y \leq 5$ are $(-1, 0)$, $(1, 0)$, $(3, 2)$, $(3, -2)$, $(-3, 2)$, $(-3, -2)$

Pythagorean Equation

Fermat's last theorem is one of the most famous theorems in number theory.

It states that the equation

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

has no integer solutions for $n > 2$.

It was solved in 1995 by English mathematician *Andrew Wiles*.

A particular case of the previous equation is when you take $n = 2$. The equation

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

is called the *Pythagorean equation*. The goal is to find the positive integer solutions x , y and z .

As you can see, it is a quadratic Diophantine equation in three variables x , y and z .

The Pythagorean equation has infinitely many solutions.

Pythagorean Triples

The solutions of the Pythagorean equation $x^2 + y^2 = z^2$ are called *Pythagorean triples*.

A Pythagorean triple is a triple of positive integers (a, b, c) that satisfies the Pythagorean equation:

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

The smallest and best-known Pythagorean triple is $(3, 4, 5)$.

It's easy to see that if (a, b, c) is a Pythagorean triple, then so is

$$(k * a, k * b, k * c)$$

for any positive integer k .

It's common to consider only *primitive Pythagorean triples* or *reduced triples* in which a, b and c are relatively prime because other solutions can be generated from the primitive ones.

Some examples of primitive Pythagorean triples are

$$(3, 4, 5)$$

$$(5, 12, 13)$$

$$(8, 15, 17)$$

$$(7, 24, 25)$$

Pythagorean Theorem

The Pythagorean triple gets its name from the *Pythagorean theorem*, which states:

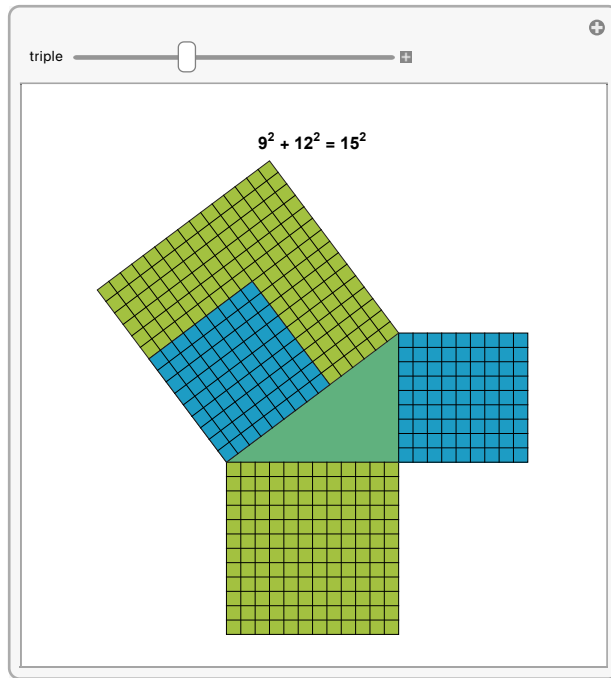
Every right triangle has side lengths satisfying the Pythagorean equation $x^2 + y^2 = z^2$.

Or:

The area of the square whose side is the hypotenuse (the side opposite the right angle) is equal to the sum of the areas of the squares on the other two sides.

So, Pythagorean triples (a, b, c) are the three integer side lengths of a right triangle.

Here is a visual representation of the Pythagorean theorem:



Morris, Rob, and Stephen Wolfram. 2007. "Pythagorean Triples." Wolfram Demonstrations Project. demonstrations.wolfram.com/PythagoreanTriples.

Summary

- A general *Diophantine equation of degree 2* or a *quadratic Diophantine equation* in two variables x and y is given by $a * x^2 + b * x * y + c * y^2 = k$, where a, b, c and k are integers. The goal is to find the integer solutions x and y .
- Quadratic Diophantine equations in two variables can be completely solved.
- An equation of the form $x^2 - n * y^2 = 1$ where n is a nonsquare natural number is called *Pell's equation*.
- Geometrically, Pell's equation defines a curve in a plane, more specifically, a *hyperbola*.
- The equation $x^2 + y^2 = z^2$ is called the *Pythagorean equation*. The goal is to find the positive integer solutions x, y and z .
- The solutions of the Pythagorean equation are called *Pythagorean triples*.
- The *Pythagorean theorem* states that every right triangle has side lengths satisfying the Pythagorean equation.
- Pythagorean triples are the three integer side lengths of a right triangle.

Part 5 Exercises

5.1 Where does the word Diophantine come from?

Solution

The word Diophantine comes from the Hellenistic mathematician of the third century, Diophantus of Alexandria, who was a Greek mathematician and made a study of such equations. He was one of the first mathematicians to introduce symbolism into algebra.

5.2 Which of these Diophantine equations are linear?

1) $2x - 14y + 35z^2 - 123 = 0$

2) $36y + 8 = -23x - 3$

3) $x^2 - 2y^2 = 1$

4) $18z = -5y$

Solution

The linear Diophantine equations are 2 and 4. It would have been much more easily answered if they were written in a more traditional way, like:

2) $23x + 36y = 5$

4) $5y + 18z = 0$

5.3 Does the linear Diophantine equation $57x + 437y = 247$ have integer solutions? If so, find one solution.

Solution

The theorem says that the linear Diophantine equation $57x + 437y = 247$ has a solution if and only if 247 is a multiple of the greatest common divisor of 57 and 247.

You can use the function GCD in Wolfram Language to find the greatest common divisor of 57 and 247:

```
In[ ]:= GCD [ 57, 247 ]
```

```
Out[ ]:= 19
```

You can then check to see if 247 is a multiple of 19:

```
In[ ]:= 247 / 19
```

```
Out[ ]:= 13
```

Indeed, $247 = 19 * 13$. So the equation has a solution. Moreover, it has infinitely many solutions.

You can find a solution with the help of FindInstance in Wolfram Language:

```
In[ ]:= FindInstance [ 57 x + 437 y == 247 , { x, y } , Integers ]
```

```
Out[ ]:= { { x → 12, y → -1 } }
```

You just found a solution: (12, -1).

5.4 Show that there are no integer solutions to the equation $35x + 150y = 19$.

Solution

Consider the equation $35x + 150y = 19$.

The left-hand side is always divisible by 5, as it both divides 35 and 150. The right-hand side, however, is not divisible by 5.

Therefore, this equation has no solution. If you use the FindInstance function again, it will produce an empty set of solutions:

```
In[ ]:= FindInstance [ 35 x + 150 y == 19 , { x, y } , Integers ]
```

```
Out[ ]:= { }
```

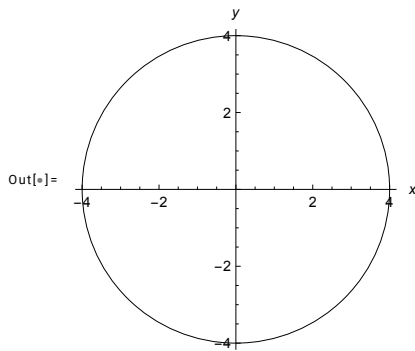
5.5 Using Wolfram Language, geometrically show that there cannot be a Pythagorean triple $(x, y, 4)$.

Solution

The Pythagorean triple $(x, y, 4)$ means there are natural numbers x and y such that $x^2 + y^2 = 4^2$.

Geometrically, $x^2 + y^2 = 4^2$ is a circle with a radius of 4 around the origin. Use Graphics and Circle to plot it in Wolfram Language:

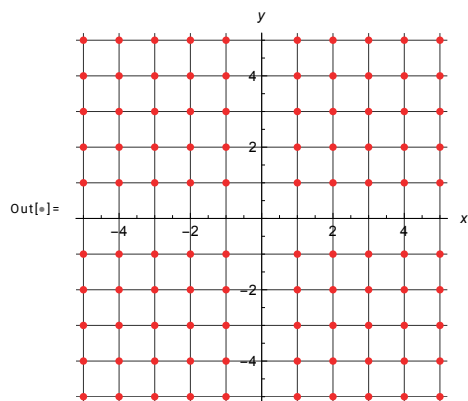
```
In[ ]:= Graphics [ Circle [ { 0, 0 } , 4 ] , Axes → True, AxesLabel → { x, y } ]
```



Now draw the points in the ranges $-5 \leq x \leq 5$ and $-5 \leq y \leq 5$ with coefficients that are natural numbers. Use Point and the option GridLines in Wolfram Language:

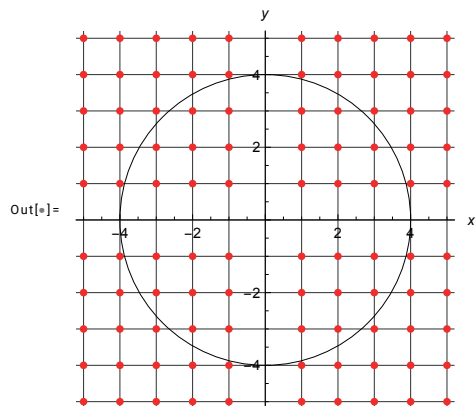
```
In[ ]:= pts = Table [ { x, y } , { x, { -5, -4, -3, -2, -1, 1, 2, 3, 4, 5 } } ,  
                    { y, { -5, -4, -3, -2, -1, 1, 2, 3, 4, 5 } } ];
```

```
In[ ]:= Graphics [ { Red, PointSize [ 0.02 ] , Point [ Flatten [ pts, 1 ] ] },
  GridLines -> { Range [ -5, 5 ], Range [ -5, 5 ] }, Axes -> True, AxesLabel -> { x, y } ]
```



Now combine those two plots:

```
In[ ]:= Graphics [ { Red, PointSize [ 0.02 ] , Point [ Flatten [ pts, 1 ] ] , Black, Circle [ { 0, 0 }, 4 ] },
  GridLines -> { Range [ -5, 5 ], Range [ -5, 5 ] }, Axes -> True, AxesLabel -> { x, y } ]
```



As you can see, no points lie on the circle. Therefore, a Pythagorean triple $(x, y, 4)$ does not exist.

Cryptography

16 | Cryptography



For many years, number theory was thought to be without many practical applications.

British mathematician G. H. Hardy once said, “The theory of numbers has always been regarded as one of the most obviously useless branches of pure mathematics.”

The significant increase in the availability and usefulness of computers in the twentieth century drastically changed that situation.

The best known application of number theory is *cryptography*.

In this chapter, you will learn about cryptography, a large and active field of research, and one very important cryptosystem, the RSA algorithm.

What Is Cryptography?

Cryptography is the practice and study of hiding information, which means codifying a message to preserve its content from unwanted eyes. The word “cryptography” was formed using the prefix “crypt-,” which means “hidden,” and the suffix “-graphy,” which means “writing.”

Mathematical concepts form the basis of the techniques used in cryptography to protect information. The goal is to convert messages in a way that makes it hard to decode them.

Mathematics, computer science, electrical engineering, communication science and physics all contribute to modern cryptography.

Generally, there are three types of cryptography:

› *Symmetric-key cryptography*

This is an encryption system where a single common key is used to encrypt and decrypt messages.

› *Asymmetric-key cryptography*

This is an encryption system where a pair of keys is used to encrypt and decrypt information.

› *Hash functions*

This type of cryptography uses no keys.

History of Cryptography

The history of cryptography can be divided into three distinct phases.



A scytale, an ancient Greek transposition cipher device

The initial phase involved manual cryptography, which has roots stretching back to antiquity. *Transposition* and *substitution* are the main classical cipher types; the former rearranges the order of letters in a message, while the latter replaces them systematically. One early substitution cipher was the *Caesar cipher*. It replaced each letter of the plaintext with another letter a set number of positions further in the alphabet.



The Enigma machine

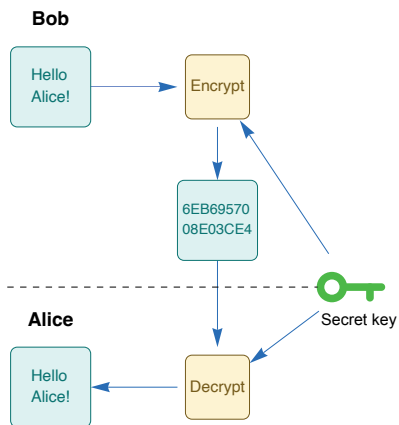
The second phase is the mechanization of cryptography. The early twentieth century saw the invention of numerous mechanical encryption/decryption devices, notably *rotor machines*, such as the *Enigma machine*, famously used by Germany's government and military from the late 1920s and during World War II.



Modern laptop

The most dramatic shift, occurring in the final two decades of the twentieth century (the third phase), was the adaptation of cryptology for the *information age*. Modern cryptography relies heavily on various mathematical fields, such as information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory and finite mathematics. Unlike classical ciphers, which only encrypted written text, computers enabled the encryption of any data in binary format.

Symmetric-Key Cryptography



In cryptography, a *key* is a character string used in encryption algorithms to transform data into an apparently random form. Data is encrypted like a physical key securing a lock, requiring a matching decryption key for access.

We call the original data *plaintext*; the encrypted data is called *ciphertext*.

Symmetric-key cryptography is a type of encryption scheme where the same key is used both to encrypt and decrypt messages.

A shared secret key, used by both sender and receiver, can be a password, code or secure random string of letters/numbers.

The Need for Asymmetric Cryptography

Symmetric algorithms allow for messages to be encrypted and decrypted quickly. Simply lengthening keys enhances the security offered by symmetric encryption.

However, there is a significant disadvantage. As you already know, in symmetric-key cryptography, both the sender and receiver share the same key.

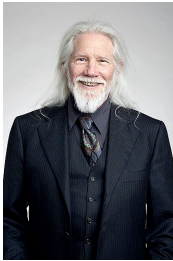
They have to exchange the key somehow.

Sharing keys over unsecured connections risks malicious interception by third parties. If they gain access to a specific symmetric key, the security of any data encrypted using that key is compromised.

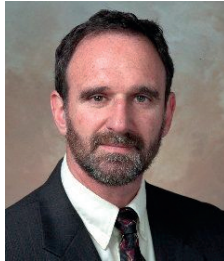
If you could find a method of encryption/decryption such that exchanging the keys does not reveal how to decrypt intercepted messages, then you would avoid this problem.

Using such a system, messages are encrypted with the receiver's public key, and only their private key can decrypt them.

Asymmetric-Key Cryptography



Whitfield Diffie



Martin Hellman

In an innovative paper from 1976, *Whitfield Diffie* and *Martin Hellman* introduced a new type of cryptographic system that uses two keys.

Here two different but mathematically related keys are used—a *public key* and a *private key*.

The public key may be freely distributed and is used for encryption.

The private must remain secret and is used for decryption.

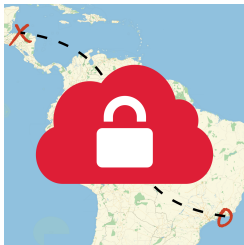
This type of cryptosystem is called *asymmetric* or *public-key cryptography*.

This system is so constructed that the calculation of the private key is computationally impossible from the public key, even though they are related.

Summary

- *Cryptography* is the practice and study of hiding information.
- A *key* is a character string used in encryption algorithms to transform data into an apparently random form.
- The original data is the *plaintext*; the encrypted data is the *ciphertext*.
- *Symmetric-key cryptography* is a cryptographic system in which the same key is used both to encrypt and decrypt messages.
- *Asymmetric- or public-key cryptography* is a cryptographic system that uses pairs of keys: a public key and a private key.

17 | The RSA Algorithm



There are many public-key cryptography algorithms. One of the most important ones is the *RSA algorithm*.

The RSA algorithm is entirely based on number theory, particularly modular arithmetic.

Its security relies on the computational difficulty of factoring large numbers.

It's a simple yet reliable and elegant algorithm.

In this lesson, you'll get to know the mathematical background of the RSA algorithm, as well as how it works in practice.

History of RSA

The concept of an asymmetric public-key cryptosystem was first proposed by Whitfield Diffie and Martin Hellman in 1976. They tried to apply number theory and used a shared secret key created from exponentiation of some number, modulo a prime number. Nevertheless, they did not present a completed algorithm, perhaps because the difficulty of factoring was not well studied then.



Ron Rivest



Adi Shamir



Leonard Adleman

At the Massachusetts Institute of Technology, *Ron Rivest*, *Adi Shamir* and *Leonard Adleman* were working to create such an algorithm. Finally, in 1977, they publicly described the algorithm, which is known as *RSA*—the initials of their surnames in the same order as their paper.



Clifford Cocks

It's worthy to note that *Clifford Cocks*, an English mathematician working for the British government, described an equivalent system in 1973. However, because it needed expensive computers, it was seen as mostly a curiosity and, to public knowledge, never put into practice. The discovery he made was kept secret until 1997 as it was classified as top secret.

RSA Algorithm

The RSA algorithm has four steps:

› Key generation

Two pairs of keys need to be generated, a private key and a public key.

› Key distribution

The exchanging parties need to know each other's public keys.

› Encryption

The sender has to encrypt the message using the public key of the receiver.

› Decryption

The receiver has to decrypt the message using his or her private key.

Key Generation

The idea is to generate two mathematically related keys, but in a way that it's computationally impossible to compute the private key from the public key. In fact, in the time it takes to derive the private key from the public key, the information no longer has significant value.

This is how we generate the keys.

1. Select p and q to be distinct large primes.

For security, the integers p and q should be chosen at random and be at least several hundred digits. The degree of security is dependent on their sizes. p and q are kept in secret.

2. Compute $n = p * q$.

n is used as the *modulus* for both the public and private keys.

3. Choose an integer e such that $1 < e < (p - 1) * (q - 1)$ and $\gcd(e, (p - 1) * (q - 1)) = 1$.

e is used as the public-key *exponent*.

The *public key* is (n, e) .

4. Choose d to satisfy the congruence relation $d * e \equiv 1 \pmod{(p - 1) * (q - 1)}$.

d is used as the private-key *exponent*.

The *private key* is (n, d) .

Key Distribution

You now have the keys:

(n, e) — public key

(n, d) — private key

Suppose that Bob wants to send information to Alice.

In order to do that, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message.

In order for Bob to send encrypted messages, Alice transmits her public key (n, e) to Bob through a trusted, but not necessarily secret, route. Alice's private key (n, d) is never distributed.

The algorithm's security depends on the difficulty of factoring large numbers. In order to calculate d , it is necessary to factor n to get p and q , which is very difficult (in fact, exponential in the number of digits in p and q).

Encryption

The public key (n, e) is used for encryption.

Once Bob gets Alice's public key, he can send a message M to Alice.

To do it, he first turns M into an integer m . It is assumed that $0 \leq m < n$. Otherwise, you can break m down with smaller pieces and encode each separately.

He then computes the ciphertext c , using Alice's public key, corresponding to

$$m^e \equiv c \pmod{n}$$

Bob then transmits c to Alice.

Using modular exponentiation, one can reasonably quickly perform this task, even for very large numbers.

Decryption

The private key (n, d) is used for decryption.

After Alice received the encrypted message c , she needs to recover m .

She can recover m from c by using her private key exponent d by computing

$$c^d \equiv m \pmod{n}$$

Given m , she can now recover the original message M .

Example

Suppose Alice wants to receive a message from Bob. She selects two primes, say

$$p = 61$$

$$q = 53$$

In reality, they would be incredibly large. Then Alice computes

$$n = p * q = 3233$$

$$(p - 1) * (q - 1) = 3120$$

She then chooses

$$e = 17$$

such that

$$\gcd(e, ((p - 1) * (q - 1))) = \gcd(17, 3120) = 1$$

The *public key* is generated:

$$(n, e) = (3233, 17)$$

Now Alice chooses

$$d = 2753$$

such that

$$d * e \equiv 1 \pmod{(p-1)*(q-1)}$$

$$2753 * 17 \equiv 1 \pmod{3120}$$

The *private key* is generated:

$$(n, d) = (3233, 2753)$$

So the keys are generated:

$$(n, e) = (3233, 17) \text{ — public key}$$

$$(n, d) = (3233, 2753) \text{ — private key}$$

Bob wants to send the message $m = 65$ to Alice.

In order to encrypt it, he uses Alice's public key and calculates c corresponding to $m^e \equiv c \pmod{n}$. So

$$c = m^e \pmod{n}$$

$$c = 65^{17} \pmod{3233} = 2790$$

The encrypted message is $c = 2790$.

To decrypt c , Alice uses her private key and calculates m corresponding to $c^d \equiv m \pmod{n}$. So

$$m = c^d \pmod{n}$$

$$m = 2790^{2753} \pmod{3233} = 65$$

Thus, the original message was 65.

Summary

- One of the most important public-key cryptosystems is the *RSA algorithm*.
- It was first publicly described by *Ron Rivest*, *Adi Shamir* and *Leonard Adleman* in 1977.
- The RSA algorithm has four steps: key generation, key distribution, encryption and decryption.
- The RSA algorithm is entirely based on modular arithmetic and its security relies on the computational difficulty of factoring large numbers.

Part 6 Exercises

6.1 What are the two different keys used in an asymmetric cryptosystem called? What is the main difference between them?

Solution

The two different keys used in an asymmetric cryptosystem are called a public key and a private key.

The public key may be freely distributed and is used for encryption. The private must remain secret and is used for decryption.

6.2 Using Wolfram Language, generate a random symmetric key and use it to encrypt and decrypt a message. Use the functions `GenerateSymmetricKey`, `Encrypt` and `Decrypt` in Wolfram Language.

Solution

Generate a random symmetric key:

```
In[ ]:= key = GenerateSymmetricKey [ ]
```

```
out[ ]= SymmetricKey[ Cipher: AES256  
Key size: 256 b]
```

Use the key to encrypt a message that says "Introduction to Number Theory":

```
In[ ]:= encrypted = Encrypt [ key, "Introduction to Number Theory" ]
```

```
out[ ]= EncryptedObject[ Data length: 32 B  
Original form: String]
```

Use the same key to decrypt it:

```
In[ ]:= decrypted = Decrypt [ key, encrypted ]
```

```
out[ ]= Introduction to Number Theory
```

6.3 Using Wolfram Language, generate an RSA cryptosystem and use it to encrypt and decrypt a message. Use the function `GenerateAsymmetricKeyPair` with the type "RSA" in Wolfram Language.

Solution

Generate corresponding public and private keys:

```
In[ ]:= keys = GenerateAsymmetricKeyPair [ "RSA" ]
```

```
Out[ ]:= { PrivateKey → PrivateKey[ Type: RSA  
Public modulus size: 2048 b  
Private exponent size: 2048 b ],  
PublicKey → PublicKey[ Type: RSA  
Public modulus size: 2048 b ] ] }
```

Encrypt a message using the public key:

```
In[ ]:= encrypted1 = Encrypt [ keys [ "PublicKey" ] , "Prime numbers never end ! " ]
```

```
Out[ ]:= EncryptedObject[ Data length: 256 B  
Original form: String ]
```

Decrypt with the private key:

```
In[ ]:= Decrypt [ keys [ "PrivateKey" ] , encrypted1 ]
```

```
Out[ ]:= Prime numbers never end !
```

Alternatively, encrypt with the private key:

```
In[ ]:= encrypted2 = Encrypt [ keys [ "PrivateKey" ] , "Prime numbers never end ! " ]
```

```
Out[ ]:= EncryptedObject[ Data length: 256 B  
Original form: String ]
```

Decrypt with the public key:

```
In[ ]:= Decrypt [ keys [ "PublicKey" ] , encrypted2 ]
```

```
Out[ ]:= Prime numbers never end !
```

6.4 Using Wolfram Language, create an RSA cryptosystem step by step and test it.

Solution

The first step is key generation.

1. Select p and q to be distinct primes. The RSA algorithm is effective when the primes are really large, but for this exercise, you don't have to select large primes. Use `RandomPrime` to get pseudorandom prime numbers up to 100:

```
In[ ]:= p = RandomPrime [ 100 ]
```

```
Out[ ]:= 59
```

```
In[ ]:= q = RandomPrime [ 100 ]
```

```
Out[ ]:= 17
```

2. Compute $n = p * q$:

```
In[ ]:= n = p * q
```

```
Out[ ]:= 1003
```

3. Choose an integer e such that $1 < e < (p-1) * (q-1)$ and $\gcd(e, (p-1) * (q-1)) = 1$.

Use the functions FindInstance and GCD in Wolfram Language:

```
In[*]:= FindInstance[1 < e < (p - 1) * (q - 1) && GCD[e, (p - 1) * (q - 1)] == 1, e, Integers]
```

```
Out[*]:= {{e -> 3}}
```

```
In[*]:= e = 3;
```

So $e = 3$ and the public key is (1003, 3).

4. Choose d to satisfy the congruence relation $d * e \equiv 1 \pmod{(p-1) * (q-1)}$, in our case, $d * 3 \equiv 1 \pmod{936}$.

Use the functions FindInstance and Mod in Wolfram Language:

```
In[*]:= FindInstance[Mod[d * e, (p - 1) * (q - 1)] == 1, d, Integers]
```

```
Out[*]:= {{d -> 619}}
```

```
In[*]:= d = 619;
```

So $d = 619$ and the private key is (1003, 619).

Suppose Bob wants to send the message $m = 73$ to Alice:

```
In[*]:= m = 73;
```

In order to encrypt it, he uses Alice's public key and calculates c corresponding to $c \equiv m^e \pmod{n}$. So

```
In[*]:= c = Mod[m^e, n]
```

```
Out[*]:= 856
```

The encrypted message is $c = 856$.

To decrypt c , Alice uses her private key and calculates m corresponding to $m \equiv c^d \pmod{n}$. So

```
In[*]:= m = Mod[c^d, n]
```

```
Out[*]:= 73
```

Thus, the original message was 73.



Additional Topics

18 | Primality Testing: Miller–Rabin

Prime numbers are of immense importance in number theory, and determining whether a number is prime is very important.

A *primality test* is an algorithm for determining whether a number is prime.

Primality tests, in contrast to integer factorization, typically don't yield prime factors; they only state whether the number is prime.

While factorization is a computationally difficult problem, primality testing is comparatively easy.

In this lesson, you are going to learn about two types of primality tests, as well as about one very efficient test called the *Miller–Rabin primality test*.

Deterministic Tests

A *primality test* is an algorithm for determining whether a number is prime or not.

There are two types of primality tests: *deterministic* and *probabilistic*.

A *deterministic* test outputs true when the number is a prime and false when the number is composite, with probability 1, so it determines with absolute certainty whether a number is prime.

Trial division is one of the simplest deterministic primality tests. It naively checks the condition of a number being prime.

If a number n is divisible by any number from 2 to $\sqrt{n}$, then n is composite; otherwise, it is prime.

For example, let's test the primality of 19. You only need to use integer divisors less than or equal to $\sqrt{19} \approx 4.35$. Those would be:

2, 3, 4

19 is not divisible by any of these, so 19 is prime.

This is not an efficient algorithm. Processing time increases exponentially with the

digits of the number. It can take days or months to factor large numbers that do not have factors in the small primes using the trial division method.

Probabilistic Tests

A *probabilistic* test attempts to determine whether a number is prime or composite. The output of the test should be correct with high probability, independent of the number being tested.

Probabilistic tests might, although with very small probability, falsely identify a composite number as prime, but never a prime number as composite. However, they are much faster than deterministic tests.

Until its primality can be demonstrated deterministically, we refer to a number that has passed a probabilistic prime test as a *probable prime*.

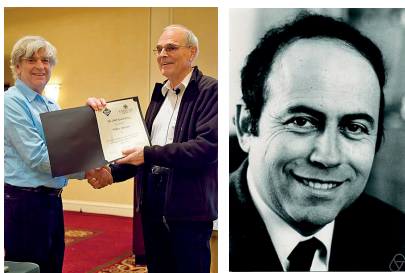
A number that passes a probabilistic test but is, in fact, composite, is known as a *pseudoprime*.

The basic structure of probabilistic tests is as follows:

1. Randomly pick a number a .
2. Check an equality involving a and the given number n . If the equality fails to hold, then n is a composite number, a is identified as a *witness* for the compositeness and the test stops.
3. Keep repeating from step 1 until you achieve the required accuracy.

If, after one or more iterations, n isn't found to be a composite number, it can be declared a probable prime.

The Origins of the Miller–Rabin Primality Test



Gary L. Miller

Michael O. Rabin

The *Miller–Rabin primality test* is a probabilistic primality test that determines whether a given number is prime.

The discovery was made by *Gary L. Miller* in 1976. His version of the test is deterministic; however, its correctness relies on the unproven extended Riemann hypothesis.

Michael O. Rabin modified it to obtain an unconditional probabilistic algorithm in 1980.

Mathematics behind the Miller–Rabin Primality Test

The Miller–Rabin test uses equalities that are only true for prime numbers. It checks whether they hold for a number that is tested for primality.

Let's discuss some mathematical concepts behind the test.

› First, suppose p is prime, and consider the modular equation:

$$x^2 \equiv 1 \pmod{p}$$

This is equivalent to

$$(x - 1)(x + 1) \equiv 0 \pmod{p}$$

Since p is prime, p has to divide either $x - 1$ or $x + 1$. This leads to the following linear congruences:

$$x \equiv 1 \pmod{p}$$

$$x \equiv -1 \pmod{p}$$

› Now suppose n is prime and a is an integer relatively prime to n . Fermat's little theorem says that:

$$a^{n-1} \equiv 1 \pmod{n}$$

If you keep taking square roots of a^{n-1} , you will get either 1 or -1 . If you get -1 , then the equality $a^{2^r * d} \equiv -1 \pmod{n}$ holds and it is done. If you never get -1 , then when you have taken out every power of 2, you are left with $a^d \equiv 1 \pmod{n}$.

So you'll arrive at the following theorem.

Let n be an odd prime and let $n - 1 = 2^s * d$, where d is an odd integer and s is a positive number. Then, for each $1 \leq a \leq n - 1$, at least one of the following must hold:

› $a^d \equiv 1 \pmod{n}$

› $a^{2^r * d} \equiv -1 \pmod{n}$ for some $0 \leq r \leq s - 1$

The Miller–Rabin Primality Test

Given an odd integer n , if you can find an a such that

$$a^d \not\equiv 1 \pmod{n}$$

and

$$a^{2^r * d} \not\equiv -1 \pmod{n}$$

for all $0 \leq r \leq s - 1$, then n is not prime. a is called a *witness* for the compositeness of n .

Otherwise, a is called a *strong liar*, and n is a *strong probable prime* to base a . The term strong liar refers to the case where n is composite but the equations hold as they would for a prime.

If n is composite, most values for a will serve as witnesses, and the test will detect n as composite with high probability.

However, there's a small chance you might encounter an a that is a strong liar for n . Repeating the test with several independently chosen values of a will reduce the chance of this type of error.

Deterministic Variants of the Test

When the number n to be tested is small, much smaller sets of potential witnesses are sufficient. It is verified that, for example:

- If $n < 2047$, it is enough to test $a = 2$.
- If $n < 9\,080\,191$, it is enough to test $a = 31$ and 73 .
- If $n < 3\,215\,031\,751$, it is enough to test $a = 2, 3, 5, 7$.
- If $n < 341\,550\,071\,728\,321$, it is enough to test $a = 2, 3, 5, 7, 11, 13, 17$.

For numbers within the appropriate range, they provide fast deterministic primality tests that require no prior assumptions.

Example

Let's determine if $n = 221$ is prime. You can write:

$$n - 1 = 220 = 2^2 * 55$$

So $s = 2$ and $d = 55$.

You randomly select a number a such that $1 < a < 220$, say, $a = 174$. You then compute:

- $a^{2^0 * d} \bmod n = 174^{55} \bmod 221 = 47 \neq 1, n - 1$
- $a^{2^1 * d} \bmod n = 174^{110} \bmod 221 = 220 = n - 1$

This means that either 221 is prime or 174 is a strong liar for 221. You try another random a , this time choosing $a = 137$:

- $a^{2^0 * d} \bmod n = 137^{55} \bmod 221 = 188 \neq 1, n - 1$
- $a^{2^1 * d} \bmod n = 137^{110} \bmod 221 = 205 \neq 1, n - 1$

So 137 is a witness for the compositeness of 221, and 174 was in fact a strong liar.

Hence, 221 is composite.

Summary

- A *primality test* is an algorithm for determining whether a number is prime or not.
- There are two types of primality tests: *deterministic* and *probabilistic*.
- A *deterministic test* determines with absolute certainty whether a number is prime, while a *probabilistic test* attempts to determine whether a number is prime.

- The *Miller–Rabin primality test* is a probabilistic primality test that determines whether a given number is prime or not.
- *Gary L. Miller* discovered the test in 1976, and *Michael O. Rabin* modified it to obtain an unconditional probabilistic algorithm in 1980.

19 | Factorization: Pollard's Rho

As you've seen, it's possible to check efficiently whether or not an integer is prime. What about factoring a number?

Factoring numbers is very hard from a computational point of view.

So it is very important to come up with a factoring algorithm that factors numbers relatively fast.

In this lesson, you will learn about one particular factoring algorithm: *Pollard's rho algorithm*.

Prime Factorization Algorithms

There are many algorithms for determining the prime factors of a given number.

The simplest method of finding factors is so-called "direct search factorization," or *trial division*.

Trial division tests to see if an integer n , which is to be factored, can be divided by each number in turn that is less than n .

For example, the only numbers that divide 12 are 1, 2, 3, 4, 6 and 12. Selecting only the largest powers of primes in this list gives the prime factorization of 12:

$$12 = 3 * 4 = 2^2 * 3$$

Trial division is practical only for very small numbers.

There are no known efficient algorithms for factoring sufficiently large integers.

If factoring could be done efficiently, then the RSA encryption scheme could be broken.

Pollard's rho algorithm is one of the prime factorization algorithms. The British mathematician *John Pollard* invented it in 1975.

The Basis of Pollard's Rho Algorithm

Pollard's algorithm relies on the following mathematical concepts:

- › Modular arithmetic, which has already been discussed
- › The greatest common divisor, which has also already been discussed
- › The birthday paradox, which says that the probability of two people having the same birthday is unexpectedly high, even for a small set of people
- › Floyd's cycle-finding algorithm, which detects whether a sequence has become periodic

We will present neither the proof of the algorithm, nor where exactly these concepts are used.

Pollard's Rho Algorithm

Let's describe how the algorithm works.

The algorithm takes the number n you want to factor, and a polynomial $g(x)$.

In the original algorithm, $g(x) = (x^2 - 1) \bmod n$, but nowadays it is more common to use $g(x) = (x^2 + 1) \bmod n$.

The algorithm either returns a prime factor of n , or it fails.

It has the following steps.

First, assign arbitrary initial values to the variables x and y , say 2:

$$x \leftarrow 2$$

$$y \leftarrow 2$$

In the algorithm, d is the greatest common divisor of the absolute value of $x - y$ and n . Its initial value is 1:

$$d \leftarrow 1$$

While the value of d is 1, do

- › $x \leftarrow g(x)$
- › $y \leftarrow g(g(y))$
- › $d \leftarrow \gcd(\text{abs}(x - y), n)$

If, after this, $d = n$, then the algorithm failed.

Otherwise you've found a prime factor in the face of d .

Example

Factor the number 253.

Randomly choose $x = 4$ and $y = 4$ to begin and $g(x) = (x^2 + 1) \bmod n$. Begin tracking the greatest common divisor d with $d = 1$.

$d = 1$:

› $x \leftarrow g(x) = 17$

› $y \leftarrow g(g(y)) = 37$

› $d \leftarrow \gcd(\text{abs}(17 - 37), 253) = 1$

$d = 1$:

› $x \leftarrow g(x) = 37$

› $y \leftarrow g(g(y)) = 147$

› $d \leftarrow \gcd(\text{abs}(37 - 147), 253) = 11$

Now d does not equal 1. That means you have found a prime factor $d = 11$.

To find the other prime factor of 253, you can perform $253 \div 11 = 23$. 23 is obviously a prime number, so the prime factorization of 253 is

$$253 = 11 * 23$$

If the number n had more than two prime factors and the division produced another composite number, you could break that number into its prime factors by going through the algorithm again.

Summary

- Factoring numbers is very hard from a computational point of view.
- Pollard's rho algorithm is a prime factorization algorithm.
- The British mathematician John Pollard invented it in 1975.
- Pollard's rho algorithm relies on the concepts of modular arithmetic, the greatest common divisor, the birthday paradox and Floyd's cycle-finding algorithm.

20 | Diophantine Equations: Hilbert's Tenth Problem



David Hilbert

In August 1900, Paris hosted the second International Congress of Mathematicians. Among the invited speakers was *David Hilbert*.

Hilbert pointed out the most important unsolved mathematical problems that the twentieth century was to inherit from the nineteenth century.

At the time, those problems were unsolved, and many of them were highly influential for twentieth-century mathematics.

At the Paris conference, Hilbert presented 10 of the problems. The complete list of 23 problems was published after.

Hilbert's tenth problem is the tenth on the list of mathematical problems. It is completely resolved.

The Background of Hilbert's Tenth Problem

A *Diophantine equation* is a polynomial equation with integer coefficients in which only integer solutions are allowed.

Mathematicians have found solutions of many Diophantine equations and have shown that many others have no solutions.

For example, the equation

$$3x^2 - 2xyz - y^2z - 7 = 0$$

has an integer solution $x = 1$, $y = 2$ and $z = -2$.

On the other hand, the equation

$$x^2 + y^2 + 8 = 0$$

has no solutions.

Unfortunately, for different types of Diophantine equations, and even for some individual ones, mathematicians had to constantly devise new techniques.

In the tenth problem, Hilbert asked for a single method that could be applied to every equation.

Hilbert's Tenth Problem

Hilbert formulated the problem as follows:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

The words “process” and “finite number of operations” mean Hilbert was asking for an algorithm.

The term “rational integer” simply refers to the integers.

So Hilbert was asking for a general algorithm to decide whether a given polynomial Diophantine equation with integer coefficients has a solution in integers.

It's worthy to note that Hilbert's problem is not concerned with finding the solutions. It only asks if you can determine, in general, whether solutions exist.

It's a decision problem, a problem consisting of infinitely many individual problems, each of which requires a “yes” or “no” answer.

Solvability in Natural Numbers

Hilbert asked about solvability in integers. You can also consider the analogous problem of solvability among natural numbers.

It turns out that any general algorithm that can decide whether a given Diophantine equation has an integer solution could be modified into an algorithm that decides whether a given Diophantine equation has a natural number solution and vice versa.

So the two problems are equivalent as:

› Every natural number is the sum of the squares of four integers (Lagrange four-square theorem).

You simply replace every parameter with the sum of squares of four extra parameters.

› Every integer can be written as the difference of two natural numbers.

You can replace every parameter that ranges in integers with the difference of two parameters that range in natural numbers.

The work on the problem has been in terms of solutions in natural numbers, as it is easier to work with variables ranging in natural numbers rather than integers.

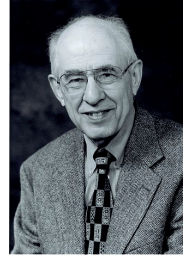
The Solution for Hilbert's Tenth Problem



Martin Davis



Yuri Matiyasevich



Hilary Putnam



Julia Robinson

Hilbert's tenth problem has been solved, and it has a negative answer.

There is no algorithm that, for a given arbitrary Diophantine equation, would tell whether or not the equation has a solution.

So, Hilbert's tenth problem is an undecidable problem.

Spanning 21 years and involving the combined efforts of *Martin Davis*, *Yuri Matiyasevich*, *Hilary Putnam* and *Julia Robinson*, the theorem was ultimately completed by Matiyasevich in 1970.

Hilbert's Tenth Problem in a Broader Sense

So the original statement of the tenth problem has a negative solution. What about solving Diophantine equations in rational numbers?

Determining the solvability of any Diophantine equation in rational numbers is the same as solving homogeneous Diophantine equations in integers.

A *homogeneous Diophantine equation* is a Diophantine equation that is defined by a homogeneous polynomial:

$$3x^2 - 2xy - y^2z = 0$$

Such equations represent only a subclass within the set of all Diophantine equations, and it is possible that there is a corresponding algorithm for this class.

Thus, you can understand the tenth problem in two senses:

- › Narrower sense: the decision problem of determining the solvability of an arbitrary Diophantine equation in integers (literally as the problem was stated)
- › Broader sense: the decision problem of determining the solvability of an arbitrary Diophantine equation in rational numbers

In the narrower sense, the tenth problem is closed; however, it is still open in the broader sense.

Solving equations in rational numbers remains one of the most important open cases of Hilbert's tenth problem taken in a broader sense.

Summary

- *Hilbert's problems* are 23 problems in mathematics published by the German mathematician *David Hilbert* in 1900.
- *Hilbert's tenth problem* is about the existence of a universal method for solving Diophantine equations.
- Hilbert's problem is not concerned with finding the solutions. It only asks if you can determine, in general, whether solutions exist.
- Hilbert's tenth problem has been solved, and it has a negative answer: no such algorithm exists.
- The impossibility of obtaining a general solution was the result of the combined work of *Martin Davis*, *Yuri Matiyasevich*, *Hilary Putnam* and *Julia Robinson* over the course of 21 years.
- Solving Diophantine equations in rational numbers remains one of the most important open cases of Hilbert's tenth problem taken in a broader sense.

21 | The Riemann Zeta Function

The *Riemann zeta function* is an extremely important special function in mathematics and physics.

It is related to deep results surrounding the prime number theorem.

Many of the properties of this function have been extensively investigated. However, several significant unsolved conjectures, most importantly the *Riemann hypothesis*, still remain.

In this lesson, we will not dig deep into analytic number theory. We will only get some insight into this remarkable function in mathematics.

Definition

Imagine the infinite sum

$$1 + 2^{-s} + 3^{-s} + 4^{-s} + \dots$$

The value of this sum will be different with every different s . Its value depends on s .

It would be interesting to look at a function of a variable s :

$$\zeta(s) = 1 + 2^{-s} + 3^{-s} + 4^{-s} + \dots$$

This function is called the *Riemann zeta function*. The variable s is, in general, a complex number.

A *complex number* is a number of the form $a + b \cdot i$.

a is called the *real part*, and b is called the *imaginary part*.

Since you have an infinite sum, you would like to find at which values of s it sums up to a particular number. Otherwise, it wouldn't make any sense.

The Riemann zeta function converges, which means the sum tends toward some number, when the real part of s is greater than 1.

Otherwise, the sum is infinite.

History



Leonard Euler

Leonard Euler first introduced and studied this function in the first half of the eighteenth century. He studied it as a function of a real variable. The complex analysis was not available at the time.



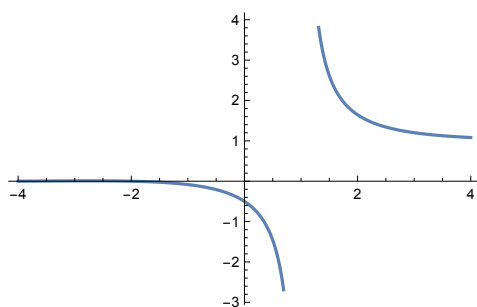
Bernhard Riemann

Bernhard Riemann, in his 1859 article, generalized Euler's definition for complex variables. Most importantly, he demonstrated a relationship between the function's zeros and the distribution of prime numbers. To this day, that article is considered to be one of the most important in number theory.

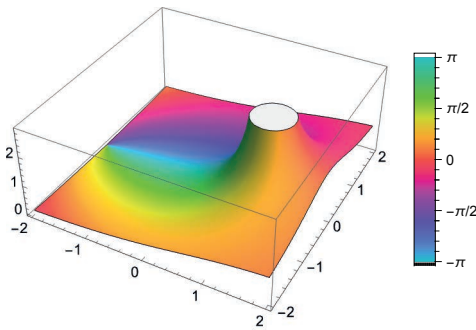
Plots of the Riemann Zeta Function

One simply cannot resist the temptation of plotting a function.

Here is the plot of the Riemann zeta function as a function of a real variable:



Now let's plot it as a function of a complex variable:



Zeros of the Riemann Zeta Function

In complex analysis, there is a technique that allows one to extend the domain of a given function. It is often done by defining further values of a function where it is not defined.

As was already said, the Riemann zeta function converges when the real part of s is greater than 1. But, in order to continue the lesson, you have to continue the Riemann zeta function to the entire complex plane, like Riemann did in his groundbreaking paper.

So from now on, keep in mind that our function is defined on the entire complex plane.

The *zeros* of the zeta function are values s such that $\zeta(s) = 0$.

There are two classifications for the zeros of the Riemann zeta function: the *trivial* and the *non-trivial*.

The *trivial* zeros are $-2, -4, \dots, -2n, \dots$. They are trivial in the sense that their existence is relatively easy to prove.

The *non-trivial* zeros have attracted far more interest. Their distribution is far less understood and, more importantly, their study yields impressive results in prime numbers and related number theory topics.

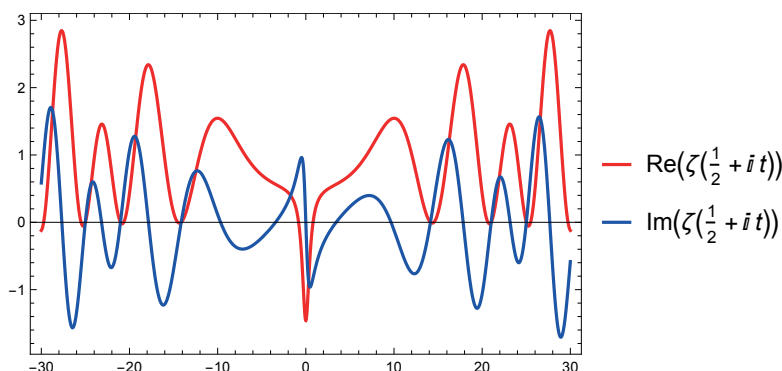
The Riemann Hypothesis

It is known that the real part of any non-trivial zero of the Riemann zeta function is greater than 0 and smaller than 1.

The *Riemann hypothesis* asserts that the real part of every non-trivial zero of the Riemann zeta function is $\frac{1}{2}$.

The Riemann hypothesis is considered to be the most important unsolved problem in pure mathematics. However, the numerical verification of the hypothesis to very high values suggests its truth.

In the following plot, the real part of the $\zeta(s)$ function is the red graph and the imaginary part is the blue graph. Here, $s = \frac{1}{2} + it$, where $-30 \leq t \leq 30$. The non-trivial zeros are the intersections between the red and blue graph on the horizontal line:



The Riemann hypothesis and some of its generalizations, along with Goldbach's conjecture and the twin prime conjecture, comprise the eighth problem in David Hilbert's list of 23 unsolved problems. The Clay Mathematics Institute also lists it as one of their Millennium Prize Problems.

Prime Numbers and the Riemann Hypothesis

Surprisingly enough, the Riemann zeta function is related to the distribution of prime numbers.

Euler made the first connection between zeta functions and prime numbers when he came up with the following formula:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

The expression states that the sum of the zeta function is equal to the product of the reciprocal of 1 minus the reciprocal of primes to the power s . We will not include the proof of it, but it is so good that you should look at it.

This remarkable connection established the basis of modern prime number theory.

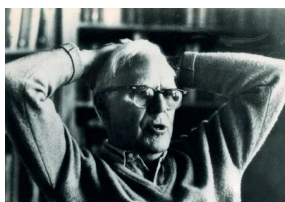
If the Riemann hypothesis turns out to be true, then it will shed light on the distribution of primes.

Summary

- The *Riemann zeta function* is a function $\zeta(s) = 1 + 2^{-s} + 3^{-s} + 4^{-s} + \dots$, where s is a complex variable.
- *Leonard Euler* first introduced and studied this function as a function of a real variable. *Bernhard Riemann* generalized Euler's definition for complex variables.

- There are two classifications for the *zeros* of the Riemann zeta function: the *trivial* and the *non-trivial*.
- The *Riemann hypothesis* asserts that the real part of every non-trivial zero of the Riemann zeta function is $\frac{1}{2}$.
- The Riemann hypothesis is considered to be the most important unsolved problem in pure mathematics.
- The Riemann hypothesis implies results about the distribution of prime numbers.

22 | Special Numbers



“One would be hard put to find a set of whole numbers with a more fascinating history and more elegant properties surrounded by greater depths of mystery—and more totally useless—than the perfect numbers.” — Martin Gardner

There are peculiar classifications within natural numbers that are of great interest both for mathematicians and lovers of mathematics.

Such subgroups of natural numbers are interesting and fun, and at first glance, one would think they don't possess any serious mathematical properties and are not connected to each other.

In reality, they do possess very serious properties and are related to each other.

So far, the book was mainly about prime and composite numbers. In this lesson, you will get to know some more.

The Aliquot Sum

A *proper* divisor is a divisor of a number n , excluding n itself.

For example, the proper divisors of 24 are {1, 2, 3, 4, 6, 8, 12}.

The sum of the proper divisors of a number is called the *aliquot sum*.

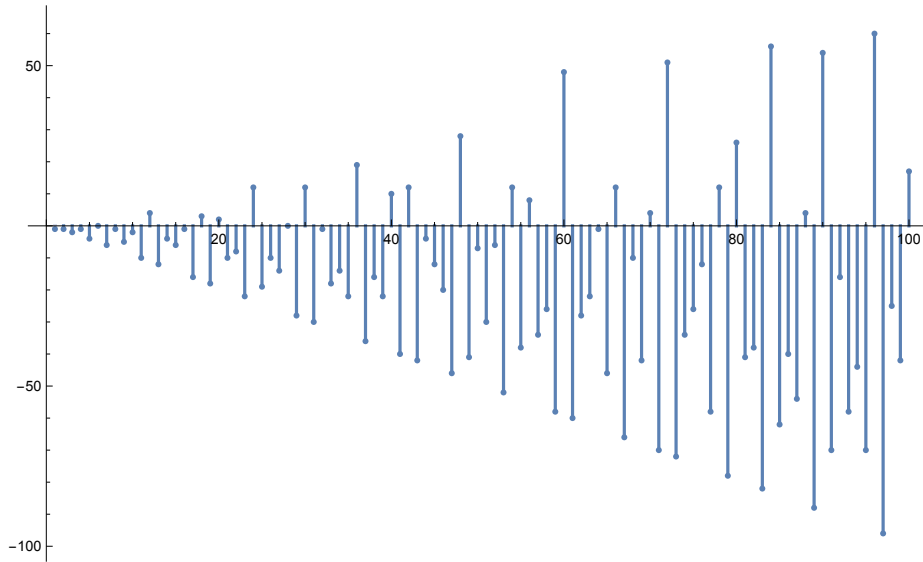
The aliquot sum of 24 is

$$1 + 2 + 3 + 4 + 6 + 8 + 12 = 36$$

Calculate the difference of the aliquot sum of the number and the number itself. In the case of 24, that will be

$$36 - 24 = 12$$

Do that with all numbers up to 100 and plot them:



As one can see, everything is possible. The values can be negative, positive or zero.

It would be very natural to classify the numbers accordingly:

- › If the aliquot sum is less than the number itself, the number is called a *deficient number*:
1, 2, 11, 47, 95, ...
- › If the aliquot sum is greater than the number itself, the number is called an *abundant number*:
12, 54, 72, 100, ...
- › And finally, if the aliquot sum is equal to the number itself, the number is called a *perfect number*, which is the most interesting case:
6, 28, 496, 8128, ...

Perfect Numbers

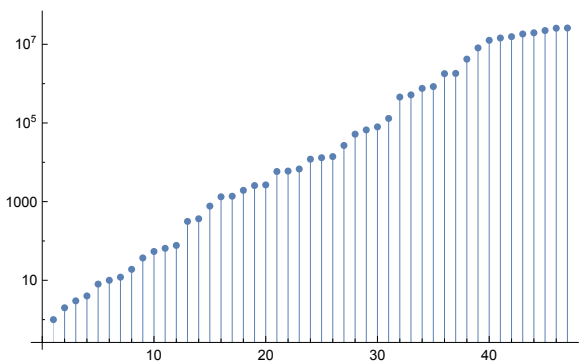
A *perfect number* is a positive integer that is equal to the sum of its positive divisors, excluding the number itself.

The first 10 perfect numbers are as follows:

n	n th perfect number
1	6
2	28
3	496
4	8128
5	33 550 336
6	8 589 869 056
7	137 438 691 328
8	2 305 843 008 139 952 128
9	2 658 455 991 569 831 744 654 692 615 953 842 176
10	191 561 942 608 236 107 294 793 378 084 303 638 130 997 321 548 169 216

As you can see, they grow incredibly fast and are very rare. In fact, the only perfect numbers in the first 100 integers are 6 and 28.

Here is the plot of the length of the first 47 even perfect numbers, with log-scaled values:



So far there are 51 known perfect numbers in total. All of them are even.

In fact, it is unknown whether there are odd perfect numbers or not.

Mersenne Numbers

Finding large primes and proving that they are prime is not easy. One approach to find large primes is to look at numbers that have a special form, for example,

$$a^n - 1$$

It's not difficult to show that in order for $a^n - 1$ to be prime, a should be equal to 2 and n should be itself prime.

A number of the form $2^n - 1$ is said to be a *Mersenne number*.

Here are the first few Mersenne numbers:

1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, ...

The n^{th} Mersenne number is denoted by M_n .

Mersenne Primes

If M_n is prime, it is called a *Mersenne prime* and n is called a *Mersenne prime exponent*.

For example, 7 is a Mersenne prime as

$$7 = 2^3 - 1$$

and 7 is a prime number.

On the contrary, 15 is a Mersenne number but is not a Mersenne prime:

$$15 = 2^4 - 1$$

If n is composite, then M_n is composite as well.

At first, it was thought that M_n is prime whenever n is prime. However, M_{11} is not prime:

$$M_{11} = 2^{11} - 1 = 2047 = 23 * 89$$

The following table shows the first 10 Mersenne prime exponents and their corresponding Mersenne primes:

n	$2^n - 1$
2	3
3	7
5	31
7	127
13	8191
17	131071
19	524287
31	2 147 483 647
61	2 305 843 009 213 693 951
89	618 970 019 642 690 137 449 562 111

Perfect Numbers and Mersenne Primes

There is a peculiar connection between perfect numbers and Mersenne primes:

➤ If p is a Mersenne prime exponent, then $2^{p-1}(2^p - 1)$ is a perfect number.

You can check. Take $p = 5$:

$$2^{5-1}(2^5 - 1) = 496$$

496 is a perfect number.

Now take $p = 13$:

$$2^{13-1} (2^{13} - 1) = 33\,550\,336$$

It is again a perfect number.

Actually, this is easy to prove.

The next statement is not as apparent as the previous one.

➤ Every even perfect number has the form $2^{p-1} (2^p - 1)$, where p is a Mersenne prime exponent.

For example, the perfect number 8128 can be written as

$$8128 = 2^{7-1} (2^7 - 1)$$

The following is the table of the first eight Mersenne primes and the corresponding perfect numbers:

p	$2^p - 1$	$2^{p-1} (2^p - 1)$
2	3	6
3	7	28
5	31	496
7	127	8128
13	8191	33 550 336
17	131 071	8 589 869 056
19	524 287	137 438 691 328
31	2 147 483 647	2 305 843 008 139 952 128

Fermat Numbers

It would be nice to have a formula that produces primes. Historically, lacking such a formula, mathematicians sought formulas that at least yield only primes.

In 1640, *Pierre de Fermat* noted that the numbers on this list are all prime:

n	0	1	2	3	4
$2^{2^n} + 1$	3	5	17	257	65 537

He conjectured that numbers of the form $2^{2^n} + 1$ are always prime.

Euler refuted Fermat's conjecture in 1732 when he showed that $2^{2^5} + 1$ is not prime. Indeed

$$2^{2^5} + 1 = 294\,967\,297 = 641 * 6\,700\,417$$

Numbers of the form $2^{2^n} + 1$ are called *Fermat numbers*. The n^{th} Fermat number is denoted by F_n .

Fermat Primes

A prime number of the form $F_n = 2^{2^n} + 1$ is a *Fermat prime*.

The only known Fermat primes are F_0, F_1, F_2, F_3 and F_4 :

n	$F_n = 2^{2^n} + 1$
0	3
1	5
2	17
3	257
4	65 537

However, little is known about Fermat numbers with large n .

In fact, it is unknown whether there are infinitely many Fermat primes or infinitely many composite Fermat numbers.

It is known that F_n is composite for $5 \leq n \leq 32$, although amongst these, complete factorizations of F_n are known only for $0 \leq n \leq 11$.

The largest Fermat number known to be composite is $F_{329\,780}$.

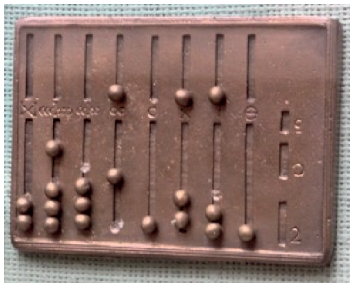
Factoring Fermat numbers is extremely difficult because of their large size.

Fermat primes are the only primes of the form $2^m + 1$.

Summary

- A *perfect number* is a positive integer that is equal to the sum of its positive divisors, excluding the number itself.
- A number of the form $2^n - 1$ is said to be a *Mersenne number*. The n^{th} Mersenne number is denoted by M_n .
- If M_n is prime, it is called a *Mersenne prime* and n is called a *Mersenne prime exponent*.
- If p is a Mersenne prime exponent, then $2^{p-1} (2^p - 1)$ is a perfect number.
- Every even perfect number has the form $2^{p-1} (2^p - 1)$, where p is a Mersenne prime exponent.
- Numbers of the form $2^{2^n} + 1$ are called *Fermat numbers*. The n^{th} Fermat number is denoted by F_n .
- A prime number of the form $F_n = 2^{2^n} + 1$ is a *Fermat prime*.

23 | Numeral Systems



A *numeral system* is a writing method for expressing numbers using digits or other symbols.

In the most common numeral system, which is the decimal system, you write numbers with combinations of 10 symbols.

But it's not the only numeral system. In fact, you can represent numbers using any number of symbols.

The same sequence of symbols can stand for different numbers in different numeral systems.

For instance, “11” represents the number 11 in the decimal numeral system, which is used in common life; the number 3 in the binary numeral system, which is used in computers; and the number 2 in the unary numeral system.

In this lesson, you will learn about the most common numeral systems, such as decimal, binary, octal and hexadecimal systems.

Numeral System

A writing method for expressing numbers is called a *numeral system*.

In the most common numeral system, you write numbers with combinations of 10 symbols:

{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

These symbols are called *digits*, and numbers that are expressed using 10 digits are called *decimals*.

With just these 10 symbols you can write any number imaginable, but it's not the only way you can represent numbers.

Actually, you can write any integer with any number of digits.

A *base* is the number of different digits or combination of digits and letters that a numeral system uses to represent numbers.

Any positive integer can be written in terms of any positive base integer expansion in a unique way.

A base b number a is usually denoted as a_b .

Decimal Numeral System

Normally, the *decimal*, or *base-10*, numeral system is used to represent numbers.

For writing numbers, the decimal system uses 10 digits:

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

For example,

2 — one digit

15 — two digits

589 — three digits

4812 — four digits

The decimal numeral system is a *positional* number representation, where the value of each digit is determined by its position in a number.

The position of every digit has a weight, which is a power of 10. In the decimal system, each position is 10 times more significant than the previous position.

Any number in the decimal numeral system can be decomposed as the sum of its digits, multiplied by the power of 10 depending on their position, starting at position 0 from the right.

For example, the number 48 967 is represented as

$$48\,967 = 7 * 10^0 + 6 * 10^1 + 9 * 10^2 + 8 * 10^3 + 4 * 10^4$$

The possible starting point of the decimal system in daily life is that there are 10 fingers on two hands and people started counting by using their fingers.

Binary Numeral System

The *binary*, or *base-2*, numeral system is the second most important system.

For writing numbers, the binary system uses two digits:

{0, 1}

The digit in the binary number system is called a *bit*.

For example, 100101 is a binary representation of a number. As you can see, it is a sequence of bits, 0s and 1s. You will later learn that this is actually the number 37 in the decimal system.

Here is a table of the first few integers in the binary system:

0	1	2	3	4	5	6	7	8	9	10
0 ₂	1 ₂	10 ₂	11 ₂	100 ₂	101 ₂	110 ₂	111 ₂	1000 ₂	1001 ₂	1010 ₂

Binary numerals are typically read digit by digit to avoid confusion with decimal numerals. For example, the binary numeral 100 is read as *one zero zero*, rather than *one hundred*, to emphasize its binary nature.

The binary numeral system is positional.

You sum each digit in the binary number system multiplied by the power of 2 depending on their position, starting at position 0 from the right.

So you can now see that the decimal value of 100 101₂ is

$$100\ 101_2 = 1 * 2^0 + 0 * 2^1 + 1 * 2^2 + 0 * 2^3 + 0 * 2^4 + 1 * 2^5 = 37$$

The advantage of the binary system is its simplicity.

A computing device has switches, each of which can be either “on” or “off.” When a switch is “on,” it represents the value of 1, and when it is “off,” it represents the value of 0.

Digital devices perform mathematical operations by turning binary switches on and off.

Decimal-to-Binary Conversion

There are several ways to convert decimal numbers to binary.

The most common is as follows:

- › Divide the number by 2.
- › Divide what’s left by 2.
- › Continue until there is nothing left (0).
- › Write down the remainder at each division stage (which is 0 or 1).
- › Once there are no more divisions, list the remainder values in reverse order.

Do that for 291:

$$291/2 = 145 * 2 + 1$$

$$145/2 = 72 * 2 + 1$$

$$72/2 = 36 * 2 + 0$$

$$36/2 = 18 * 2 + 0$$

$$18/2 = 9 * 2 + 0$$

$$9/2 = 4 * 2 + 1$$

$$4/2 = 2 * 2 + 0$$

$$2/2 = 1 * 2 + 0$$

$$1/2 = 0 * 2 + 1$$

So,

$$291 = 100100011_2$$

Binary-to-Decimal Conversion

As you know, the binary number system is positional and you sum each digit in the binary number system multiplied by the power of 2 depending on their position, starting at position 0 from the right, so

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

...

As an example, convert 1011101_2 to a decimal. You will have:

$$1011101_2 = 1 * 2^0 + 0 * 2^1 + 1 * 2^2 + 1 * 2^3 + 1 * 2^4 + 0 * 2^5 + 1 * 2^6 = 93$$

Now convert 1111111_2 to a decimal:

$$1111111_2 = 1 * 2^0 + 1 * 2^1 + 1 * 2^2 + 1 * 2^3 + 1 * 2^4 + 1 * 2^5 + 1 * 2^6 = 127$$

You got 127, which is $2^7 - 1$. Blame this simple formula for that:

$$2^0 + 2^1 + \dots + 2^{n-1} = 2^n - 1$$

Octal Numeral System

The *base-8* numeral system is also known as the *octal* numeral system.

For writing numbers, the octal system uses 8 digits:

$$\{0, 1, 2, 3, 4, 5, 6, 7\}$$

Here is a table of the first few integers in the octal system:

0	1	2	3	4	5	6	7	8	9	10
0 ₈	1 ₈	2 ₈	3 ₈	4 ₈	5 ₈	6 ₈	7 ₈	10 ₈	11 ₈	12 ₈

The octal numeral system is positional.

The position of every digit has a weight that is a power of 8. Each position in the octal system is eight times more significant than the previous position.

The numeric value of an octal number is found by multiplying each digit of the number by the value of the position in which the digit appears and then adding the products.

For example, the value of the octal number 123₈ is

$$123_8 = 3 * 8^0 + 2 * 8^1 + 1 * 8^2 = 83$$

Octal-to-Binary Conversion

The conversion between octal and binary numbers is very interesting.

First, let's consider this equivalence table of binary and octal numbers:

0 ₂	1 ₂	10 ₂	11 ₂	100 ₂	101 ₂	110 ₂	111 ₂
0 ₈	1 ₈	2 ₈	3 ₈	4 ₈	5 ₈	6 ₈	7 ₈

The conversion from octal to binary is very simple. You just replace each octal digit with its binary representation from the previous table.

For example, convert the octal number 53₈:

$$5_8 = 101_2$$

$$3_8 = 011_2$$

Therefore,

$$53_8 = 101011_2$$

Binary-to-Octal Conversion

Now convert a binary number to an octal one.

The process is the reverse of the previous algorithm:

- Group the binary digits by threes, starting from the least significant bit.
- Add leading zeros to fill out the last group of three if necessary.
- Replace each trio with the equivalent octal digit.

For example, convert the binary $11\ 001\ 110_2$:

$$110_2 = 6_8$$

$$001_2 = 1_8$$

$$011_2 = 3_8$$

Therefore,

$$11\ 001\ 110_2 = 613_8$$

The simplicity of this conversion is because both bases, 2 and 8, are powers of 2.

You group by three as $2^3 = 8$.

Hexadecimal Numeral System

The *base-16* numeral system is known as the *hexadecimal* numeral system.

For writing numbers, the hexadecimal system uses:

- › The digits 0 to 9 to represent the values zero to nine:

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

- › The letters *A* to *F* to represent the values 10 to 15:

$\{A, B, C, D, E, F\}$

This is the first system that has a base greater than 10, and that's why the digits 0–9 are not enough.

Here are the first few integers in the hexadecimal system:

0	1	2	3	4	5	6	7	8	9
0_{16}	1_{16}	2_{16}	3_{16}	4_{16}	5_{16}	6_{16}	7_{16}	8_{16}	9_{16}

10	11	12	13	14	15
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}

The hexadecimal numeral system is positional.

The position of every digit has a weight, which is a power of 16. Each position in the hexadecimal system is 16 times more significant than the previous position.

The numeric value of a hexadecimal number is determined by multiplying each value of the digit of the number by the value of the position in which the digit appears and then adding the products.

For example, the value of the hexadecimal number $A5C6_{16}$ is:

$$A5C6_{16} = 6 * 16^0 + 12 * 16^1 + 5 * 16^2 + 10 * 16^3 = 42\,438$$

Computer system designers and programmers widely use hexadecimal numerals.

Hexadecimal-to-Binary Conversion

The conversion between hexadecimal and binary numbers is very much like the conversion between octal and binary.

Let's begin with the conversion from hexadecimal to binary.

First, let's consider these equivalence tables of binary and hexadecimal numbers:

0_2	1_2	10_2	11_2	100_2	101_2	110_2	111_2	1000_2	1001_2
0_{16}	1_{16}	2_{16}	3_{16}	4_{16}	5_{16}	6_{16}	7_{16}	8_{16}	9_{16}

1010_2	1011_2	1100_2	1101_2	1110_2	1111_2
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}

Just replace each hexadecimal digit by its binary representation from the previous table.

For example, convert the hexadecimal number $CD8_{16}$:

$$C_{16} = 1100_2$$

$$D_{16} = 1101_2$$

$$8_{16} = 1000_2$$

Therefore,

$$CD8_{16} = 110\,011\,011\,000_2$$

Binary-to-Hexadecimal Conversion

Now convert a binary number to a hexadecimal one.

- › Group the binary digits by fours, starting from the least significant bit and proceeding to the left and to the right.
- › Add leading zeros to fill out the last group of four if necessary.
- › Replace each four with the equivalent hexadecimal digit.

For example, convert the binary $1\,010\,111\,100_2$:

$$1100_2 = C_{16}$$

$$1011_2 = B_{16}$$

$$0010_2 = 2_{16}$$

Therefore,

$$1\,010\,111\,100_2 = CB2_{16}$$

This is easy, because both bases, 2 and 16, are powers of 2.

You group by four as $2^4 = 16$.

Summary

- A writing method for expressing numbers is called a *numeral system*.
- A *base* is the number of different digits or combination of digits and letters that a numeral system uses to represent numbers.
- Any positive integer can be written in terms of any positive base integer expansion in a unique way.
- The *decimal*, or *base-10*, numeral system uses the digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ to represent numbers.
- The *binary*, or *base-2*, numeral system uses the digits $\{0, 1\}$ to represent numbers.
- The *octal*, or *base-8*, numeral system uses the digits $\{0, 1, 2, 3, 4, 5, 6, 7\}$ to represent numbers.
- The *hexadecimal*, or *base-16*, numeral system uses the symbols $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$ to represent numbers.
- These numeral systems are *positional* number representations, where the value of each digit is determined by its position in a number.

Part 7 Exercises

7.1 What does proving the Riemann hypothesis accomplish?

Solution

The Riemann hypothesis, if true, will shed light on the distribution of prime numbers.

7.2 Use the definition of perfect numbers to determine which of the following numbers are perfect:

15, 28, 160, 496, 824, 1048, 8128

Solution

A perfect number is a positive integer that is equal to the sum of its positive divisors, excluding the number itself.

You can write a function in Wolfram Language to test if the number is perfect or not using the definition. Use the function `DivisorSigma` in Wolfram Language:

```
In[⌘]:= perfectQ [ n_ ] := ( DivisorSigma [ 1, n ] - n ) == n
```

Test it on the list of given numbers:

15, 28, 160, 496, 824, 1048, 8128

```
In[⌘]:= perfectQ [ 15 ]
```

```
Out[⌘]= False
```

```
In[⌘]:= perfectQ [ 28 ]
```

```
Out[⌘]= True
```

```
In[⌘]:= perfectQ [ 160 ]
```

```
Out[⌘]= False
```

```
In[⌘]:= perfectQ [ 496 ]
```

```
Out[⌘]= True
```

```
In[⌘]:= perfectQ [ 824 ]
```

```
Out[⌘]= False
```

```
In[⌘]:= perfectQ [ 1048 ]
```

```
Out[⌘]= False
```

```
In[ ]:= perfectQ [ 8128 ]
```

```
Out[ ]:= True
```

So the perfect numbers are 28, 496 and 8128.

There already exists a function PerfectNumberQ in Wolfram Language to check if a number is perfect or not. For example,

```
In[ ]:= PerfectNumberQ [ 15 ]
```

```
Out[ ]:= False
```

```
In[ ]:= PerfectNumberQ [ 28 ]
```

```
Out[ ]:= True
```

7.3 Write the fifth perfect number in the form $2^{p-1} (2^p - 1)$, where p is a Mersenne prime exponent.

Solution

You can find out the fifth perfect number by using the function PerfectNumber in Wolfram Language:

```
In[ ]:= PerfectNumber [ 5 ]
```

```
Out[ ]:= 33550336
```

To find the highest power of 2 that divides 33550336, use the function IntegerExponent in Wolfram Language:

```
In[ ]:= IntegerExponent [ 33550336, 2 ]
```

```
Out[ ]:= 12
```

Hence, $p - 1 = 12 \Rightarrow p = 13$:

```
In[ ]:= p = 13;
```

```
In[ ]:= 2 ^ ( p - 1 ) ( 2 ^ p - 1 )
```

```
Out[ ]:= 33550336
```

Use the function MersennePrimeExponentQ in Wolfram Language to see that 13 is indeed a Mersenne prime exponent:

```
In[ ]:= MersennePrimeExponentQ [ 13 ]
```

```
Out[ ]:= True
```

So $33550336 = 2^{12} (2^{13} - 1)$.

7.4 What is the biggest binary number you can write in 7 bits?

Solution

The decimal value of a binary number $a_1 a_2 a_3 a_4 a_5 a_6 a_7$ in 7 bits is

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 = a_7 * 2^0 + a_6 * 2^1 + a_5 * 2^2 + a_4 * 2^3 + a_3 * 2^4 + a_2 * 2^5 + a_1 * 2^6$$

where all $a_1, a_2, \dots, a_7$ are 0 or 1. Consequently, it has the largest value when all a_i are 1.

So the biggest binary number you can write in 7 bits is 1111111_2 .

Use the function `FromDigits` in Wolfram Language to get its decimal value:

```
In[*]:= FromDigits [ { 1, 1, 1, 1, 1, 1 }, 2 ]
```

```
Out[*]= 127
```

7.5 Convert the binary number $11\,111\,101\,001_2$ to its hexadecimal equivalent.

Solution

Convert the binary number $11\,111\,101\,001_2$ to a hexadecimal number.

Group the binary digits by fours, starting from the least significant bit and proceeding to the left and to the right, adding leading zeros to fill out the last group of four if necessary:

$\{0, 1, 1, 1\} \{1, 1, 1, 0\} \{1, 0, 0, 1\}$

Replace each four with the equivalent hexadecimal digit. First, use the function `FromDigits` in Wolfram Language to see what decimal number it is:

```
In[*]:= FromDigits [ { 0, 1, 1, 1 }, 2 ]
```

```
Out[*]= 7
```

Then use the function `BaseForm` in Wolfram Language to get its hexadecimal representation:

```
In[*]:= BaseForm [ 7, 16 ]
```

```
Out[*]= 716
```

Do the same thing with the other two groups:

```
In[*]:= BaseForm [ FromDigits [ { 1, 1, 1, 0 }, 2 ], 16 ]
```

```
Out[*]= E16
```

```
In[*]:= BaseForm [ FromDigits [ { 1, 0, 0, 1 }, 2 ], 16 ]
```

```
Out[*]= 916
```

So the hexadecimal representation of $11\,111\,101\,001_2$ is $7\,E9_{16}$.



Wolfram eTextbook Series

- › **Introduction to Calculus:
A Computational Approach**
John Clark and Devendra Kapadia
- › **Signals, Systems, and Signal Processing:
A Computational Approach**
Mariusz Jankowski
- › **Essentials of Complex Analysis:
A Computational Approach**
Marco Saragnese
- › **Laplace Transforms in Theory and Practice:
A Computational Approach**
Hrachya Khachatryan
- › **Navigating Probability:
A Computational Approach**
Marc Vicuna
- › **Quantum Computing by Model and Simulation:
A Computational Approach**
Mohammad Bahrami
- › **Special Functions from Theory to Application:
A Computational Approach**
Tigran Ishkhanyan
- › **Exploring Partial Differential Equations:
A Computational Approach**
Aram Manaselyan

By Stephen Wolfram

- › **What Is ChatGPT Doing ...
and Why Does It Work?**
- › **A New Kind of Science**
- › **An Elementary Introduction
to the Wolfram Language**
- › **Metamathematics: Foundations
& Physicalization**
- › **The Second Law: Resolving the Mystery of the
Second Law of Thermodynamics**
- › **A Project to Find the Fundamental
Theory of Physics**
- › **Combinators: A Centennial View**
- › **Idea Makers: Personal Perspectives
on the Lives & Ideas of Some Notable People**

By Other Authors

- › **Query: Getting Information from Data
with the Wolfram Language**
Seth J. Chandler
- › **Introduction to Machine Learning**
Etienne Bernard
- › **A Field Theory of Games: Introduction to
Decision Process Engineering, Volume 1**
Gerald H. Thomas
- › **A Field Theory of Games: Introduction to
Decision Process Engineering, Volume 2**
Gerald H. Thomas
- › **A Numerical Approach to Real Algebraic
Curves with the Wolfram Language**
Barry H. Dayton
- › **The Math(s) Fix:
An Education Blueprint for the AI Age**
Conrad Wolfram
- › **Hands-on Start to Wolfram|Alpha
Notebook Edition**
Cliff Hastings and Kelvin Mischo
- › **Hands-on Start to Wolfram Mathematica
and Programming with the Wolfram Language**
Cliff Hastings, Kelvin Mischo and Michael Morrison
- › **Introduction to Statistics
with the Wolfram Language**
Juan H. Klopfer

