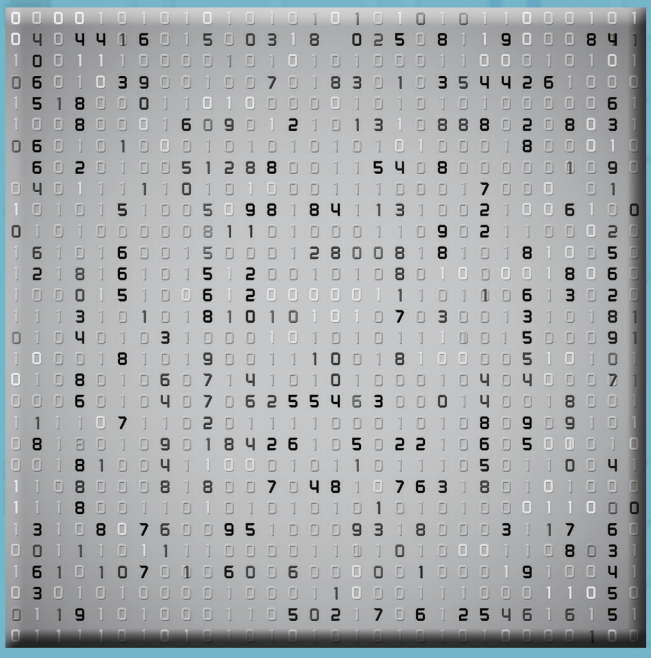
TEXTBOOKS in MATHEMATICS

# ELEMENTARY NUMBER THEORY



James S. Kraft
Lawrence C. Washington

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

TEXTBOOKS in MATHEMATICS

# ELEMENTARY NUMBER THEORY

James S. Kraft

Gilman School
Baltimore, Maryland, USA

Lawrence C. Washington

University of Maryland
College Park, Maryland, USA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group an **informa** business
A CHAPMAN & HALL BOOK

# TEXTBOOKS in MATHEMATICS

Series Editors: Al Boggess and Ken Rosen

PUBLISHED TITLES

ABSTRACT ALGEBRA: AN INQUIRY-BASED APPROACH
Jonathan K. Hodge, Steven Schlicker, and Ted Sundstrom

ABSTRACT ALGEBRA: AN INTERACTIVE APPROACH
William Paulsen

ADVANCED CALCULUS: THEORY AND PRACTICE
John Srdjan Petrovic

ADVANCED LINEAR ALGEBRA
Nicholas Loehr

ANALYSIS WITH ULTRASMALL NUMBERS
Karel Hrbacek, Olivier Lessmann, and Richard O'Donovan

APPLYING ANALYTICS: A PRACTICAL APPROACH
Evan S. Levine

COMPUTATIONS OF IMPROPER REIMANN INTEGRALS
Ioannis Roussos

CONVEX ANALYSIS
Steven G. Krantz

COUNTEREXAMPLES: FROM ELEMENTARY CALCULUS TO THE BEGINNINGS OF ANALYSIS
Andrei Bourchtein and Ludmila Bourchtein

DIFFERENTIAL EQUATIONS: THEORY, TECHNIQUE, AND PRACTICE, SECOND EDITION
Steven G. Krantz

DIFFERENTIAL EQUATIONS WITH MATLAB®: EXPLORATION, APPLICATIONS, AND THEORY
Mark A. McKibben and Micah D. Webster

ELEMENTARY NUMBER THEORY
James S. Kraft and Lawrence C. Washington

ELEMENTS OF ADVANCED MATHEMATICS, THIRD EDITION
Steven G. Krantz

EXPLORING LINEAR ALGEBRA: LABS AND PROJECTS WITH MATHEMATICA®
Crista Arangala

PUBLISHED TITLES CONTINUED

AN INTRODUCTION TO NUMBER THEORY WITH CRYPTOGRAPHY
James Kraft and Larry Washington

AN INTRODUCTION TO PARTIAL DIFFERENTIAL EQUATIONS WITH MATLAB®, SECOND EDITION
Mathew Coleman

INTRODUCTION TO THE CALCULUS OF VARIATIONS AND CONTROL WITH MODERN APPLICATIONS
John T. Burns

LINEAR ALGEBRA, GEOMETRY AND TRANSFORMATION
Bruce Solomon

THE MATHEMATICS OF GAMES: AN INTRODUCTION TO PROBABILITY
David G. Taylor

QUADRACTIC IRRATIONALS: AN INTRODUCTION TO CLASSICAL NUMBER THEORY
Franz Holter-Koch

REAL ANALYSIS AND FOUNDATIONS, THIRD EDITION
Steven G. Krantz

RISK ANALYSIS IN ENGINEERING AND ECONOMICS, SECOND EDITION
Bilal M. Ayyub

RISK MANAGEMENT AND SIMULATION
Aparna Gupta

TRANSFORMATIONAL PLANE GEOMETRY
Ronald N. Umble and Zhigang Han

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742


Version Date: 20141007

International Standard Book Number-13: 978-1-4987-0269-0 (eBook - PDF)

*To Kristi, Danny, and Aaron,*
*and to Miriam Kraft and the memory of Norman Kraft*

*To Susan and Patrick,*
*and to Ida H. Washington and Lawrence M. Washington*

# *Contents*

# *Preface*

Number theory has a rich history. For many years, it was one of the purest areas of pure mathematics, studied because of the intellectual fascination with properties of integers. More recently, it has been an area that also has important applications to subjects such as cryptography. The goal of this book is to present both sides of the picture, giving a selection of topics that we find exciting.

The main thing to remember is number theory is supposed to be fun. We hope you enjoy the book.

The book is designed for use in a basic undergraduate course in number theory, but the book has also been used in a course for advanced high school students and could work well for independent study.

How does this book differ from our book *An Introduction to Number Theory with Cryptography* (also published by CRC)? Since number theory is often the first theoretical course a student takes, we have added an introductory section on how to do proofs, including a brief discussion of what lemmas, propositions, theorems, and corollaries are. We have added a few more cryptographic topics such as Hill ciphers and transposition ciphers. To fulfill our goal of a more basic course, we have removed topics that are often not covered in a one-semester course: geometry of numbers, algebraic integers, analytic techniques, and some of the more advanced material on primality and factorization. The chapter on continued fractions contains the highlights, in particular the solution of Pell's equation, which is too beautiful to omit, but leaves out the rather technical proofs. We have also adjusted the exercises to fit with the present version of the book.

**The Chapters.** The flowchart (following this preface) gives the dependencies of the chapters. The section number 7.5 that occurs with an arrow means that only that section from Chapter 7 is needed for Chapter 9 at the end of the arrow.

The core material is Chapters 1, 2, 3, 5, 6, and 8, plus Section 10.1.

These should be covered if at all possible. At this point, there are several possibilities. It is highly recommended that some sections of Chapters 4, 7, and 9 be covered. These present some of the exciting applications of number theory to various problems, especially in cryptography. If time permits, additional topics from Chapters 11 through 14 can be covered. These chapters are mostly independent of one another, so the choices depend on the interests of the audience.

We have tried to keep the prerequisites to a minimum. Besides the introduction to proofs in Chapter 1, there is Appendix A, which treats some topics such as induction, the binomial theorem, and $2 \times 2$ matrices (for use in Hill ciphers). Our experience is that many students have seen these topics but that a review is worthwhile. The appendix also treats Fibonacci numbers, since they occur as examples in a few places throughout the book and are interesting in their own right.

**Notes to the reader.** At the end of each chapter, we have a short list of Chapter Highlights. We were tempted to use the label "If you don't know these, no one will believe you read the chapter." In other words, when you finish a chapter, make sure you thoroughly know the highlights. (Of course, there is more that is worth knowing.) At the end of several sections, there are problems labeled "CHECK YOUR UNDERSTANDING." These are problems that check whether you have learned some basic ideas. The solutions to these are given at the ends of the chapters. You should not leave a topic until you can do these problems easily.

**Problems.** At the end of every chapter, there are problems to solve. The *Exercises* are intended to give practice with the concepts and sometimes to introduce interesting ideas related to the chapter's topics. Computations have had a great influence on number theory, and the *Computer Explorations* introduce this type of experimentation. Sometimes they ask for specific data, sometimes they are more open-ended. But they represent the type of exploration that number theorists often do in their research.

Appendix B contains answers or hints for the odd-numbered problems. For the problems where the answer is a number, the answer is given. When the exercise asks for a proof, usually a sketch or a key step is given.

**Computers.** Many students are familiar with computers these days and many have access to software packages such as Mathematica®,

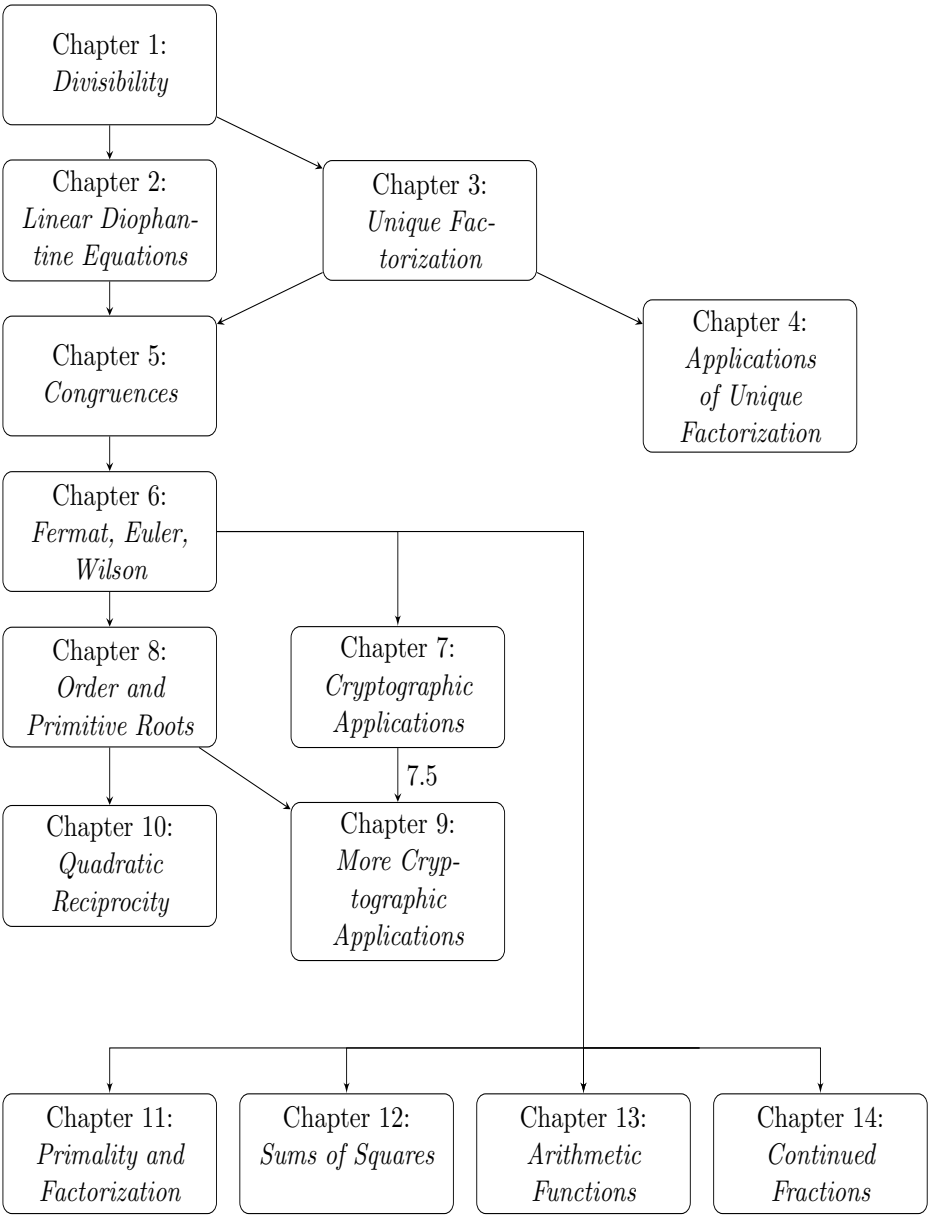
Maple®, MATLAB®, Sage, or Pari that perform number theoretical calculations with ease. Some of the exercises (the ones that use numbers of five or more digits) are intended to be used in conjunction with a computer. Many can probably be done with an advanced calculator. The Computer Explorations definitely are designed for students with computer skills.

**Acknowledgments.** Jim Kraft thanks the Gilman School for its generous support during the writing of this book. He also thanks his students Rishi Bedi, John Chirikjian, Anthony Kim, and John Lee, whose comments helped make this a better book. Many thanks are also due to Manjit Bhatia, who made many very useful suggestions. We both thank our many students over the years who have taught us while we have taught them. This book would not have been possible without them.

We welcome comments, corrections, and suggestions. Corrections and related matter will be listed on the website for the book (www.math.umd.edu/∼lcw/elementarynumbertheory.html).

*James S. Kraft*
*Gilman School*
*jkraft@gilman.edu*

*Lawrence C. Washington*
*University of Maryland*
*lcw@math.umd.edu*


Chapter 1: *Divisibility*
Chapter 2: *Linear Diophantine Equations*
Chapter 3: *Unique Factorization*
Chapter 4: *Applications of Unique Factorization*
Chapter 5: *Congruences*
Chapter 6: *Fermat, Euler, Wilson*
Chapter 7: *Cryptographic Applications*
Chapter 8: *Order and Primitive Roots*
7.5
Chapter 9: *More Cryptographic Applications*
Chapter 10: *Quadratic Reciprocity*
Chapter 11: *Primality and Factorization*
Chapter 12: *Sums of Squares*
Chapter 13: *Arithmetic Functions*
Chapter 14: *Continued Fractions*

# Introduction

At Columbia University there is a Babylonian clay tablet called Plimpton 322 that is more than 3800 years old and not much larger than a cell phone. Written in cuneiform script with 4 columns and 15 rows, it contains numbers written in base 60 (just as base 10 is standard today, base 60 was standard in Babylon). Each row gives a Pythagorean triple, that is, three whole numbers $x, y, z$ satisfying

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

(for example, $3^2 + 4^2 = 5^2$ and $12709^2 + 13500^2 = 18541^2$ are triples from the tablet). This is one of the earliest examples where integers are studied for their interesting properties, not just for counting objects.

Throughout history, there has been a fascination with whole numbers. For example, the Pythagorean school (ca. 500 BCE) believed strongly that every quantity could be expressed in terms of integers or ratios of integers, and they successfully applied the idea to the theory of musical scales. However, this overriding belief received a sharp setback when one of the Pythagoreans, possibly Hippasus, proved that $\sqrt{2}$ is irrational. There is a story, which may be apocryphal, that he discovered this at sea and was promptly thrown overboard by his fellow Pythagoreans. Despite their attempt at suppressing the truth, the news of this discovery soon got out. Nevertheless, even though irrational numbers exist and are plentiful, properties of integers are still important.

Approximately 200 years after Pythagoras, Euclid's *Elements*, perhaps the most important mathematics book in history, was published. Although most people now think of the *Elements* as a book concerning geometry, a large portion of it is devoted to the theory of numbers. Euclid proves that there are infinitely many primes, demonstrates fundamental properties concerning divisibility of integers, and derives a formula that yields *all* possible Pythagorean triples, as well as many

other seminal results. We will see and prove these results in the first four chapters of this book.

Number theory is a rich subject, with many aspects that are inextricably intertwined but which also retain their individual characters. In this introduction, we give a brief discussion of some of the ideas and some of the history of number theory as seen through the themes of Diophantine equations, modular arithmetic, the distribution of primes, and cryptography.

# 1 Diophantine Equations

Diophantus lived in Alexandria, Egypt, about 1800 years ago. His book *Arithmetica* gives methods for solving various algebraic equations and had a great influence on the development of algebra and number theory for many years. The part of number theory called **Diophantine equations**, which studies integer (and sometimes rational) solutions of equations, is named in his honor. However, the history of this subject goes back much before him. The Plimpton tablet shows that the Babylonians studied integer solutions of equations. Moreover, the Indian mathematician Baudhāyana ($\approx$ 800 BCE) looked at the equation $x^2 - 2y^2 = 1$ and found the solutions $(x, y) = (17, 12)$ and $(577, 408)$. The latter gives the approximation $577/408 \approx 1.4142157$ for $\sqrt{2}$, which is the diagonal of the unit square. This was a remarkable achievement, considering that, at the time, a standardized system of algebraic notation did not yet exist.

The equation

$$x^2 - ny^2 = 1,$$

where $n$ is a positive integer not a square, was studied by Brahmagupta (598–668) and later mathematicians. In 1768, Joseph-Louis Lagrange (1736–1813) presented the first published proof that this equation always has a nontrivial solution (that is, with $y \neq 0$). Leonhard Euler (1707–1783) mistakenly attributed some work on this problem to the English mathematician John Pell (1611–1685), and ever since it has been known as **Pell's equation**, but there is little evidence that Pell did any work on it. In Chapter 14, we show how to solve Pell's equation.

Perhaps $x^2+y^2=z^2$, the equation for Pythagorean triples, is the most well-known Diophantine equation. Since sums of two nonzero squares can be a square, people began to wonder if this could be generalized. For example, Abu Mohammed Al-Khodjandi, who lived in the late 900s, claimed to have a proof that a sum of nonzero cubes cannot be a cube (that is, the equation $x^3+y^3=z^3$ has no nonzero solutions). Unfortunately, our only knowledge of this comes from another manuscript, which mentions that Al-Khodjandi's proof was defective, but gives no evidence to support this claim. The real excitement began when the great French mathematician Pierre de Fermat (1601–1665) penned a note in the margin of his copy of Diophantus's *Arithmetica* saying that it is impossible to solve $x^n+y^n=z^n$ in positive integers when $n\geq 3$ and that he had found a truly marvelous proof that the margin was too small to contain. After Fermat's son, Samuel Fermat, published an edition of Diophantus's book that included his father's comments, the claim became known as **Fermat's Last Theorem**. Today, it is believed that he actually had proofs only in the cases $n=4$ (the only surviving proof by Fermat of any of his results) and possibly $n=3$. But the statement acquired a life of its own and led to many developments in mathematics. Euler is usually credited with the first complete proof that Fermat's Last Theorem (abbreviated as FLT) is true for $n=3$. Progress proceeded exponent by exponent, with Adrien-Marie Legendre (1752–1833) and Johann Peter Gustav Lejeune Dirichlet (1805–1859) each doing the case $n=5$ around 1825 and Gabriel Lamé (1795–1870) treating $n=7$ in 1839. Important general results were obtained by Sophie Germain (1776–1831), who showed that if $p<100$ is prime and $xyz$ is not a multiple of $p$, then $x^p+y^p\neq z^p$.

The scene changed dramatically around 1850, when Ernst Eduard Kummer (1810–1893) developed his theory of *ideal numbers*, which are now known as *ideals* in ring theory. He used them to give general criteria that allowed him to prove FLT for all exponents up to 100, and many beyond that. His approach was a major step in the development of both algebraic number theory and abstract algebra, and it dominated the research on FLT until the 1980s. In the 1980s, new methods, based on work by Taniyama, Shimura, Weil, Serre, Langlands, Tunnell, Mazur, Frey, Ribet, and others, were brought to the problem, resulting in the proof of Fermat's Last Theorem by Andrew Wiles (with the help of Richard Taylor) in 1994. The techniques developed during this pe-

riod have opened up new areas of research and have also proved useful in solving many classical mathematical problems.

# 2 Modular Arithmetic

Suppose you divide $1234^{25147}$ by 25147. What is the remainder? Why should you care? A theorem of Fermat tells us that the remainder is 1234. Moreover, as we'll see, results of this type are surprisingly vital in cryptographic applications (see Chapters 7 and 9).

Questions about divisibility and remainders form the basis of modular arithmetic, which we introduce in Chapter 5. This is a very old topic, and its development is implicit in the work of several early mathematicians. For example, the Chinese Remainder Theorem is a fundamental and essential result in modular arithmetic and was discussed by Sun Tzu around 1600 years ago.

Although early mathematicians discovered number theoretical results, the true beginnings of modern number theory began with the work of Fermat, whose contributions were both numerous and profound. We will discuss several of them in this book. For example, he proved that if $a$ is a whole number and $p$ is a prime then $a^p - a$ is always a multiple of $p$. Results such as this are best understood in terms of modular arithmetic.

Euler and Karl Friedrich Gauss (1777–1855) greatly extended the work done by Fermat. Gauss's book *Disquisitiones Arithmeticae*, which was published in 1801, gives a treatment of modular arithmetic that is very close to the present-day version. Many of the original ideas in this book laid the groundwork for subsequent research in number theory.

One of Gauss's crowning achievements was the proof of Quadratic Reciprocity (see Chapter 10). Early progress toward this fundamental result, which gives a subtle relation between squares of integers and prime numbers, had been made by Euler and by Legendre. Efforts to generalize Quadratic Reciprocity to higher powers led to the development of algebraic number theory in the 1800s by Kummer, Richard Dedekind (1831–1916), David Hilbert (1862–1943), and others. In the first half of the 1900s, this culminated in the development of *class field theory* by

many mathematicians, including Hilbert, Weber, Takagi, and Artin. In the second half of the 1900s up to the present, the *Langlands Program*, which can be directly traced back to Quadratic Reciprocity, has been a driving force behind much number-theoretic research. Aspects of it played a crucial role in Wiles's proof of Fermat's Last Theorem in 1994.

# 3 The Distribution of Primes

> *There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that, despite their simple definitions and role as the building blocks of the natural numbers, the prime numbers belong to the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision.* – Don Zagier

Euclid proved that there are infinitely many primes, but we can ask for more precise information. Let $\pi(x)$ be the number of primes less than or equal to $x$. Legendre and Gauss used experimental data to conjecture that

$$\frac{\pi(x)}{x/\ln x} \approx 1,$$

and this approximation gets closer to equality as $x$ gets larger. For example,

$$\frac{\pi(10^4)}{10^4/\ln 10^4} = 1.132, \quad \text{and} \quad \frac{\pi(10^{10})}{10^{10}/\ln 10^{10}} = 1.048.$$

In 1852, Pafnuty Chebyshev (1821–1894) showed that the conjecture of Legendre and Gauss is at least approximately true by showing that,

for sufficiently large values of $x$,

$$0.921 \leq \frac{\pi(x)}{x/\ln x} \leq 1.106.$$

A few years later, Bernhard Riemann (1826–1866) introduced techniques from the theory of complex variables and showed how they could lead to more precise estimates for $\pi(x)$. Finally, in 1896, using Riemann's ideas, Jacques Hadamard (1865–1963) and Charles de la Vallée-Poussin (1866–1962) independently proved that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1,$$

a result known as the **Prime Number Theorem**.

If we look at the list of *all* integers, we know that within that list there is an infinite number of primes. Suppose we look at a list like this:

$$1, 6, 11, 16, 21, 26, \ldots,$$

or like this:

$$3, 13, 23, 33, 43, 53, \ldots,$$

or like this:

$$1, 101, 201, 301, 401, \ldots.$$

Does each of the three lists contain an infinite number of primes as well? The answer is yes, and we owe the proof of this remarkable fact to Dirichlet. In 1837, he proved that every arithmetic progression of the form $a, a+b, a+2b, a+3b, \ldots$ contains infinitely many primes if $a$ and $b$ are positive integers with no common factor greater than 1. We will not prove this result in this book.

There are many other questions that can be asked about primes. One of the most famous is **Goldbach's Conjecture**. In 1742, Christian Goldbach (1690–1764) conjectured that every even integer greater than 2 is a sum of two primes (for example, $100 = 83 + 17$). Much progress has been made on this conjecture over the last century. In 1937, I. M. Vinogradov (1891–1983) proved that every sufficiently large odd integer is a sum of three primes, and in 1966, Jingrun Chen (1933–1996) proved that every sufficiently large even integer is either a sum of two primes or the sum of a prime and a number that is the product of two primes (for example, $100 = 23 + 7 \cdot 11$). In 2013, Helfgott completed Vinogradov's

work by showing that every odd integer greater than or equal to 7 is a sum of three primes. These results require very delicate analytic techniques. Work on Goldbach's Conjecture and related questions remains a very active area of modern research in number theory.

# 4 Cryptography

For centuries, people have sent secret messages by various means. But in the 1970s, there was a dramatic change when Fermat's theorem and Euler's theorem (a generalization of Fermat's theorem), along with other results in modular arithmetic, became fundamental ingredients in many cryptographic systems. In fact, whenever you buy something over the Internet, it is likely that you are using Euler's theorem.

In 1976, Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography and also gave a key establishment protocol (see Chapter 9) that uses large primes. A year later, Ron Rivest, Adi Shamir, and Len Adleman introduced the RSA cryptosystem (see Chapter 7), an implementation of the public key concept. It uses large prime numbers and its security is closely tied to the difficulty of factoring large integers.

Topics such as factorization and finding primes became very popular, and soon there were several major advances in these subjects. For example, in the mid-1970s, factorization of 40-digit numbers was the limit of technology. As of 2014, the limit was 230 digits. Some factorization methods will be discussed in Chapter 11.

Cryptography brought about a fundamental change in how number theory is viewed. For many years, number theory was regarded as one of the purest areas of mathematics, with little or no application to real-world problems. In 1940, the famous British number theorist G. H. Hardy (1877–1947) declared, "No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years" (*A Mathematician's Apology*, section 28). Clearly this statement is no longer true.

Although the basic purpose of cryptography is to protect communications, its ideas have inspired many related applications. In Chapter 9, we'll explain how to sign digital documents, along with more light-

hearted topics such as playing mental poker and flipping coins over the telephone.

# Chapter 1

# Divisibility

## 1.1 What Is a Proof?

If you are studying chemistry and read that the boiling point of salt water changes as the concentration of salt changes, you might try an experiment to see if this is really true. How do you proceed? You use a thermometer to measure the water temperature and you calculate the concentration of the salt in the water. After performing this experiment several times, you conclude that the statement is, in fact, correct.

If you are studying mathematics and read that the sum of two even integers is always an even integer, you might also try an experiment to see if this is really true. How do you proceed in this case? You can write down two lists of even numbers, take a number from each list, and add them up. If you do this correctly, can you conclude that the sum of two even numbers is always even? If you suspect that this does not completely justify the statement, you're on to something. This is not how mathematics works. Although mathematicians can do experiments (often with computers) to try to decide if something seems to be true, they do not use experiments to conclude that things are true. Instead, mathematicians *prove* things. What is a proof? Why do we prove things? How is a proof different from experimental verification? We'll answer these questions in the next few paragraphs.

Simply put, we prove things to convince others (and ourselves) that a statement we're asserting to be true really is true. We start off with an initial assumption or hypothesis and use a chain of logical deductions

to arrive at what we want to prove. The validity of our proof rests on our correct use of logic, not on the consistency of experimental data. Let's see how this works as we prove that the sum of two even integers is an even integer.

To begin, coming up with several examples

$$4 + 12 = 16, \quad 36 + 20 = 56, \quad 128 + 416 = 544$$

does not constitute a proof because it's impossible to write down the sum of every pair of even integers. Even if you calculated the sum of 1000 different pairs of even integers, it's possible that the next pair you'd try would contradict what you believe to be true. Instead, you need to come up with some general method that handles all possibilities. In order to do this, you need to begin with a clear and precise definition of even integers. (You can't prove something about even integers until you have defined them.) This is the motivation behind the following definition.

**Definition 1.1.** *An integer $n$ is an* **even** *integer if $n$ is a multiple of 2. In other words, there is an integer $k$ with $n = 2k$.*

For example, 26 is even because $26 = 2 \cdot 13$, and 100 is even because $100 = 2 \cdot 50$.

Now that we've defined even, let's take another look at what we want to prove, namely that the sum of two even integers is also an even integer. When trying to prove something, it's essential to recognize what your assumptions are and be absolutely certain what it is you want to prove. In this case, we're assuming that we have two even integers and we want to prove that their sum is even. Sometimes it helps to link our assumption with what we want to prove in an "if, then" sentence called a conditional statement. Here's what a conditional statement looks like in this example.

**If** you have two even integers, **then** their sum is even.

The underlined clause that follows the "if" is called the **hypothesis**, and the underlined clause that follows the "then" is called the **conclusion**. The hypothesis is what you assume; the conclusion is what you want to prove.

Now, let's begin the proof. We start off with our even integers: we'll

call them $m$ and $n$. (Giving the numbers names such as $m$ and $n$ makes it much easier to work with them. Don't skip this step.) We want to prove that $m + n$ is also even. The best way to begin is to make use of the hypotheses. Since both $m$ and $n$ are even, we'll write down the only thing we know about even integers, namely their definition. Since $m$ is even, we know that $m = 2k_1$ for some integer $k_1$, and since $n$ is even, $n = 2k_2$ for some integer $k_2$. What do we do now? Since we want to prove something about the sum of $m$ and $n$, we'll add $m$ to $n$ and see what happens. We see that $m + n = 2k_1 + 2k_2$. Our goal is to show that $m + n$ is even, which means (by the definition) that we want to express $m + n$ as a multiple of 2. If fact, this is what we've done:

$$m + n = 2k_1 + 2k_2 = 2(k_1 + k_2).$$

This shows that $m + n$ is twice the integer $k_1 + k_2$, which tells us that $m + n$ is even.

This proof is in many ways a model for how you should think of any proof you try to do. First, make sure you have an unambiguous definition of all your terms. Next, write what you want to prove as a conditional statement, making sure you understand the hypothesis and conclusion. Then, translate the hypothesis into a mathematical statement. Finally, develop a strategy that will allow you to go from the hypothesis to the conclusion. Although many of the proofs in this book are more complex than the present example, the method that we just outlined will always apply.

When you finish reading a proof (yes, you should always try to read the proofs; that's how to learn how concepts fit together and how to do proofs), it is very good practice to look back and see where the hypotheses were used. In our example, the hypothesis was that $m$ and $n$ are even. How was this used? It allowed us to write $m = 2k_1$ and $n = 2k_2$, which is what got us started. If a proof is not using one of the hypotheses, it is likely that something is wrong (or that the hypothesis is not needed).

No discussion of how to prove things is complete without saying how to disprove things. Suppose you see the statement that all integers are less than 100. That's absurd, you say. For example, 123 is an integer and it is not less than 100. You have disproved the statement. Whenever you want to disprove a statement, all you need to do is find a counterexam-

ple. One counterexample suffices. This is in complete contrast to most proofs, where an example is not the same as a proof.[1]

For practice, let's try to prove or disprove the following statements. For each you should first try a few examples ("experiments") to get a feel for what is being said. If you find a counterexample, you are done, since you have disproved the statement. If your examples seem to indicate that the statement is true, try to give a proof. We'll give answers after the statements, but you should try each before looking at the solutions.

**Prove or Disprove:**

1. The sum of two odd integers is always even. (*Note:* First, you need a definition of *odd*; we say that $n$ is odd if there is an integer $k$ such that $n = 2k + 1$.)
2. The product of two even integers is always a multiple of 4.
3. Every multiple of 3 is odd.
4. Every multiple of 6 is even.
5. Every odd number larger than 1 is a prime number.

**Solutions:**

1. Some examples show that this seems to be true: $5 + 9 = 14$, $21 + 111 = 132$, $1 + 3 = 4$. Now let's prove it. First, write the statement as a conditional statement: If $m$ and $n$ are odd integers, then $m + n$ is even. The hypothesis is that $m$ and $n$ are odd. To write this mathematically, use the definition: $m = 2k_1 + 1$ for some integer $k_1$, and $n = 2k_2 + 1$ for some integer $k_2$. Our goal is to say something about the sum $m+n$, so we compute

$$m + n = (2k_1 + 1) + (2k_2 + 1) = 2k_1 + 2k_2 + 2.$$

What do we do now? Look at the conclusion. It says that $m+n$

[1] An exception: If the statement you want to prove is an existence statement, then an example might suffice. For example, if the statement says that there exists a cube that is two more than a square, then the example $3^3 = 5^2 + 2$ shows that the statement is true.

is even, which means that we need to be able to express $m+n$ as a multiple of 2. Our expression for $m + n$ lets us do this:

$$m + n = 2k_1 + 2k_2 + 2 = 2(k_1 + k_2 + 1).$$

Therefore, $m + n$ is even, which is what we wanted to prove.

2. Try some examples: $2 \cdot 6 = 12$, $8 \cdot 6 = 48$, $10 \cdot 10 = 100$. The products are multiples of 4, so the statement seems to be true. Let's prove it. The hypothesis is that we have two even integers. Let's call them $m$ and $n$. Since $m$ and $n$ are even, we can write $m = 2k_1$ and $n = 2k_2$ for some integers $k_1$ and $k_2$. The conclusion says something about the product $mn$, so we write

$$mn = (2k_1)(2k_2) = 4(k_1k_2).$$

This says that $mn$ is a multiple of 4, so we have completed the proof.

3. Let's try some examples: $3 \cdot 1 = 3$, $3 \cdot 2 = 6$, $3 \cdot 3 = 9$. Two out of three; not bad. In most sporting events, winning two out of three is awesome. But in math, one counterexample to a statement is enough to disprove the statement. Since $2 \cdot 3 = 6$ shows that there is a multiple of 3 that is even, the statement that all multiples of 3 are odd is false. So we have disproved the statement.

4. Try some examples: $6 \cdot 1 = 6$, $6 \cdot 2 = 12$, $6 \cdot 3 = 18$. All of these are even, so the statement looks correct. Let's try to prove it. A conditional form of the statement is "If $n$ is an integer, then $6n$ is even." The hypothesis is that $n$ is an integer. There's not much that we can say about $n$, so let's look at what we're trying to do. The conclusion says something about $6n$, so let's look at this number. We're trying to prove that $6n$ is even, which means that we need to express it as a multiple of 2. In fact, this is easy:

$$6n = 2(3n).$$

Therefore, $6n$ is a multiple of 2, so $6n$ is even. This proves the statement.

5. Let's look at some odd numbers: 3, 5, 7, 9, 11, 13. The numbers 3, 5, 11, and 13 are primes, but 9 is 3·3, so it is not prime. Since

> the odd number 9 is not prime, we have a counterexample, which means the statement is false.

Throughout this book you will see proofs and wonder how in the world anyone could have thought of them. Don't be disheartened. They might represent hours, or years, of work by brilliant people. We don't see their mistakes and false starts — we see only the final successes. Andrew Wiles, who proved Fermat's Last Theorem (see the Introduction and Chapter 15), explained it as follows:

> "Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room, and it's dark, completely dark. One stumbles around bumping into the furniture, and gradually, you learn where each piece of furniture is, and finally, after six months or so, you find the light switch. You turn it on, and suddenly, it's all illuminated. You can see exactly where you were." *(PBS NOVA Broadcast, October 28, 1997)*

Although none of the proofs you will be asked to do in this book should take six months, don't be afraid of stumbling around and making mistakes. Learning what doesn't work is sometimes as important as learning what does work.

We'll wrap up this introductory section with a brief discussion of some of the terminology concerning proofs you'll be seeing throughout this book. A **proposition** is a statement that we'll be able to prove. A **theorem** is an extremely important proposition, and is usually a highlight of the topic under consideration. If something is called a theorem, you should make a special effort to remember its statement and to understand what it says. A **lemma** is a statement that is used to prove a proposition or theorem. Often, a lemma is singled out because it is useful and interesting in its own right, but is not considered to be as important as a proposition or a theorem. (Admittedly, this can be somewhat subjective. One person's lemma can, at times, be someone else's proposition.) A **corollary** is a result that is an easy consequence of a proposition or theorem.

A statement that says "$A$ is true if and only if $B$ is true" is a combination of two statements: "If $A$ is true then $B$ is true" and "If $B$ is true then $A$ is true." To prove such a statement, you assume $A$ is true and deduce that $B$ is true. Then you assume $B$ is true and deduce that $A$ is true.

Often, "$A$ if and only if $B$" is written as "$A \Leftrightarrow B$." Similarly, "$A \Rightarrow B$" means that "$A$ implies $B$."

Sometimes you will see a statement saying that $A$, $B$, and $C$ are equivalent. This is the same as saying that $A$ is true if and only if $B$ is true, $B$ is true if and only if $C$ is true, and $A$ is true if and only if $C$ is true. However, it is not necessary to prove all six implications. Instead, prove that if $A$ is true then $B$ is true, then prove that if $B$ is true then $C$ is true, and finally prove that if $C$ is true then $A$ is true. This suffices to prove all of the necessary implications and is much more efficient. For example, since $A$ implies $B$ and $B$ implies $C$, we automatically conclude that $A$ implies $C$ without proving it directly.

### 1.1.1 Proof by Contradiction

Sometimes, the easiest way to prove a statement is to suppose the statement is false and deduce a false consequence. This is known as *proof by contradiction*. Classically, it was called *reductio ad absurdum* (Latin for "reduction to absurdity").

In the following, we give three examples of proof by contradiction. In each case, proof by contradiction arises naturally because the conclusion is a negative statement ("there is no such number" and "the number is not rational"). The proof proceeds by assuming the positive statement ("there is such a number" or "the number is rational") and showing that this leads to a contradiction, so the negative statement must be true.

Recall that a rational number is a number that can be expressed as the ratio of two integers; for example, $2/3$, $-15/2$, $71 = 71/1$, and $0 = 0/1$ are rational. An irrational number is a number that is not rational. We will see in Chapter 4 that $\sqrt{2}$ and $\sqrt{3}$ are examples of irrational numbers.

**I.** *Prove that there is no largest integer.*

*Proof.* If someone told you that there exists a largest integer, you would probably say something like this: "That's ridiculous. Adding one to any integer gives you a larger integer. So there can't be a largest one."

This reasoning is essentially the proof of the statement: Suppose that the statement to be proved is false. Then there exists a largest integer $n$. Let $m = n + 1$. Then $m$ is an integer and $m > n$, which contradicts

the assumption that $n$ was the largest integer. So, no largest integer can exist. This completes the proof. □

**II.** *Prove that there is no smallest positive rational number. (Recall that "positive" means greater than 0, and does not include 0.)*

*Proof.* Let's suppose the statement is false. Then there is a smallest positive rational number. Call it $r$. Since $r$ is rational, we can write $r = a/b$, where $a$ and $b$ are integers. Then $r/2 = a/(2b)$ is positive, rational, and smaller than $r$, which contradicts the assumption that $r$ is the smallest positive rational number. Therefore, the assumption that there is a smallest positive rational number has led to a contradiction. The only possibility that remains is that there is no smallest positive rational number. □

**III.** *Prove that a rational number plus an irrational number is irrational.*

*Proof.* Let's translate the statement into symbols: It says that if $x$ is rational and $y$ is irrational, then $z = x+y$ is irrational. We need to show that $z$ is irrational, which means that $z$ cannot be written in the form $z = c/d$ with integers $c$ and $d$. Because we're saying that something is *not* rational, it's very natural to use a proof by contradiction. So let's assume that $z$ is rational, which means that $z = c/d$ for some integers $c$ and $d$. Moreover, one of the hypotheses is that $x$ is rational, so $x$ can be written in the form $x = a/b$, where $a$ and $b$ are integers. Therefore, $x + y = z$ tells us that $y = z - x$, which we can write as

$$y = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

But $bc-ad$ and $bc$ are integers, so $y$ can be expressed as the ratio of two integers. This contradicts the assumption that $y$ is irrational. Therefore, the assumption that $z$ is rational led to the false consequence that $y$ is rational. Therefore, we conclude that $z$ must be irrational. □

A consequence of what we just proved is that $3 - \sqrt{2}$ is irrational. How do we show this? As mentioned earlier, we'll show in Chapter 4 that $\sqrt{2}$ is irrational. Suppose $3 - \sqrt{2}$ is rational. Then $3 = (3 - \sqrt{2}) + \sqrt{2}$ is a rational plus an irrational, which is irrational by what we just proved. But 3 is rational, so we have a contradiction. Therefore, our assumption that $3 - \sqrt{2}$ is rational must be false, so $3 - \sqrt{2}$ is irrational.

For the record, we now note that an irrational plus an irrational can be either rational or irrational. For example, $\sqrt{2} + \sqrt{2} = 2\sqrt{2}$ is an

example where the sum of two irrational numbers is irrational. On the other hand, $\sqrt{2} + (3 - \sqrt{2}) = 3$ is an example where the sum of two irrationals is rational.

When we have an "if–then" statement such as "if $A$ is true then $B$ is true," its *contrapositive* is "if $B$ is false then $A$ is false." A statement is true if and only if its contrapositive is true. A proof by contradiction is really just proving the contrapositive of the statement in question.

*Warning:* Proof by contradiction is a very useful tool, but do not overuse it. It is not uncommon to see something like the following: You are asked to prove that $x^2 - x = 12$ has a solution that is an integer. You write, "Suppose it does not have such a solution. Let $x = 4$. Then $4^2 - 4 = 12$, so the equation has a solution. Contradiction. Therefore, the equation has an integral solution." What's wrong? Technically, nothing. But what you've really done is say, "Suppose this does not have a solution. But it does! Let $x = 4$. Since $4^2 - 4 = 12$, the equation has a solution that is an integer." It makes much more sense to state directly that $x = 4$ is a solution. The moral is, don't use proof by contradiction when a direct proof is more straightforward.

## 1.2 Divisibility

A large portion of this book will be spent studying and proving properties of the integers. You can add, subtract, and multiply integers, and doing so always gives you another integer. Division is a little trickier — sometimes when you divide one integer by another you get an integer (12 divided by 3) and sometimes you don't (12 divided by 5). Because of this, the first idea we have to make precise is that of divisibility.

**Definition 1.2.** *Given two integers $a$ and $d$ with $d$ nonzero, we say that $d$* **divides** *$a$ (written $d \mid a$) if there is an integer $c$ with $a = cd$. If no such integer exists, so $d$ does* **not** *divide $a$, we write $d \nmid a$. If $d$ divides $a$, we say that $d$ is a* **divisor** *of $a$ and that $a$ is a* **multiple** *of $d$.*

**Examples.** $5 \mid 30$ since $30 = 5 \cdot 6$, and $3 \mid 102$ since $102 = 3 \cdot 34$, but $6 \nmid 23$ and $4 \nmid -3$. Also, $-7 \mid 35$, $8 \mid 8$, $3 \mid 0$, $-2 \mid -10$, and $1 \mid 4$.

**Remark.** There are two technical points that need to be mentioned. First, we never consider 0 to be a divisor of anything. Of course, we could agree that $0 \mid 0$, but it's easiest to avoid this case completely since we never need it. Second, if $d$ is a divisor of $a$, then $-d$ is a divisor of $a$. However, whenever we talk about the *set of divisors* of a positive integer, we follow the convention that we mean the *positive* divisors. So we say that the divisors of 6 are 1, 2, 3, and 6 (and ignore $-1$, $-2$, $-3$, $-6$).

There are several basic results concerning divisibility that we will be using throughout this book.

**Proposition 1.3.** *Assume that $a$, $b$, and $c$ are integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

*Proof.* We first need to change the hypotheses into something we can use. We are assuming that $a \mid b$ and $b \mid c$. What can we deduce from this? Maybe the best thing to do is use the definition of divisibility: Since $a \mid b$, we can write $b = ea$ for some integer $e$, and since $b \mid c$, we can write $c = fb$ for some integer $f$. Since we are trying to show $a \mid c$, we need to find an equation that relates $a$ and $c$. Let's try putting together what we have so far. Substitute $b = ea$ into $c = fb$ to obtain

$$c = fb = f(ea) = (fe)a.$$

Therefore, $c$ equals $a$ times an integer so, by definition, $a \mid c$. □

**Example.** The proposition implies, for example, that a multiple of 6 is even: Let $a = 2$ and $b = 6$, and let $c$ be an arbitrary integer. Then $a \mid b$. If $6 \mid c$, the proposition says that $2 \mid c$, which says that $c$ is even.

**Proposition 1.4.** *Assume that $a, b, d, x$, and $y$ are integers. If $d \mid a$ and $d \mid b$, then $d \mid ax + by$.*

*Proof.* Write $a = md$ and $b = nd$. Then

$$ax + by = (md)x + (nd)y = d(mx + ny),$$

so $c \mid ax + by$ by definition. □

Often, $ax + by$ is called a *linear combination* of $a$ and $b$, so Proposition 1.4 says that every divisor of both $a$ and $b$ is also a divisor of each linear combination of $a$ and $b$.

**Corollary 1.5.** *Assume that $a, b$, and $d$ are integers. If $d \mid a$ and $d \mid b$, then $d \mid a + b$ and $d \mid a - b$.*

*Proof.* To show that $d \mid a + b$, set $x = 1$ and $y = 1$ in the proposition and to show that $d \mid a - b$, set $x = 1$ and $y = -1$ in the proposition. □

**Examples.** Since $3 \mid 9$ and $3 \mid 21$, the proposition says that

$$3 \mid 5 \cdot 9 + 4 \cdot 21 = 129.$$

Since $5 \mid 20$ and $5 \mid 30$, we have $5 \mid 20 + 30 = 50$. Since $10 \mid 40$ and $10 \mid 60$, we have $10 \mid 40 - 60 = -20$.

---

**CHECK YOUR UNDERSTANDING**[2]

1. Does 7 divide 1001?
2. Show that $7 \nmid 1005$.

---

# 1.3 Euclid's Theorem

Fundamental to the study of the integers is the idea of a prime number.

**Definition 1.6.** *A* **prime number** *is an integer $p \geq 2$ whose only divisors are 1 and itself. A* **composite number** *is an integer $n \geq 2$ that is not prime.*

You may be wondering why 1 is not considered to be prime. After all, its only divisors are 1 and itself. Although there have been mathematicians in the past who have included 1 in the list of primes, nobody does so anymore. The reason for this is that mathematicians want to say there's *exactly one* way to factor an integer into a product of primes. If 1 were a prime, and we wanted to factor 6, for example, we'd have $6 = 2 \cdot 3 = 2 \cdot 3 \cdot 1 = 2 \cdot 3 \cdot 1 \cdot 1, \ldots$ and we would have an infinite number of ways to factor an integer into primes. So, to avoid this, we simply declare that 1 is not prime.

[2]Answers are at the end of the chapter.

The first ten prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

Notice that 2 is prime because its only divisors are 1 and 2, but no other even number can be prime because every other even number has 2 as a divisor.

It's natural to ask if the list of primes ever terminates. It turns out that it doesn't; that is, there are infinitely many primes. This fact is one of the most basic results on number theory. The first written record we have of it is in Euclid's *Elements*, which was written more than 2300 years ago. In the next section, we'll discuss Euclid's original proof. Before we do that, here's a proof that is a variation of his idea. We begin with a lemma.

**Lemma 1.7.** *Every integer greater than 1 is either prime or is divisible by a prime.*

*Proof.* If an integer $n$ is not a prime, then it is divisible by some integer $a_1$, with $1 < a_1 < n$. If $a_1$ is prime, we've found a prime divisor of $n$. If $a_1$ is not prime, it must be divisible by some integer $a_2$ with $1 < a_2 < a_1$. If $a_2$ is prime, then since $a_2 \mid a_1$ and $a_1 \mid n$, we have $a_2 \mid n$, and $a_2$ is a prime divisor of $n$. If $a_2$ is not prime, we continue and get a decreasing sequence of positive integers $a_1 > a_2 > a_3 > a_4 > \cdots$, all of which are divisors of $n$. Since you can't have a sequence of *positive* integers that decreases forever, this sequence must stop at some $a_m$. The fact that the sequence stops means that $a_m$ must be prime, which means that $a_m$ is a prime divisor of $n$. □

**Example.** In the proof of the lemma, suppose $n = 72000 = 720 \times 100$. Take $a_1 = 720 = 10 \times 72$. Take $a_2 = 10 = 5 \times 2$. Finally, take $a_3 = 5$, which is prime. Working backwards, we see that $5 \mid 72000$.

**Euclid's Theorem.** *There are infinitely many primes.*

*Proof.* We assume that there is a finite number of primes and arrive at a contradiction. So, let

$$2, 3, 5, 7, 11, ..., p_n \tag{1.1}$$

be the list of all the prime numbers. Form the integer

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p_n + 1.$$

To begin, $N$ can't be prime since it's larger than $p_n$ and $p_n$ is assumed to be the largest prime. So, we can use the previous lemma to choose a prime divisor $p$ of $N$. Since equation (1.1) is a list of every prime, $p$ is equal to one of the $p_i$ and therefore must divide $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p_n$. But $p$ now divides both $N$ and $N - 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p_n$. By Corollary 1.5, $p$ divides their difference, which is 1. This is a contradiction: $p \nmid 1$ because $p > 1$. This means that our initial assumption that there is a finite number of primes must be incorrect. □

Since mathematicians like to prove the same result using different methods, we give an alternative proof.

**Another proof of Euclid's Theorem.** We'll show that for each $n > 0$, there is a prime number larger than $n$. Let $N = n! + 1$ and let $p$ be a prime divisor of $N$. Either $p > n$ or $p \leq n$. If $p > n$, we're done. If $p \leq n$, then $p$ is a factor of $n!$, so $p \mid N - 1$. Recall that $p$ was chosen so that $p \mid N$, so we now have $p \mid N$ and $p \mid N - 1$. Therefore, $p \mid N - (N - 1) = 1$, which is impossible. This means that $p \leq n$ is impossible, so we must have $p > n$.

In particular, if $n$ is prime, there is a prime $p$ larger than $n$, so there is no largest prime. This means that there are infinitely many primes. □

---

**CHECK YOUR UNDERSTANDING**

3. Explain why $5 \nmid 2 \cdot 3 \cdot 5 \cdot 7 + 1$.

---

## 1.4 Euclid's Original Proof

Here is Euclid's proof that there is an infinite number of primes, using the standard translation of Sir Thomas Heath. Euclid's statements are written in italics. Since his terminology and notation may be unfamiliar, we have added comments in plain text where appropriate. It will be helpful to know that when Euclid says "*A measures B*" or "*B is*

*measured by A*," he means that $A$ divides $B$ or, equivalently, that $B$ is a multiple of $A$. Rather than saying that there are infinitely many primes, he says that, given a finite set of primes, there is at least one prime that is not in this set.

| **Euclid's Statements** | **Explanation** |
|---|---|
| *Let A, B, and C be the assigned prime numbers.* | This is the finite set of primes. Euclid assumes that there are only three. You can think of this as representing some arbitrary, unknown number of primes. |
| *I say that there are more prime numbers than A, B, and C.* | I will show that there is a prime that is not in our finite set. |
| *Take the least number DE measured by A, B, and C. Add the unit DF to DE.* | DE is the least common multiple of A, B, and C, and EF = DE + 1. |
| *Then EF is either prime or not. Let it be prime.* | Either EF is prime or it's not. First, assume that it's prime. |
| *Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C.* | Then we have found a set of primes that is larger than our original set of primes. |
| *Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number G.* | Next, assume that EF is not prime. Then, it is a multiple of some prime. Let it be a multiple of the prime G. |
| *I say that G is not the same with any of the numbers A, B, and C.* | We will now show that G is not in our set of primes. |
| *For if possible, let it be so. Now A, B, and C measure DE, therefore G also will measure DE.* | Assume that G is in our set. Since DE is a multiple of all of the primes in our set, G divides DE. |
| *But it also measures EF.* | But, EF is also a multiple of G. |

*Therefore G, being a number, will measure the remainder, the unit DF, which is absurd.*

Since EF is a multiple of G, and DE = EF + 1 is a multiple of G, their difference (EF + 1 - EF ), which equals 1, is also a multiple of G. This is a contradiction.

*Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore, the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C. Therefore, prime numbers are more than any assigned multitude of prime numbers. Q.E.D.*

So G is a prime number that is not in our set of primes. Therefore, no finite set can contain all of the primes. □

## 1.5 The Sieve of Eratosthenes

Eratosthenes was born in Cyrene (in modern-day Libya) and lived in Alexandria, Egypt, around 2300 years ago. He made important contributions to many subjects, especially geography. In number theory, he is famous for a method of producing a list of prime numbers up to a given bound without using division. To see how this works, we'll find all the prime numbers up to 50.

List the integers from 1 to 50. Ignore 1 and put a circle around 2. Now cross out every second number after 2. This yields (we give just the beginning of the list)

1 ② 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~
11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~.

Now look at the next number after 2 that is not crossed out. It's 3. Put a circle around 3 and cross out every third number after 3. This yields

1 ② ③ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~
11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~.