AN INTRODUCTION TO
Number Theory with Cryptography

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

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 book is designed to be used at several levels. It should fit well with an undergraduate course in number theory, but the book has also been used in a course for advanced high school students. It could also be used for independent study. We have included several topics beyond the standard ones covered in classes in order to open up new vistas to interested students.

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

The Chapters. The flowchart (following this preface) gives the dependencies of the chapters. When a section number occurs with an arrow, it means that only that section is needed for the chapter at the end of the arrow. For example, only the statement of quadratic reciprocity (Section 9.1) from Chapter 9 is needed in Chapter 10.

The core material is Chapters 1, 2, 4, 7, along with Sections 6.1 and 9.1. These should be covered if at all possible. At this point, there are several possibilities. It is highly recommended that some sections of Chapters 3, 5, and 8 be covered. These present some of the exciting applications of number theory to various problems, especially in cryptography. If time permits, some of the more advanced topics from Chapters 9 through 16 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. Appendix A treats some topics such as induction and the binomial theorem.

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 various places throughout the book.

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. The *Projects* are more substantial problems. Often, they consist of several steps that develop ideas more extensively. Although there are exceptions, generally they should take much longer to complete. Several could be worked on in groups. 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 wants to thank the Gilman School for its generous support during the writing of this book and 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 want to 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 web site for the book (www.math.umd.edu/∼lcw/numbertheory.html).

James S. Kraft
Gilman School
jkraft@gilman.edu

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

Chapter 0

Introduction

At Columbia University there is a Babylonian clay tablet called Plimpton 322 that is over 3800 years old and not much larger than a cell phone. Written in cuneiform script with four 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 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 three 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.

0.1 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 Chapters 11 and 13, we show how to solve Pell's equation, and in Chapter 15, we discuss its place in algebraic number theory.

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

0.2 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 5 and 8).

Questions about divisibility and remainders form the basis of modular arithmetic, which we introduce in Chapter 4. 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 (1777-1850) 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 9). Early progress towards 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.

0.3 Primes and 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 result we'll discuss in Chapter 16. 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 Valleé-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; however, special cases are Projects and Exercises in Chapters 1, 4, and 9.

There are many other questions that can be asked about primes. One of the most famous is the **Goldbach 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, $100 = 23 + 7 \cdot 11$). 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.

0.4 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 8) that uses large primes. A year later, Ron Rivest, Adi Shamir, and Len Adleman introduced the RSA cryptosystem (see Chapter 5), 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 2013, the limit was 230 digits. Some of these factorization methods will be discussed in Chapter 10.

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 8, 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 Divisibility

A large portion of this book will be spent studying 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 1.1. *Given two integers a and d with d non-zero, 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.*

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 1.2.[1] *Assume that a, b, and c are integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Since $a \mid b$, we can write $b = ea$ and since $b \mid c$, we can write $c = fb$ with e and f integers. Then, $c = fb = f(ea) = (fe)a$. So, by definition, $a \mid c$. $\square$

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 1.3. *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 $d \mid ax + by$ by definition. $\square$

Often, $ax + by$ is called a *linear combination* of a and b, so Proposition 1.3 says that every divisor of both a and b is also a divisor of each linear combination of a and b.

Corollary 1.4. *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. $\square$

Examples. Since $3 \mid 9$ and $3 \mid 21$, the proposition tells us 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 $10 \mid 40 - 60 = -20$.

[1] There is a set of names for results: A *theorem* is an important result that is usually one of the highlights of the subject. A *proposition* is an important result, but not as important as a theorem. A *lemma* is a result that helps to prove a proposition or a theorem. It is often singled out because it is useful and interesting in its own right. A *corollary* is a result that is an easy consequence of a theorem or proposition.

CHECK YOUR UNDERSTANDING[2]

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

1.2 Euclid's Theorem

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

Definition 1.5. *A* **prime number** *is an integer $p \geq 2$ whose only divisors are* 1 *and p. 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.

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 in number theory. The first written record we have of it is in Euclid's *Elements*, which was written over

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

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 1.6. *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 1.4, 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'll give several other proofs of this result throughout the book. As you'll see, each new proof will employ a different idea in number theory, reflecting the fact that Euclid's theorem is connected with many of its branches.

Here's one example of 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 $5 \nmid 2 \cdot 3 \cdot 5 \cdot 7 + 1$.

1.3 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 plaintext 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.

Euclid's Statements	**Explanation**
Let A, B, and C be the assigned prime numbers.	This is the assumption that there is a finite number of primes. Instead of assuming that there are n of them as we did, 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 no finite list could have all primes in it.
Take the least number DE measured by A, B, and C. Add the unit DF to DE.	In this step, Euclid multiplies all the primes together and then adds 1. So, 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.	This contradicts our assumption that A, B, and C is the list of all 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, EF is a multiple of some prime G.
I say that G is not the same with any of the numbers A,	We will now show that G is not in our list of all possible

B, and C.

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 list. Since DE is a multiple of A, and of B, and of C and since G is one of the listed primes, DE must also be a multiple of G.

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 list of all possible primes, and so there can be no finite list of all primes. Therefore, there is an infinite number of primes. $\square$

1.4 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	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	9	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	15	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$

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	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$

The first number after 3 that is not crossed out is 5, so circle 5 and cross out every 5th number after 5. After we do this, the next number after 5 that is not crossed out is 7, so we cross out every 7th number after 7. Listing all numbers up to 50, we now have

1	2	3	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	17	$\cancel{18}$	19	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	23	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	29	$\cancel{30}$
31	$\cancel{32}$	$\cancel{33}$	$\cancel{34}$	$\cancel{35}$	$\cancel{36}$	37	$\cancel{38}$	$\cancel{39}$	$\cancel{40}$
41	$\cancel{42}$	43	$\cancel{44}$	$\cancel{45}$	$\cancel{46}$	47	$\cancel{48}$	$\cancel{49}$	$\cancel{50}$.

The numbers that remain are 1 and the prime numbers up to 50. We can stop at 7 because of the following.

Proposition 1.7. *If n is composite, then n has a prime factor $p \leq \sqrt{n}$.*

Proof. Since n is composite, we can write $n = ab$ with $1 < a \leq b < n$. Then

$$a^2 \leq ab = n,$$

so $a \leq \sqrt{n}$. Let p be a prime number dividing a. Then $p \leq a \leq \sqrt{n}$. $\square$

The proposition says that the composite numbers up to 50 all have prime factors at most $\sqrt{50} \approx 7.07$, so we could stop after crossing out the multiples of 7. If we want to list the primes up to 1000, we need to cross out the multiples of only the primes through 31 (since $\sqrt{1000} \approx 31.6$).

Why is the process called a sieve? In our example, the multiples of the primes 2, 3, 5, 7 created a net. The numbers that fell through this net are the prime numbers.

CHECK YOUR UNDERSTANDING

4. Use the Sieve of Eratosthenes to compute the prime numbers less than 20.

1.5 The Division Algorithm

If a and b are integers, when we divide a by b we get an integer if and only if $b \mid a$. What can we say when b does not divide a? We can still make a statement using only integers by considering remainders. For example, we can say that 14 divided by 3 is 4 with a remainder of 2. We write this as

$$14 = 3 \cdot 4 + 2$$

to emphasize that our division statement can be written using addition and multiplication of integers. This is just the division with remainder that is taught in elementary school. Our next theorem says that this can always be done.

The Division Algorithm. *Let a and b be integers with $b > 0$. Then there exist unique integers q (the quotient) and r (the remainder) so that*

$$a = bq + r$$

with $0 \leq r < b$.

Proof. Let q be the largest integer less than or equal to a/b, so

$$q \leq a/b < q + 1.$$

Multiplying by b yields $bq \leq a < bq + b$, which implies that $0 \leq a - bq < b$. Let $r = a - bq$. Then

$$0 \leq r < b.$$

Since $a = bq + r$, we have proved that the desired q and r exist. It remains to prove that q and r are unique. If

$$a = bq + r = bq_1 + r_1$$

with $0 \leq r$, $r_1 < b$ then

$$b(q - q_1) = r_1 - r.$$

Since the left-hand side of this equation is a multiple of b, so is $r_1 - r$. Because $0 \leq r, r_1 < b$, we must have

$$-b < r_1 - r < b. \tag{1.2}$$

The only multiple of b that satisfies equation (1.2) is 0, so $r_1 - r = 0$. Therefore, $r_1 = r$ and the choice of r is unique. Since $b(q - q_1) = r_1 - r$, we now have $b(q - q_1) = 0$. Finally, because $b \neq 0$, we get that $q_1 - q = 0$, so $q_1 = q$ and q is also unique. This completes the proof. □

Examples: (a) Let $a = 27, b = 7$. Then $27 = 7 \cdot 3 + 6$, so $q = 3$ and $r = 6$.
(b) Let $a = -27, b = 7$. Then $-27 = 7 \cdot (-4) + 1$, so $q = -4$ and $r = 1$.
(c) Let $a = 24, b = 8$. Then $24 = 8 \cdot 3$, so $q = 3$ and $r = 0$.
(d) Let $a = 0$ and $b = 5$. Then $0 = 5 \cdot 0 + 0$, so $q = 0$ and $r = 0$.

CHECK YOUR UNDERSTANDING

5. Let $a = 200, b = 7$. Compute q and r such that $a = bq + r$ and $0 \leq r < b$.
6. Let $a = -200, b = 7$. Compute q and r such that $a = bq + r$ and $0 \leq r < b$.

1.5.1 A Cryptographic Application

Here's an amusing cryptographic application of the Division Algorithm. Let's say there is a 16-person committee that has to vote to approve a budget. The members prefer to keep their votes anonymous. Here's a mathematical way to have every person vote Yes, vote No, or Abstain, while ensuring that all votes are kept secret.

We'll call the chair A_1 and the other 15 members $A_2, A_3, ..., A_{16}$. The chair takes a blank piece of paper, writes a large number, say 7923, on it, and passes this to A_2. Then A_2 adds 17 for Yes, 1 for No, or 0 for Abstain. A_2 writes this sum on a new piece of paper, hands the new number to A_3, and returns the paper with 7923 written on it back to the chair. A_3 now has a piece of paper with either 7940 (if A_2 voted Yes), 7924 (if A_2 voted No), or 7923 (if A_2 abstained). Because A_3 does not know the original number, there is no way to know how A_2 voted. This process continues with A_3 adding 17 for Yes, 1 for No, or 0 for an abstention, and then passing the result to A_4. They continue until A_{16} gives a number to A_1, who adds a number for A_1's vote. Let's say the final sum is 8050. The chair subtracts the secret number 7923 from 8050 and gets 127. Then 127 is divided by 17 using the Division Algorithm:

$$127 = 7 \cdot 17 + 8$$

The chair announces that 7 people voted Yes, 8 people voted No, and there was 1 abstention (since $7 + 8$ is one less than 16, one person must have abstained).

Why do we count a Yes vote as 17 in this example? It's one more than the number of voters. If we used 16 for a Yes vote, we couldn't tell the difference between 16 No votes, and one Yes plus 15 abstentions since both give a total of 16.

Let's do another example with 23 people voting. Let's say the chair's random number is 27938. Now, committee members add 24 if they vote Yes and 1 if they vote No. We'll tell you what the votes were so that you can see why the method works. Let's say there are 16 Yes votes, 5 No votes, and 2 abstentions. Then the chair receives the number

$$27938 + 16 \cdot 24 + 5 + 2 \cdot 0 = 27938 + 389 = 28327.$$

Of course, when the chair subtracts 27938 from 28327 the answer is 389, and the Division Algorithm says that

$$389 = 16 \cdot 24 + 5.$$

The voting scheme does have a security flaw. If A_2 and A_4 compare notes, they can figure out how A_3 voted. Therefore, this method should be used only with a friendly committee.

1.6 The Greatest Common Divisor

The divisors of 12 are 1, 2, 3, 4, 6, and 12. The divisors of 18 are 1, 2, 3, 6, 9, and 18. Then $\{1, 2, 3, 6\}$ is the set of common divisors of 12 and 18. Notice that this set has a largest element, 6. If you have any two non-zero integers a and b, you can always form the set of their common divisors. Since 1 is a divisor of every integer, this set is nonempty. Because this set is finite, it must have a largest element. This idea is so basic, we make special note of it:

Definition 1.8. *Assume that a and b are integers and they are not both zero. Then the set of their common divisors has a largest element d, called the* **greatest common divisor** *of a and b. We write $d = \gcd(a, b)$.*

Examples. gcd(24, 52) = 4, gcd(9, 27) = 9, gcd(14, 35) = 7, gcd(15, 28) = 1.

Definition 1.9. *Two integers a and b are said to be* **relatively prime** *if $\gcd(a, b) = 1$.*

Examples. 14 and 15 are relatively prime. So are 21 and 40.

Remark. If $a \neq 0$, then $\gcd(a, 0) = a$. However, we do not define $\gcd(0, 0)$. Since arbitrarily large integers divide 0, there is no largest divisor. This is the reason we often explicitly write that at least one of a and b is nonzero when we are going to make a statement about $\gcd(a, b)$. In any case, whenever we write $\gcd(a, b)$, it is implicitly assumed that at least one of a and b is nonzero.

We saw that $\gcd(24, 52) = 4$, so 24 and 52 are not relatively prime. If we divide both 24 and 52 by 4, we get 6 and 13, which are relatively prime. This makes sense, since we've divided these numbers by their gcd, which is the largest possible common divisor. We now prove in the following that dividing two integers by their gcd always results in two relatively prime integers.

Proposition 1.10. *If a and b are integers with $d = \gcd(a, b)$, then*

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof. If $c = \gcd(a/d, b/d)$, then $c \mid (a/d)$ and $c \mid (b/d)$. This means that there are integers k_1 and k_2 with

$$\frac{a}{d} = ck_1 \text{ and } \frac{b}{d} = ck_2,$$

which tells us that $a = cdk_1$ and $b = cdk_2$. So, cd is a common divisor of a and b. Since d is the greatest common divisor and $cd \geq d$, we must have $c = 1$. $\square$

We'll see later that calculating the greatest common divisor has important applications. So, it's natural to ask, how do we go about finding the gcd when the answer is not immediately obvious? One way would be to factor each integer into primes and then take the product of all the primes that they have in common, including repetitions. For example, to find $\gcd(84, 264)$, we write

$$84 = 2 \cdot 2 \cdot 3 \cdot 7 \text{ and } 264 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 11,$$

so their common primes are 2, 2, and 3. We see that $\gcd(84, 264) = 2 \cdot 2 \cdot 3 = 12$. This may seem to be quite efficient but as we'll see later on, for the numbers of the size (i.e., hundreds of digits) that we'll be interested in, factoring is so slow as to be completely impractical. It's much easier to calculate $\gcd(a, b)$ by the method of the next section.

For reasonably small numbers, Proposition 1.3 is useful for calculating gcd's. For example, suppose we want to calculate $d = \gcd(1005, 500)$. Then $d \mid 1005$ and $d \mid 500$, so $d \mid 1005 - 2 \cdot 500$. Therefore, $d \mid 5$, which means that $d = 1$ or 5. Since $5 \mid 1005$ and $5 \mid 500$, we see that $5 = \gcd(1005, 500)$.

As another example, suppose n is an integer and we want to find all possibilities for $d = \gcd(2n+3, 3n-6)$. By Proposition 1.3,

$$d \mid 2n+3, \quad d \mid 3n-6 \Longrightarrow d \mid 3(2n+3) - 2(3n-6) = 21,$$

so $d = 1, 3, 7$, or 21. In fact, all possibilities occur: when $n = 1$ we have $d = \gcd(5, -3) = 1$, when $n = 3$ we have $d = \gcd(9, 3) = 3$, when $n = 2$ we have $d = \gcd(7, 0) = 7$, and when $n = 9$ we have $d = \gcd(21, 21) = 21$.

CHECK YOUR UNDERSTANDING

7. Evaluate $\gcd(24, 42)$.
8. Find an n with $1 < n < 10$ such that $\gcd(n, 60) = 1$.
9. Let n be an integer. Show that $\gcd(n, n+3) = 1$ or 3, and show that both possibilities occur.

1.7 The Euclidean Algorithm

The Euclidean Algorithm is one of the oldest and most useful algorithms in all of number theory. It is found as Proposition 2 in Book VII of Euclid's *Elements*. One of its features is that it allows us to compute gcd's without factoring. In cryptographic situations, where the numbers often have several hundred digits and are hard to factor, this is very important.

Suppose that we want to compute $\gcd(123, 456)$. Consider the following calculation:

$$\begin{aligned}
456 &= 3 \cdot 123 + 87 \\
123 &= 1 \cdot 87 + 36 \\
87 &= 2 \cdot 36 + 15 \\
36 &= 2 \cdot 15 + 6 \\
15 &= 2 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0.
\end{aligned}$$

By looking at the the prime factorizations of 456 and 123 we see that the last non-zero remainder, namely 3, is the gcd. Let's look at what we did. We divided the smaller of the original two numbers into the larger and got the remainder 87. Then we shifted the 123 and the 87 to the left, did the division, and got a remainder of 36. We continued the "shift left and divide" procedure until we got a remainder of 0.

Let's try another example. Compute gcd(119, 259):

$$\begin{aligned} 259 &= 2 \cdot 119 + 21 \\ 119 &= 5 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0. \end{aligned}$$

Again, the last non-zero remainder is the gcd. Why does this work? Let's start by showing why 7 is a common divisor in the second example. The fact that the remainder on the last line is 0 says that $7 \mid 14$. Since $7 \mid 7$ and $7 \mid 14$, the next-to-last line says that $7 \mid 21$, since 21 is a linear combination of 7 and 14. Now move up one line. We have just shown that $7 \mid 14$ and $7 \mid 21$. Since 119 is a linear combination of 21 and 14, we deduce that $7 \mid 119$. Finally, moving to the top line, we see that $7 \mid 259$ because 259 is a linear combination of 119 and 21, both of which are multiples of 7. Since $7 \mid 119$ and $7 \mid 259$, we have proved that 7 is a common divisor of 119 and 259.

We now want to show that 7 is the largest common divisor. Let d be any divisor of 119 and 259. The top line implies that 21, which is a linear combination of 259 and 119 (namely, $259 - 2 \cdot 119$), is a multiple of d. Next, go to the second line. Both 119 and 21 are multiples of d, so 14 must be a multiple of d. The third line tells us that since $d \mid 21$ and $d \mid 14$, we must have $d \mid 7$. In particular, $d \leq 7$, so 7 is the greatest common divisor, as claimed. We also have proved the additional fact that any common divisor must divide 7.

All of this generalizes to the following:

Euclidean Algorithm. *Let a and b be non-negative integers and* *assume that* $b \neq 0$. *Do the following computation:*

$$\begin{aligned}
a &= q_1 b \ \ + r_1, \ \ \textit{with } 0 \le r_1 < b \\
b &= q_2 r_1 + r_2, \ \ \textit{with } 0 \le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \ \ \textit{with } 0 \le r_3 < r_2 \\
&\ \vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \ \ \textit{with } 0 \le r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + 0.
\end{aligned}$$

The last non-zero remainder, namely r_{n-1}*, equals* $\gcd(a, b)$.

The proof that $r_{n-1} = \gcd(a, b)$ follows exactly the steps used in the example of $7 = \gcd(259, 119)$. Since the last remainder is 0, r_{n-1} divides r_{n-2}. The next-to-last line yields $r_{n-1} \mid r_{n-3}$. Moving up, line by line, we eventually find that r_{n-1} is a common divisor of a and b.

Now suppose that d is a common divisor of a and b. The first line yields $d \mid r_1$. Since $d \mid b$ and $d \mid r_1$, the second line yields $d \mid r_2$. Continuing downwards, line by line, we eventually find that $d \mid r_{n-1}$. Therefore, $d \le r_{n-1}$, so r_{n-1} is the largest divisor, which means that $r_{n-1} = \gcd(a, b)$. We also obtain the extra fact that each common divisor of a and b divides $\gcd(a, b)$.

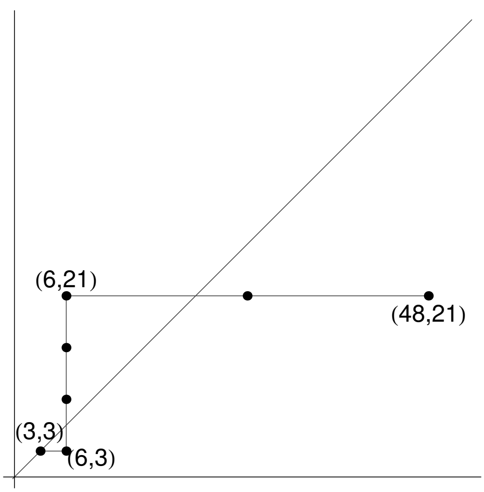

FIGURE 1.1: Computation of gcd(48, 21)

There is a geometrical way to view the Euclidean Algorithm. For example, suppose we want to compute $\gcd(48, 21)$. Start at the point $(48, 21)$ in the plane. Move to the left in steps of size 21 until you land on or cross the line $y = x$. In this case, we take two steps of size 21 and move to $(6, 21)$. Now move downward in steps of size 6 (the smaller of the two coordinates) until you land on or cross the line $y = x$. In this case, we take three steps of size 6 and move to $(6, 3)$. Now move to the left in steps of size 3. In one step we end up at $(3, 3)$ on the line $y = x$. The x-coordinate (also the y-coordinate) is the gcd.

In each set of moves, the number of steps is the quotient in the Euclidean Algorithm and the remainder is the amount that the last step overshoots the line $y = x$.

1.7.1 The Extended Euclidean Algorithm

The Euclidean Algorithm yields an amazing and very useful fact: $\gcd(a, b)$ can be expressed as a linear combination of a and b. That is, there exist integers x and y such that $\gcd(a, b) = ax + by$. For example,

$$\begin{aligned} 3 &= \gcd(456, 123) = 456 \cdot 17 - 123 \cdot 63 \\ 7 &= \gcd(259, 119) = 259 \cdot 6 - 119 \cdot 13. \end{aligned}$$

The method for obtaining x and y is called the **Extended Euclidean Algorithm**. Once you've used the Euclidean Algorithm to arrive at $\gcd(a,\ b)$, there's an easy and very straightforward way to implement the Extended Euclidean Algorithm. We'll show you how it works with the two examples we've just calculated.

When we computed $\gcd(456, 123)$, we performed the following calculation:

$$\begin{aligned} 456 &= 3 \cdot 123 + 87 \\ 123 &= 1 \cdot 87 + 36 \\ 87 &= 2 \cdot 36 + 15 \\ 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

We'll form a table with three columns and explain how they arise as we compute them.

We begin by forming two rows and three columns. The first entries in the rows are the numbers we started with. In this case these numbers are 456 and 123. The columns tell us how to form each of these numbers as a linear combination of 456 and 123. In other words, we will always have

$$\text{entry in first column } = 456x + 123y,$$

where x and y are integers. Initially, this is trivial: $456 = 1 \cdot 456 + 0 \cdot 123$ and $123 = 0 \cdot 456 + 1 \cdot 123$:

$$\begin{array}{cccl} & x & y & \\ 456 & 1 & 0 & (456 = 1 \cdot 456 + 0 \cdot 123) \\ 123 & 0 & 1 & (123 = 0 \cdot 456 + 1 \cdot 123). \end{array}$$

Now things get more interesting. If we look at the first line in our gcd(456, 123) calculation, we see $456 = 3 \cdot 123 + 87$. We rewrite this as $87 = 456 - 3 \cdot 123$. Using this as a guide, we compute

$$(\text{1st row}) \ - 3 \cdot (\text{2nd row}),$$

yielding the following

$$\begin{array}{cccl} & x & y & \\ 456 & 1 & 0 & \\ 123 & 0 & 1 & \\ 87 & 1 & -3 & (\text{1st row}) - 3 \cdot (\text{2nd row}). \end{array}$$

The last line tells us that $87 = 456 \cdot 1 + 123 \cdot (-3)$.

We now move to the second row of our gcd calculation. This says that $123 = 1 \cdot 87 + 36$, which we rewrite as $36 = 123 - 1 \cdot 87$. Again, in the column and row language, this tells us to compute (2nd row) $-$ (3rd row). We write this as

$$\begin{array}{rrrl} & x & y & \\ 456 & 1 & 0 & \\ 123 & 0 & 1 & \\ 87 & 1 & -3 & \\ 36 & -1 & 4 & \text{(2nd row)} - \text{(3rd row)}. \end{array}$$

The last line tells us that $36 = 456 \cdot (-1) + 123 \cdot 4$.

Moving to the third row of our gcd calculation, we see that $15 = 87 - 2 \cdot 36 =$(3rd row) $-2\cdot$(4th row) in our row and column language. This becomes

$$\begin{array}{rrrl} & x & y & \\ 456 & 1 & 0 & \\ 123 & 0 & 1 & \\ 87 & 1 & -3 & \\ 36 & -1 & 4 & \\ 15 & 3 & -11 & \text{(3rd row)} - 2\cdot\text{(4th row)}. \end{array}$$

We continue in this way and end when we have $3 = \gcd(456,\ 123)$ in the first column:

$$\begin{array}{rrrl} & x & y & \\ 456 & 1 & 0 & \\ 123 & 0 & 1 & \\ 87 & 1 & -3 & \\ 36 & -1 & 4 & \\ 15 & 3 & -11 & \\ 6 & -7 & 26 & \text{(4th row)} - 2\cdot\text{(5th row)} \\ 3 & 17 & -63 & \text{(5th row)} - 2\cdot\text{(6th row)}. \end{array}$$

This tells us that $3 = 456 \cdot 17 + 123 \cdot (-63)$.

Notice that as we proceeded, we were doing the Euclidean Algorithm in the first column. The first entry of each row is a remainder from the gcd calculation and the second and third entries allow us to express the number in the first column as a linear combination of 456 and 123. The quotients in the Euclidean Algorithm told us what to multiply a row by before subtracting it from the previous row.

Here's another example, where we calculate gcd(259, 119). You should go step-by-step to make sure that you understand how we're arriving at the numbers in each row.

	x	y	
259	1	0	
119	0	1	
21	1	-2	(1st row) $-$ 2·(2nd row)
14	-5	11	(2nd row) $-$ 5·(3rd row)
7	6	-13	(3rd row) $-$ (4th row).

The end result is $7 = 259 \cdot 6 - 119 \cdot 13$.

To summarize, we state the following.

Theorem 1.11. *Let a and b be integers with at least one of a, b non-zero. There exist integers x and y, which can be found by the Extended Euclidean Algorithm, such that*

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

Proof. Although it would be fairly straightforward to write a detailed proof that follows the reasoning of the examples, the numerous indices and variables would make the proof rather unenlightening. Therefore, we spare the reader. Instead, we give the following non-constructive proof that $\gcd(a, b)$ is a linear combination of a and b.

Let S be the set of integers that can be written in the form $ax+by$ with integers x and y. Since a, b, $-a$, and $-b$ are in S, we see that S contains at least one positive integer. Let d be the smallest positive integer in S (this is an application of the Well Ordering Principle; see Appendix A). Since $d \in S$, we know that $d = ax_0 + by_0$ for some integers x_0 and y_0. We claim that a and b are multiples of d, so d is a *common divisor* of both a and b. To see this, write $a = dq + r$ with integers q and r such that $0 \le r < d$. Since

$$r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q),$$

we have that $r \in S$. Since d is the smallest positive element of

S and $0 \le r < d$, we must have $r = 0$. This means that $d \mid a$. Similarly, $d \mid b$, so d is a common divisor of a and b.

Now suppose that e is any common divisor of a and b. Proposition 1.3 implies that e divides $ax_0 + by_0 = d$, so $e \le d$. Therefore, d is the greatest common divisor. By construction, d is a linear combination of a and b. □

Finally, we give a version of Theorem 1.11 that applies to more than two numbers.

Theorem 1.12. *Let $n \ge 2$ and let $a_1, a_2, \ldots, a_n$ be integers (at least one of them must be nonzero). Then there exist integers $x_1, x_2, \ldots, x_n$ such that*

$$\gcd(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Proof. We'll use mathematical induction (see Appendix A). By Theorem 1.11, the result is true for $n = 2$. Assume that it is true for $n = k$. Then

$$\gcd(a_1, a_2, \cdots, a_k) = a_1y_1 + a_2y_2 + \cdots + a_ky_k \tag{1.3}$$

for some integers $y_1, y_2, \ldots, y_k$. But

$$\begin{aligned}\gcd(a_1, a_2, \ldots, a_{k+1}) &= \gcd(\gcd(a_1, a_2, \ldots, a_k), a_{k+1}) \\ &= \gcd(a_1, a_2, \ldots, a_k)x + a_{k+1}y\end{aligned}$$

for some integers x and y, again by Theorem 1.11. Substituting (1.3) into this equation yields

$$\begin{aligned}\gcd(a_1, a_2, \ldots, a_{k+1}) &= (a_1y_1 + a_2y_2 + \cdots + a_ky_k)x + a_{k+1}y \\ &= a_1(xy_1) + a_2(xy_2) + \cdots + a_k(xy_k) + a_{k+1}y_{k+1},\end{aligned}$$

which is the desired result, with $x_i = xy_i$ for $1 \le i \le k$ and $x_{k+1} = y$. Therefore, the result is true for $n = k+1$. By induction, the result holds for all positive integers $n \ge 2$. □

Theorem 1.11 (and its generalization 1.12) are among the most important tools in number theory and they'll be used to deduce many fundamental properties of the integers. The following is an example.

Proposition 1.13. *Let a, b, c be integers with $a \neq 0$ and $\gcd(a, b) = 1$. If $a \mid bc$ then $a \mid c$.*

Proof. Theorem 1.11 says that we can write $1 = ax + by$ for some integers x and y. Multiply by c to obtain $c = acx + bcy$. Since $a \mid a$ and $a \mid bc$, Proposition 1.3 implies that $a \mid c$. ☐

CHECK YOUR UNDERSTANDING

10. Compute $\gcd(654, 321)$ without factoring.
11. Find x and y such that $17x + 12y = 1$.

1.8 Other Bases

The numbers that we use in our everyday life are written using base 10 notation. For example, 783 means $7 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0$. The position of each digit tells us what power of 10 that digit will be multiplied by to give us our number, so 58 and 85 represent different numbers because of the positions of the 5 and 8. In the past there have been other ways to represent integers. When Abraham Lincoln wrote the Gettysburg Address, he didn't begin with "Eighty-seven years ago," but with "Four score and seven years ago" using the word *score* (which comes from the Norse *skar*, meaning *mark* or *tall*) for the number 20. In Britain, people still say they weigh 10 stone 7 pounds instead of 147 pounds, using the word stone for 14 from an old unit of measurement.

Our reliance on base 10 is most likely an accident of evolution, and is a reflection of the ten fingers that we use to count. The Babylonians used a base 60 for their number system, and the Mayans used base 20. (Perhaps they also used their toes.) Computers are based on a binary system and often use base 16 ($= 2^4$) to represent numbers.

If we have a number in a different base, let's say base 7, then it's easy to rewrite it as a base 10 number. Let's say we had 3524_7

where the subscript 7 means we are working in base 7. Then,

$$3524_7 = 3{\cdot}7^3+5{\cdot}7^2+2{\cdot}7^1+4{\cdot}7^0 = 3{\cdot}343+5{\cdot}49+2{\cdot}7+4{\cdot}1 = 1292_{10}.$$

We can also convert a number from base 10 to any other base with the use of the Division Algorithm.

We give three examples to show how this works.

Example. Convert the base 10 number 21963 to a base 8 number.

We proceed by dividing 21963 by 8, then dividing the quotient by 8, and continuing until the quotient is 0. At the end of the example, we'll show why the process works.

$$\begin{array}{rcll} 21963 & = & 2745 \cdot 8 & + \; 3 \\ 2745 & = & 343 \cdot 8 & + \; 1 \\ 343 & = & 42 \cdot 8 & + \; 7 \\ 42 & = & 5 \cdot 8 & + \; 2 \\ 5 & = & 0 \cdot 8 & + \; 5. \end{array}$$

This tells us that $21963_{10} = 52713_8$. To see why this works, we start from the beginning, making sure to group our factors of 8 together.

$$\begin{gathered} 21963 = 2745 \cdot 8 + 3 = (343 \cdot 8 + 1)8 + 3 = \\ 343 \cdot 8^2 + 1 \cdot 8 + 3 = (42 \cdot 8 + 7)8^2 + 1 \cdot 8 + 3 = \\ 42 \cdot 8^3 + 7 \cdot 8^2 + 1 \cdot 8 + 3 = (5 \cdot 8 + 2)8^3 + 7 \cdot 8^2 + 1 \cdot 8 + 3 = \\ 5 \cdot 8^4 + 2 \cdot 8^3 + 7 \cdot 8^2 + 1 \cdot 8 + 3 = \\ 52713_8. \end{gathered}$$

Example. Convert the base 10 number 1671 to base 2.

$$\begin{array}{rcll} 1671 & = & 835 \cdot 2 & + \; 1 \\ 835 & = & 417 \cdot 2 & + \; 1 \\ 417 & = & 208 \cdot 2 & + \; 1 \\ 208 & = & 104 \cdot 2 & + \; 0 \\ 104 & = & 52 \cdot 2 & + \; 0 \\ 52 & = & 26 \cdot 2 & + \; 0 \\ 26 & = & 13 \cdot 2 & + \; 0 \\ 13 & = & 6 \cdot 2 & + \; 1 \\ 6 & = & 3 \cdot 2 & + \; 0 \\ 3 & = & 1 \cdot 2 & + \; 1 \\ 1 & = & 0 \cdot 2 & + \; 1. \end{array}$$

So, $1671_{10} = 11010000111_2$.

Example. It's always a good idea to make sure that any mathematical method works for an example where you already know the answer. This serves as a type of "reality check." So, let's take a base 10 number, say 314159, and use the above algorithm to "convert" it to base 10:

$$\begin{array}{rcllcl} 314159 & = & 31415 \cdot 10 & + & 9 \\ 31415 & = & 3141 \cdot 10 & + & 5 \\ 3141 & = & 314 \cdot 10 & + & 1 \\ 314 & = & 31 \cdot 10 & + & 4 \\ 31 & = & 3 \cdot 10 & + & 1 \\ 3 & = & 0 \cdot 10 & + & 3. \end{array}$$

It should be reassuring that this gives back the original 314159.

CHECK YOUR UNDERSTANDING

12. Convert 1234_{10} to base 7.
13. Convert 321_5 to base 10.

1.9 Linear Diophantine Equations

As we mentioned in the introduction, Diophantus lived in Alexandria, Egypt, about 1800 years ago. His book *Arithmetica* gave 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.

In this section we study the equation

$$ax + by = c$$

where a, b, and c are integers. Our goal is to find out when **integer** solutions to this equation exist, and when they do exist, to find all of them.

Equations of this form can arise in real life. For example, how many dimes and quarters are needed to pay someone \$1.05? This means we have to solve $10x + 25y = 105$. One solution is $x = 3,\ y = 3$. Another solution is $x = 8,\ y = 1$. There are also solutions such as $x = -2,\ y = 5$, which means you pay 5 quarters and get back 2 dimes.

Before we get to the main result of this section, we look at two more examples that will help us understand the general situation. First, consider $6x - 9y = 20$. Notice that 3 must divide the left-hand side but 3 is not a divisor of the right-hand side. This tells us that this equation can never have an integer solution. To make things notationally simpler, let $d = \gcd(a, b)$. We then see that in order for $ax + by = c$ to have a solution, we must have $d \mid c$. Now let's look at an example where this does occur, say $6x + 9y = 21$. We can divide both sides by 3, giving us $2x + 3y = 7$. After a brief inspection, we see that $x = 2$ and $y = 1$ is a solution. Are there others? It's easy to see that if t is any integer, then $x = 2 + 3t$ and $y = 1 - 2t$ is also a solution. Let's verify this by substituting these expressions for x and y into the original equation, $6x + 9y = 21$:

$$6(2 + 3t) + 9(1 - 2t) = 12 + 18t + 9 - 18t = 21,$$

so our single solution gives rise to an infinite number of them. This can be generalized in the following theorem:

Theorem 1.14. *Assume that a, b, and c are integers where at least one of a, b is non-zero. Then the equation*

$$ax + by = c \tag{1.4}$$

has a solution if and only if $\gcd(a, b) \mid c$. If it has one solution, then it has an infinite number. If (x_0, y_0) is any particular solution, then all solutions are of the form

$$x = x_0 + \frac{b}{gcd(a, b)}t, \qquad y = y_0 - \frac{a}{gcd(a, b)}t \tag{1.5}$$

with t an integer.

Proof. We begin by setting $\gcd(a, b) = d$. We have already seen that if $d \nmid c$, then there are no solutions. Now, assume $d \mid c$. From

Theorem 1.11 we know that there are integers r and s so that $ar + bs = d$. Since $d \mid c$, we have that $df = c$ for some integer f. Therefore,

$$a(rf) + b(sf) = df = c.$$

So, $x_0 = rf$ and $y_0 = sf$ is a solution to $ax + by = c$.

Now let

$$x = x_0 + \frac{b}{d}t \text{ and } y = y_0 - \frac{a}{d}t.$$

Then

$$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 + \frac{ab}{d}t - \frac{ba}{d}t = c.$$

This shows that a solution to (1.4) exists (assuming that $\gcd(a, b)$ divides c) and that once we have one solution, we have an infinite number of a specific form.

Next, we need to prove that every solution of equation (1.4) is of the stated form. Fix one solution x_0, y_0 and let u, v be *any* solution of equation (1.4). (Any solution continues to mean any integer solution.) Then

$$au + bv = c \tag{1.6}$$

and

$$ax_0 + by_0 = c. \tag{1.7}$$

Subtracting equation (1.7) from equation (1.6) gives us

$$a(u - x_0) + b(v - y_0) = 0,$$

so

$$a(u - x_0) = -b(v - y_0) = b(y_0 - v). \tag{1.8}$$

After dividing both sides of equation (1.8) by d, we get

$$\frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v). \tag{1.9}$$

There is a small technicality that needs to be dealt with. If $a = 0$, then we can't say that a/d divides the right-hand side, because we don't allow 0 to divide anything. But if $a = 0$ then our original equation is $by = c$. This means that $v = y_0 = c/b$ and x can be arbitrary, since there is no restriction on x. This is exactly the conclusion of the theorem, which says that all solutions have the form $y = y_0$ and $x = x_0 + t$ (since $\gcd(a, b) = \gcd(0, b) = b$). For the rest of the proof, we now assume that $a \neq 0$.

Equation (1.9) implies that

$$(a/d) \mid (b/d)(y_0 - v).$$

Since $\gcd(a/d,\, b/d) = 1$, Proposition 1.13 implies that (a/d) divides $(y_0 - v)$. By definition, this means that there is an integer t with

$$y_0 - v = t\frac{a}{d}. \tag{1.10}$$

Substituting the value for $y_0 - v$ from (1.10) into (1.9), we get

$$\frac{a}{d}(u - x_0) = \frac{b}{d}\left(\frac{a}{d}t\right). \tag{1.11}$$

Multiplying both sides by $\dfrac{d}{a}$, we have

$$u - x_0 = \frac{b}{d}t \qquad \text{or} \qquad u = x_0 + \frac{b}{d}t. \tag{1.12}$$

Combining (1.10) and (1.12), we have

$$u = x_0 + \frac{b}{d}t \qquad \text{and} \qquad v = y_0 - \frac{a}{d}t. \tag{1.13}$$

Since u and v were arbitrary solutions of (1.4), we have completed the proof. $\square$

In practice, if we want to solve equation (1.4), we first verify that $d \mid c$. If it doesn't, we're done since there are no solutions. If it does, we divide both sides by d to get a new equation

$$a'x + b'y = c'$$

and in this equation, $\gcd(a', b') = 1$. For example, if we want to solve $6x + 15y = 30$, we divide by 3 and instead solve $2x + 5y = 10$. This means that we will usually be using the following:

Corollary 1.15. *Assume that a, b, and c are integers with at least one of a, b non-zero. If $\gcd(a, b) = 1$, then the equation*

$$ax + by = c$$

always has an infinite number of solutions. If (x_0, y_0) is any particular solution, then all solutions are of the form

$$x = x_0 + bt, \qquad y = y_0 - at$$

with t an integer.

It may seem that we've ignored the problem of actually finding a solution to a linear Diophantine equation; however, the Extended Euclidean Algorithm from the previous section provides an efficient method. For example, to solve $13x + 7y = 5$, we write $\gcd(7, 13) = 1$ as a linear combination of 7 and 13 and then multiply our solution by 5. Here's how it works.

We begin by calculating $\gcd(7, 13)$ using the Euclidean Algorithm.

$$\begin{aligned} 13 &= 1 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0. \end{aligned}$$

Now, we use the Extended Euclidean Algorithm to express 1 as a linear combination of 7 and 13:

$$\begin{array}{rrrl} & x & y & \\ 13 & 1 & 0 & \\ 7 & 0 & 1 & \\ 6 & 1 & -1 & \text{(1st row)} - \text{(2nd row)} \\ 1 & -1 & 2 & \text{(2nd row)} - \text{(3rd row)}. \end{array}$$

We see that $1 = -1 \cdot 13 + 2 \cdot 7$, so that $x = -1,\ y = 2$ is a solution to $13x + 7y = 1$:

$$13(-1) + 7(2) = 1.$$

Multiplying both x and y by 5 gives us $x = -5,\ y = 10$ is the desired solution to the original equation, $13x + 7y = 5$:

$$13(-5) + 7(10) = 5.$$

Theorem 1.14 tells us that all solutions have the form

$$x = -5 + 7t, \quad y = 10 - 13t,$$

where t is an integer.

Here is another example. Let's find all solutions of $10x+25y = 105$, the equation for paying \$1.05 in dimes and quarters. First, divide by $5 = \gcd(10, 25)$ to get

$$2x + 5y = 21.$$

At this point, you can find a solution by any method. For example you can try values until something works or use the Extended Euclidean Algorithm. In any case, one solution is $x_0 = 8,\ y_0 = 1$. The set of all solutions is

$$x = 8 + 5t, \quad y = 1 - 2t.$$

The solution $x = 3,\ y = 3$ given at the beginning of this section is obtained by letting $t = -1$. The solution with $x = -2,\ y = 5$ is obtained by letting $t = -2$.

Now, a warning. It's quite possible that two people working on the same problem may get correct answers that look different. If a problem says find all solutions to $5x - 3y = 1$, you may notice that (2, 3) is a particular solution, so all solutions look like $x = 2-3t, \quad y = 3-5t$. A friend may choose a particular solution to be $(-1, -2)$ and say that all solutions are of the form $x = -1-3t, y = -2-5t$. These two apparently different sets of solutions are in fact the same, as the following shows:

Solutions of the form $x = 2 - 3t, y = 3 - 5t$:

$$\ldots, (-4, -7), (-1, -2),\ (\mathbf{2}, \mathbf{3}),\ (5, 8),\ (8, 13),\ (11, 18),\ \ldots$$

Solutions of the form $x = -1 - 3t, y = -2 - 5t$:

$$\ldots, (-4, -7), (\mathbf{-1}, \mathbf{-2}),\ (2, 3),\ (5, 8),\ (8, 13),\ (11, 18),\ \ldots$$

CHECK YOUR UNDERSTANDING

14. Find all integer solutions to $6x + 8y = 4$.

1.10 The Postage Stamp Problem

If you went to the post office to mail a letter and discovered that they had only three-cent and five-cent stamps, what postage values would you be able to put on your mail? What values are unobtainable from these two stamps? These questions are special cases of what is called the Postage Stamp Problem.

The Postage Stamp Problem: If a and b are positive integers, what positive integers can be written as $ax + by$ with both x and y non-negative?

To begin, notice that we want to consider only the case where a and b are relatively prime. If, for example, they were both even, then no odd numbers would ever be expressible as a linear combination of them, and the problem becomes less interesting.

We'll call numbers that can be written as $ax + by$ with both x and y non-negative **feasible**. For example, a, b, and ab are always feasible since

$$a = 1 \cdot a + 0 \cdot b, \quad b = 0 \cdot a + 1 \cdot b, \text{ and } ab = b \cdot a + 0 \cdot b = 0 \cdot a + a \cdot b.$$

The requirement that x and y both be non-negative is what makes this an interesting problem. For example, our initial question had three-cent and five-cent stamps, so $a = 3$ and $b = 5$. Since 3 and 5 are relatively prime, if negative coefficients were allowed, then *every* integer could be expressed as a linear combination of them from Theorem 1.11. Let's try to understand which numbers are feasible and which are not by making a chart to see if any patterns occur:

Postage Stamp Problem with $a = 3$ and $b = 5$

Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Feasible			✓		✓	✓		✓	✓	✓	✓	✓	✓	✓

An empty space means that the number above it cannot be written as a permissible linear combination of 3 and 5, while a ✓ means that it can be. For example, 13 has a ✓underneath it because $13 = 1 \cdot 3 + 2 \cdot 5$.

Notice that every number in our list that's greater than 7 is feasible. In fact, once we notice that the three consecutive integers 8, 9, and 10 are feasible, we can show that every number greater than 10 is also feasible. Here's how the argument goes. Every number greater than 10 differs from 8, 9, or 10 by a multiple of 3. (You can use the Division Algorithm to formally prove this.) So, to get any number greater than 10, just add enough three-cent stamps to get the desired amount. For example, suppose you want 92 cents. Since $92 - 8 = 84 = 3 \cdot 28$, take the three-cent and five-cent stamps needed to get eight cents, and add 28 more 3-cent stamps to get 92 cents.

One more thing to point out before we do another example. The last number in our list that is not feasible is 7, which can be written as $3 \cdot 5 - 3 - 5$. Let's see if this pattern holds.

Postage Stamp Problem with $a = 2$ and $b = 7$

Number	1	**2**	3	4	5	6	**7**	8	9	10	11	12	13	**14**
Feasible		✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓

Again, $5 = 2 \cdot 7 - 2 - 7$ is the last number that is not feasible. If you try another small example (say with $a = 4$ and $b = 9$) you will see the same thing occurs, namely every integer greater than $ab - a - b$ can be written as a linear combination of a and b while $ab - a - b$ cannot be. We'll now use two steps to show that this is always the case.

- $ab - a - b$ is not feasible.
- If $m > ab - a - b$, then m is feasible.

We begin by verifying the first step.

Proposition 1.16. *Assume that $a > 1$ and $b > 1$ are positive, relatively prime integers. Then there are no non-negative integers x and y with $ax + by = ab - a - b$.*

Proof. We start by observing that

$$a(-1) + b(a-1) = ab - a - b,$$

so $x = -1, y = a - 1$ is a solution to $ax + by = ab - a - b$.

Since $\gcd(a, b) = 1$, we see from Corollary 1.15 that every solution to $ax + by = ab - a - b$ has the form

$$x = -1 + bt, \quad y = a - 1 - at$$

for some integer t. In order to get an x value that's non-negative, we have to choose a value of t that's positive. But if $t > 0$, then $1 - t \leq 0$ so $y = a - 1 - at = a(1 - t) - 1 \leq -1$. Forcing x to be non-negative forces y to be negative. This means it is impossible to find a non-negative solution to $ax + by = ab - a - b$. $\square$

We've now shown that $ab - a - b$ can never be feasible. We next show that every integer larger than $ab - a - b$ is feasible.

Proposition 1.17. *Assume that a and b are positive with* $\gcd(a, b) = 1$. *If $n \geq ab - a - b + 1$, there are non-negative integers x and y with $ax + by = n$.*

Proof. We again appeal to Corollary 1.15. We find a pair of integers (x_0, y_0) with

$$ax_0 + by_0 = n \geq ab - a - b + 1 \tag{1.14}$$

which enables us to express every solution in the form

$$x = x_0 + bt, \quad y = y_0 - at.$$

It is possible that x_0 or y_0 is negative. What we'll do is find the solution to $ax + by = n$ with the smallest possible non-negative y, and then show that the corresponding x must be non-negative. After all, this is our best chance, because making y smaller makes x bigger, so if anything works, it must be the smallest non-negative value of y. Using the Division Algorithm, we can divide y_0 by a and write $y_0 = at + y_1$, with $0 \leq y_1 \leq a - 1$, for some integer t. This y_1 is our choice of y. Since $y_1 = y_0 - at$, we take $x_1 = x_0 + bt$ as our choice of x. We'll show that $x_1 \geq 0$. If $x_1 \leq -1$, then, because $y_1 \leq a-1$,

$$\begin{aligned} n &= ax_0 + by_0 \\ &= a(x_1 - bt) + b(y_1 + at) \\ &= ax_1 + by_1 \\ &\leq a(-1) + b(a-1) \\ &= ab - a - b, \end{aligned}$$

and this contradicts our assumption that $n \geq ab - a - b + 1$. So, (x_1, y_1) is a non-negative solution. □

Somewhat surprisingly, if there are three or more stamps, there are no known formulas analogous to those we have when there are two stamps.

1.11 Fermat and Mersenne Numbers

When Euclid proved that there are infinitely many primes, he did so by showing that there cannot be a largest prime number. Nevertheless, there is a long history, going back at least 2000 years ago to the Sieve of Eratosthenes, of finding primes, especially large ones. It is remarkable that this area of mathematics, which was long considered a somewhat recreational academic exercise, has now turned out to have important cryptographic uses. We'll discuss these applications in Chapter 5.

Most of the large primes that are found are too large (and not random enough) for cryptographic applications, but they are often a way to test algorithmic advances. Since exponential functions grow very rapidly, it seems reasonable to look for exponential expressions that take on prime values in order to find large prime numbers. This was the motivation behind the work of some sixteenth century mathematicians, whose ideas on generating large primes still spark our interest today.

The most common function to look at was $2^n - 1$. Primes of this form appear in Euclid's *Elements* in his discussion of perfect numbers (see Chapter 12). Many people have thought that this expression is always prime if n is prime, but Hudalricus Regius, in 1536, seems to have been the first person to realize that $2^{11}-1 = 23 \cdot 89$. (This was before calculators, computers, and the widespread knowledge of algebra. Factoring was very hard and very slow.) Today, numbers of the form

$$M_n = 2^n - 1 \tag{1.15}$$

are called **Mersenne numbers**, after the French monk Marin Mersenne who lived from 1588 to 1648. Mersenne, and others before him, were most likely aware that in order for M_n to be prime, n must be prime. This is the content of the following result.

Proposition 1.18. *If n is composite then $2^n - 1$ is composite.*

Proof. Recall that for every $k \geq 1$,

$$x^k - 1 = (x-1)\left(x^{k-1} + x^{k-2} + x^{k-3} + \cdots + x + 1\right) \tag{1.16}$$

(if we divide both sides of equation (1.16) by $x - 1$, we get the well known formula for a geometric sum; see Appendix A). Since n is composite, $n = ab$ with $1 < a < n$ and $1 < b < n$. Substitute $x = 2^a$ and $k = b$ to get

$$2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right).$$

Since $1 < a < n$, we have $1 < 2^a - 1 < 2^n - 1$, so the factor $2^a - 1$ is nontrivial. This means that $2^{ab} - 1$ is composite. $\square$

The proposition tells us that if we want to find n such that M_n is prime, we should look only at prime values of n. This works well at the beginning:

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127.$$

All of these are primes. However, Hudalricus Regius's example with $n = 11$ shows that if n is prime, M_n may still be composite. Continuing past the case $n = 11$, we find that

$$2^{13} - 1, \quad 2^{17} - 1, \quad 2^{19} - 1$$

are prime, but $2^{23}-1$ is composite. As of 2013, there are 48 values of n for which M_n is known to be prime.

In honor of Mersenne, who made some early (and partly incorrect) lists of values of n that make M_n prime, a prime number of the form M_n is called a *Mersenne prime.*

Because of the special form of Mersenne primes, there are very fast tests (see the Lucas-Lehmer Test in Chapter 10) to determine whether M_n is a prime number. Whenever you read that a new "largest" prime has been discovered, you'll likely see that it's a Mersenne prime. In fact, for much of recent history, the largest known prime has been a Mersenne prime. In 1876, Eduoard Lucas proved that M_{127} is prime, and that remained the largest known prime until 1951, when the non-Mersenne $180(M_{127})^2+1$ became the champion. In 1952, Mersenne primes took back the lead, with M_{521} being proved prime. Subsequently, larger and larger Mersenne primes were discovered through 1985, when M_{216091} became the leader. Then, in 1989 the non-Mersenne $391581 \times 2^{216193}-1$ took over and reigned until 1992, when M_{756839} regained the title for the Mersennes. Since then, the largest known prime has always been Mersenne. As of July 2013, the largest known Mersenne prime was $2^{57885161}-1$. The base 10 expansion of this number has more than 17 million digits. The Great Internet Mersenne Prime Search (GIMPS) is an Internet-based distributed computing project with numerous volunteers using spare time on their computers to carry out the search for Mersenne primes. The 14 most recent Mersenne primes were found by GIMPS.

Instead of looking at 2^n-1, the great French mathematician Pierre de Fermat (1601-1665) examined 2^m+1. Fermat realized that the only way for 2^m+1 to be prime is for the exponent m to be a power of 2.

Proposition 1.19. *If $m>1$ is not a power of 2, then 2^m+1 is composite.*

Proof. If k is odd then

$$x^k+1=(x+1)\left(x^{k-1}-x^{k-2}+x^{k-3}-\cdots-x+1\right).$$

Since m is not a power of 2, it has a nontrivial odd factor: $m=ab$

with a an odd integer and $a \geq 2$. Let $k = a$ and let $x = 2^b$. Then

$$2^{ab} + 1 = (2^b + 1)\left(x^{b(a-1)} - x^{b(a-2)} + x^{b(a-3)} - \cdots - x^b + 1\right).$$

Since $1 \leq b < m$, we have $1 < 2^b + 1 < 2^m + 1$, so the factor $2^b + 1$ is nontrivial. Therefore, $2^{ab} + 1$ is composite. $\square$

The proposition tells us that if we want to find m such that $2^m + 1$ is prime, we should take m to be a power of 2, leading to the definition of the nth Fermat number:

$$F_n = 2^{2^n} + 1.$$

Fermat incorrectly believe that F_n is prime for every integer $n \geq 0$. Although this is true for small values of n:

$$F_0 = 2^1 + 1 = 3, \quad F_1 = 2^2 + 1 = 5, \quad F_2 = 2^4 + 1 = 17,$$
$$F_3 = 2^8 + 1 = 257, \quad F_4 = 2^{16} + 1 = 65537,$$

Euler showed in 1732 that $F_5 = 4294967297 = 641 \cdot 6700417$. More recently, F_n has been factored for $6 \leq n \leq 11$, and many more have been proved to be composite, although they are yet to be factored. Many people now believe that F_n is *never* prime if $n \geq 5$.

Fermat primes occur in compass and straightedge constructions in geometry. Using only a compass and a straightedge, it is easy to make an equilateral triangle or a square. It's a little harder to make a regular pentagon, but it's possible. The constructions of equilateral triangles and regular pentagons can be combined to produce a regular 15-gon. Moreover, by bisecting angles, it's easy to double the number of sides of a polygon that is already constructed, so 30-sided, 60-sided, and 120-sided regular polygons can be constructed. What else can be done? In 1796, just before he turned 19, Gauss discovered how to construct a regular 17-gon. Moreover, his methods (completed by Wantzel) yield the following:

Let $n \geq 3$. A regular n-gon can be constructed by compass and straightedge if and only if n is a power of 2 times a product of distinct Fermat primes:

$$n = 2^a F_{n_1} \cdot F_{n_2} \cdots F_{n_r}$$

with $a \geq 0$ and $r \geq 0$.

As mentioned above, the largest known Fermat prime is 65537. Johann Hermes spent 10 years writing down the explicit construction of a 65537-gon, finishing in 1894. The result is stored in a box in Göttingen.

There are heuristic arguments that predict that the number of Mersenne primes should be infinite while the number of Fermat primes should be finite. Arguments such as the ones we'll give are common in number theory when people want to get a rough idea of what is happening. They are not proofs; instead, they are arguments that point in the direction of what is hoped to be the truth.

Here are the heuristic arguments. The Prime Number Theorem (Theorem 16.11) says that the probability that a randomly chosen integer of size x is prime is approximately $1/\ln x$. Therefore, the probability that $2^p - 1$ is prime is approximately

$$\frac{1}{\ln(2^p - 1)} \geq \frac{1}{\ln(2^p)} = \frac{1}{p \ln 2}.$$

The number of Mersenne primes $2^p - 1$ as p ranges through all primes should be approximately

$$\frac{1}{\ln 2} \sum_p \frac{1}{p} = \infty$$

(the fact that the sum diverges in proved in Chapter 16).

On the other hand, the probability that $2^{2^n} + 1$ is prime should be approximately

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

Since

$$\sum_{n=0}^{\infty} \frac{1}{2^n \ln 2} = \frac{2}{\ln 2} \approx 2.885,$$

the expectation is that the number of Fermat primes is finite. You might have noticed that there are five Fermat primes, while the prediction is for only 2.885. This can be explained by the fact that all the Fermat numbers are odd, and the chance that a random odd number of size x is prime is $2/\ln x$. When we double 2.885, we get a prediction of 5.77, which is closer to the actual count.

1.12 Chapter Highlights

1. Euclid's theorem: There are infinitely many prime numbers.
2. The Euclidean Algorithm for computing gcd's.
3. If $\gcd(a, b) = 1$, then there exist integers x, y with $ax + by = 1$.
4. Finding solutions of linear diophantine equations $ax + by = c$ using the Extended Euclidean Algorithm.

1.13 Problems

1.13.1 Exercises

Section 1.1: Divisibility

1. Show that $5 \mid 120$, $11 \mid 165$, and $14 \mid 98$.
2. Show that $7 \mid 7$, $10 \nmid 25$, and $32 \mid -160$.
3. Find all positive divisors of the following integers:
(a) 20 (b) 52 (c) 195 (d) 203
4. Find all positive divisors of the following integers:
(a) 12 (b) 13 (c) 15 (c) 16
5. Prove or give a counterexample for the following statements:
(a) If $c \mid a$ and $c \mid b$, then $c \mid ab$.
(b) If $c \mid a$ and $c \mid b$, then $c^2 \mid ab$.
(c) If $c \nmid a$ and $c \nmid b$, then $c \nmid (a + b)$.
6. Recall that a number n is even if $n = 2k$ and is odd if $n = 2k + 1$. Prove the following:
(a) The sum of two even numbers is even.
(b) The sum of two odd numbers is even.

(c) The product of two even numbers is even *and* is divisible by 4.
(d) The product of two odd numbers is odd.

7. Find all integers n (positive or negative) such that $n^2 - n$ is prime.

8. Show that if a is any integer, then 3 divides $a^3 - a$.

9. (a) Find all primes p such that $3p + 1$ is a square.
(b) Find all primes such that $5p + 1$ is a square.
(c) Find all primes such that $29p + 1$ is a square.
(d) If we fix a prime p and ask to find all primes q so that $qp + 1$ is a square, what relationship must p and q have if we find a q that works?

10. (a) If $n \geq 2$, show that each of

$$n! + 2,\ n! + 3,\ n! + 4,\ \ldots, n! + n$$

is composite.
(b) Find a list of 100 consecutive composite integers.

11. (a) Find all prime numbers that can be written as a difference of two squares.
(b) Find all prime numbers that can be written as a difference of two fourth powers.

Section 1.2: Euclid's Theorem

12. Let p_k denote the kth prime. Show that

$$p_{n+1} \leq p_1 p_2 p_3 \cdots p_n + 1$$

for all $n \geq 1$.

13. Consider the numbers

$$2 + 1, \quad 2 \cdot 3 + 1, \quad 2 \cdot 3 \cdot 5 + 1, \quad 2 \cdot 3 \cdot 5 \cdot 7 + 1, \quad \cdots .$$

Show, by computing several values, that there are composite numbers in this sequence. (This shows that in the proof of Euclid's theorem, these numbers are not necessarily prime, so it is necessary to look at prime factors of these numbers.)

14. The famous Goldbach Conjecture says that every even integer $n \geq 4$ is a sum of two primes. This conjecture is not yet proved. Prove the weaker statement that there are infinitely many even integers that are sums of two primes.

15. It is conjectured, but not proved, that there is always a prime between every two consecutive squares n^2 and $(n+1)^2$ for $n \geq 1$. Prove the weaker statement that there are infinitely many n such that there is a prime between n^2 and $(n+1)^2$.

Section 1.5: The Division Algorithm

16. For each of the following, find the quotient and remainder when a is divided by b in the Division Algorithm.
(a) $a = 43$, $b = 7$ (b) $a = 96$, $b = 11$,
(c) $a = 140$, $b = 12$ (d) $a = -200$, $b = 21$.

17. For each of the following, find the quotient and remainder when a is divided by b in the Division Algorithm.
(a) $a = 7$, $b = 7$ (b) $a = 9$, $b = 11$,
(c) $a = 246$, $b = 10$ (d) $a = 18$, $b = 3$.

18. When dividing a by b in the Division Algorithm, find the quotient q and remainder r when
(a) $1 \leq a = b$.
(b) $a = kb$, k an integer.
(c) $0 \leq a < b$.

19. Find all integers n (positive, negative, or zero) so that $n^2 + 1$ is divisible by $n + 1$.

20. Find all integers n (positive, negative, or zero) so that $n^3 - 1$ is divisible by $n + 1$.

21. Suppose that a group of 18 billionaires want to see how many in their group are worth 1 billion, how many are worth 2 billion, etc., but they do not want to reveal their individual wealths. The first person chooses a large integer N (around 100 digits) and computes $N + 20^i$, where i is an integer indicating a net worth of i billions (they round off to the nearest billion). This sum, call it N_1, is given to the second person. This second person computes $N_2 = N_1 + 20^j$, where j is an integer indicating a net worth

of j billions. The sum N_2 is given to the third person. This continues until all 18 have added on their numbers. The first person then subtracts N. Show how to determine how many people are worth 0 billion, how many are worth 1 billion, etc.

Section 1.6: The Greatest Common Divisor

22. Evaluate
(a) $\gcd(6, 9)$
(b) $\gcd(10, 14)$
(c) $\gcd(8, -9)$

23. Evaluate
(a) $\gcd(12, 36)$
(b) $\gcd(3, 0)$
(c) $\gcd(6, 7)$

24. Show that if n is an integer then $\gcd(n, n+1) = 1$.

25. Show that if n is an integer then $\gcd(2n-1, 2n+1) = 1$.

26. If $\gcd(a, b) = 1$, prove that $\gcd(a+b, a-b) = 1$ or 2.

27. Show that if $\gcd(a, b) = 1$ and $c \mid a$, then $\gcd(b, c) = 1$.

28. Let a be an integer. Find all possibilities for $\gcd(5a+1, 12a+9)$ (there are four of them). For each possibility, find an integer a such that the gcd has that value. (*Hint:* If d is the gcd, then d divides any combination of the two numbers. Find a combination that gets rid of the a.)

29. Show that $n! + 1$ and $(n+1)! + 1$ are relatively prime. (*Hint:* Try multiplying $n! + 1$ by $n + 1$ and then using various linear combinations.)

30. Let n be an integer.
(a) Show that $\gcd(n^2+n+6, n^2+n+4) = 2$. (*Hint:* n^2+n is always even.)
(b) Show that $\gcd(n^2+n+5, n^2+n+3) = 1$.

Section 1.7: The Euclidean Algorithm

31. Evaluate each of the following and use the Extended Euclidean Algorithm to express each $\gcd(a, b)$ as a linear

combination of a and b.
(a) $\gcd(14, 100)$
(b) $\gcd(6, 84)$
(c) $\gcd(182, 630)$
(d) $\gcd(1776, 1848)$

32. Evaluate each of the following and use the Extended Euclidean Algorithm to express each $\gcd(a, b)$ as a linear combination of a and b.
(a) $\gcd(13, 203)$
(b) $\gcd(57, 209)$
(c) $\gcd(465, 2205)$
(d) $\gcd(1066, 42)$

33. Let n be an integer. Show that $\gcd(n^2, n^2 + n + 1) = 1$.

34. (a) Compute $\gcd(89, 55)$.
(b) If F_n denotes the nth Fibonacci number, describe the quotients and remainders in the Euclidean Algorithm for $\gcd(F_{n+1}, F_n)$.

35. (a) Use the Euclidean Algorithm to compute $\gcd(13, 5)$.
(b) Let $n = 1111111111111$ (that's thirteen 1's) and $m = 11111$. Use the Euclidean Algorithm to compute $\gcd(n, m)$.
(c) Observe the relation between the calculations in (a) and (b). Generalize this to show that if $c = (10^a - 1)/9$ and $d = (10^b - 1)/9$ (so c has a 1's and d has b 1's), then $\gcd(c, d)$ is the number with $\gcd(a, b)$ 1's.

36. Let $a_1, a_2, \ldots, a_n$ be integers (with at least one of them nonzero). Let T be the set of integers of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n,$$

with integers $x_1, x_2, \ldots, x_n$. Use the proof of Theorem 1.11 with appropriate changes to show that $\gcd(a_1, a_2, \ldots, a_n)$ is a linear combination of $a_1, a_2, \ldots, a_n$. (This gives another proof of Theorem 1.12.)

Section 1.8: Other Bases

37. Express the following in base 10:
(a) 1234_5

(b) 10101_2
(c) 111_{11}

38. (a) Convert the base 10 number 54321 to base 6.
(b) Convert the base 10 number 1000000 to base 2.
(c) Convert the base 10 number 31416 to base 7.

Section 1.9: Linear Diophantine Equations

39. For each of the following equations, find all integral solutions or show that it has none.
(a) $3x + 4y = 10$
(b) $5x - 7y = 9$
(c) $9x + 23y = 1$
(d) $4x + 6y = 11$

40. For each of the following equations, find all integral solutions or show that it has none.
(a) $8x + 2y = 26$
(b) $44x - 17y = 9$
(c) $60x + 9y = 31$
(d) $60x + 9y = 51$

41. A farmer pays 1770 crowns in purchasing horses and oxen. He pays 31 crowns for each horse and 21 crowns for each ox. How many horses and oxen did he buy? (This problem is from Euler's *Algebra*, which was published in 1770.)

42. You cash a check at the bank, but the teller accidentally switches the dollars and the cents. The amount you are given is 47 cents more than twice the correct amount. What was the amount on the original check? Assume that the number of dollars and the number of cents are less than 100. (*Hint:* If the original check is for x dollars and y cents, then the check was for $100x + y$. You received $100y + x$.)

43. Let a, b, c be integers with $\gcd(a, b) = 1$ and with $a > 0$ and $b > 0$. Show that

$$ax - by = c$$

has infinitely many solutions in positive integers x, y.

44. You have nickels, dimes, and quarters, for a total of 20 coins. If the total value of the coins is \$2.00, what are the possibilities for the numbers of nickels, dimes, and quarters? (Assume that you have at least one of each type of coin.)

45. An all-you-can-eat restaurant charges \$15 for teenagers and \$13 for adults. At the end of a day, the restaurant had collected \$500. What is the largest number of people who could have eaten there that day? What is the smallest number of people?

Section 1.10: The Postage Stamp Problem

46. (a) Suppose you have only 13-dollar and 7-dollar bills. You need to pay someone 71 dollars. Is this possible without receiving change? If so, show how to do it. If not, explain why it is impossible.
(b) Suppose you need to pay someone 75 dollars. Is this possible? If so, show how to do it. If not, explain why it is impossible.

47. (a) In the Postage Stamp Problem with stamps worth 3 cents and 5 cents, use the fact that 8, 9, and 10 are feasible to show that
    (i) 100 is feasible, (ii) 260 is feasible,
    (iii) 302 is feasible.
(b) If we have stamps of denomination a and b and we can show that the a consecutive numbers $k, k+1, k+2, \ldots, k+a-1$ are feasible, show that every number greater than $k+a-1$ must also be feasible.

Section 1.11: Fermat and Mersenne Numbers

48. Show that if $n > 1$ and a is a positive integer with $a^n - 1$ prime, then $a = 2$ and n is prime. (*Hint:* Look at the proof of Proposition 1.18.)

49. Show that if $n > 1$ and $a \geq 2$ is an integer with $a^n + 1$ prime, then $n = 2^k$ for some $k \geq 0$. (*Hint:* Look at the proof of Proposition 1.19.)

1.13.2 Projects

1. (a) Use the Division Algorithm to show that every odd number is of the form

$$4k + 1 \text{ or } 4k + 3$$

for some integer k.

(b) From (a), every odd prime falls into one of the two sets:

$$S_1 = \{4k + 1 \mid k \text{ is an integer, and } 4k + 1 \text{ is prime}\}$$
$$S_3 = \{4k + 3 \mid k \text{ is an integer, and } 4k + 3 \text{ is prime}\}.$$

It turns out that both of these sets are infinite. Explain why you already know that at least one of them is infinite (without specifying which one).

(c) We'll now show that S_3 is infinite. (In Exercise 58 in Chapter 4, we'll show that S_1 is also infinite.) To do this, we proceed in steps.

(i) Show that the product of elements of S_1 has the form $4k + 1$ for some integer k.

(ii) Suppose that S_3 is finite, and $3, 7, \ldots, p_n$ are *all* the elements in S_3. Show that $N = 4p_1p_2p_3 \cdots p_n - 1$ cannot be divisible by a prime in S_3.

(iii) Use (i) to show that N cannot be a product only of elements of S_1.

(iv) Show that we have a contradiction, and therefore S_3 is infinite.

For more on S_1 and S_3, see the Computer Explorations.

(d) We will see in Chapter 4 (Exercise 58) that a prime divisor of a number of the form $4N^2 + 1$ must be in S_1. Assume this for the moment. Show that S_1 must be infinite. (*Hint:* What should you use as N?)

(e) Let

$$T_1 = \{6k + 1 \mid k \text{ is an integer, and } 6k + 1 \text{ is prime}\}$$
$$T_5 = \{6k + 5 \mid k \text{ is an integer, and } 6k + 5 \text{ is prime}\}.$$

Use the method of (c) to show that T_5 is infinite.

(f) We'll see later (Exercise 23 of Chapter 9) that every prime divisor of a number of the form $N^2 + N + 1$ is 3 or is in T_1. Use this fact to show that T_1 is infinite.

Dirichlet proved in 1837 that if $\gcd(a, b) = 1$ then there are infinitely many primes of the form $ak + b$. His proof is one of the first examples of analytic number theory, where techniques from calculus (in this case, infinite series) are used to prove results about the distribution of prime numbers. One of the key ingredients of his proof is the fact that $\sum 1/p$ (the sum is over all primes) diverges. See Chapter 16 for a proof of this last fact.

2. The Euclidean Algorithm for the greatest common divisor can be visualized in terms of a tiling analogy. Assume that we wish to cover an $a \times b$ rectangle with square tiles exactly, where a is the larger of the two numbers. We first attempt to tile the rectangle using $b \times b$ square tiles; however, this leaves an $r_0 \times b$ rectangle untiled, where $0 \le r_0 < b$. We then attempt to tile the residual rectangle with $r_0 \times r_0$ square tiles. This leaves a second rectangle untiled of size $r_1 \times r_0$, which we attempt to tile using $r_1 \times r_1$ square tiles with $0 \le r_1 < r_0$. We continue with this process, ending when there is no residual rectangle, that is, when the square tiles cover the previous residual rectangle exactly. The length of the sides of the smallest square tile is the gcd of the dimensions of the original rectangle.
(a) Draw a picture for each step in this process when $a = 3$ and $b = 2$.
(b) Draw a picture for each step in this process when $a = 11$ and $b = 8$.
(c) Draw a picture for each step in this process when $a = 8$ and $b = 6$.
(d) Draw a picture for what happens when $a = F_n$ and $b = F_{n-1}$ are successive Fibonacci numbers.

3. Let $a \ge b > 0$. In the Euclidean Algorithm for computing $\gcd(a, b)$, let r_{n-1} be the last nonzero remainder (we may assume that $b \nmid a$, so r_{n-1} exists, since otherwise the conclusion of (e) is trivial).
(a) Let F_k be the kth Fibonacci number (see Appendix

A). Use induction to show that $r_{n-k} \geq F_{k+1}$ for $k = 0, 1, 2, 3, \ldots, n-1$. (*Hint:* We must have $r_{n-2} \geq 2 = F_3$; otherwise, the division by r_{n-2} would leave no remainder.)
(b) Show that $b \geq F_{n+1}$.
(c) Let $\phi = (1+\sqrt{5})/2$ be the Golden Ratio. Use induction to show that $F_k > \phi^{k-2}$ for all $k \geq 1$. (*Hint:* Use the relations $\phi^2 = \phi + 1$ and $F_{k+1} = F_k + F_{k-1}$.)
(d) Show that $\log_{10}(b) > (n-1)/5$.
(e) Suppose that b has m decimal digits. Show that the number of divisions (which is just n) in the Euclidean Algorithm for $\gcd(a, b)$ is at most $5m$.
This result, namely that the number of divisions in the Euclidean Algorithm for two numbers is at most 5 times the number of decimal digits in the smaller number, is known as *Lamé's theorem*. It is generally regarded as the first theorem in the complexity theory of algorithms.

1.13.3 Computer Explorations

1. Define a function on positive integers by

$$f(n) = \begin{cases} n/2 \text{ if } n \text{ is even} \\ 3n+1 \text{ if } n \text{ is odd.} \end{cases}$$

For example, $f(5) = 16$ and $f(6) = 3$. If we start with a positive integer m, we can form the sequence $m_1 = f(m)$, $m_2 = f(m_1)$, $m_3 = f(m_2)$, etc. The *Collatz Conjecture* predicts that we eventually get $m_k = 1$ for some k. For example, if we start with $m = 7$, we get $m_1 = 22$, $m_2 = 11$, $m_3 = 34$, $m_4 = 17$, $m_5 = 52$, $m_6 = 26$, $m_7 = 13$, $m_8 = 40$, $m_9 = 20$, $m_{10} = 10$, $m_{11} = 5, m_{12} = 16$, $m_{13} = 8$, $m_{14} = 4$, $m_{15} = 2$, $m_{16} = 1$.
(a) Show that the Collatz Conjecture is true for all $m \leq 60$. Which starting value of m required the most steps?
(b) Suppose you change $3n+1$ to $n+1$ in the definition of $f(n)$. What happens? Can you prove this?
(c) Suppose you change $3n+1$ to $5n+1$ in the definition of $f(n)$. Try a few examples and see what happens. Do

you see a different behavior for starting values $m = 5$, $m = 6$, and $m = 7$?

2. Let $\pi_{n,a}(x)$ be the number of primes of the form $nk + a$ that are less than or equal to x. For example, $\pi_{4,3}(20) = 4$ since it is counting the primes $3, 7, 11, 19$.
(a) Let $\pi(x)$ be the number of primes less than or equal to x. Compute the ratios
$$\frac{\pi_{4,1}(x)}{\pi(x)} \text{ and } \frac{\pi_{4,3}(x)}{\pi(x)}$$
for $x = 1000$, $x = 100000$, and $x = 1000000$. Make a guess as to what each ratio approaches as x gets larger and larger.
(b) Show that $\pi_{4,1}(x) \leq \pi_{4,3}(x)$ for all integers $x < 30000$ except for two (consecutive) integers x. This comparison is sometimes called a "prime number race." Chebyshev observed in 1853 that usually $\pi_{4,3}(x)$ is ahead of $\pi_{4,1}(x)$, but Littlewood showed in 1914 that the lead changes infinitely often. In 1994, Rubinstein and Sarnak showed (under some yet-to-be-proved assumptions) that $\pi_{4,3}(x)$ is ahead most of the time.

3. Find 20 examples of numbers that are sixth powers. What is true about the remainders when these sixth powers are divided by 7? Can you make a conjecture and then prove it?

4. Write a program that generates 10000 "random" pairs (a, b) of integers, and then use the Euclidean Algorithm (or your software gcd routine) to decide whether $\gcd(a, b) = 1$. If m is the number of pairs that are relatively prime, calculate
$$\frac{m}{10000},$$
which is the fraction of these pairs that are relatively prime. Follow the same procedure for 10^5 pairs and then 10^6 pairs. Can you make a guess a guess as to what number this ratio approaches? (*Hint:* It is an integer divided by π^2.)

5. By Exercise 10 above, there are arbitrarily long sequences of consecutive composite numbers. Find the first string of (at least) 10 consecutive composites, of (at least) 50 consecutive composites, and of (at least) 100 consecutive composites. How do these numbers compare in size to the numbers used in Exercise 10?

6. (a) Show that $n^4 + 4$ is composite for several values of $n \geq 2$. There is a reason for this. Let's find it.
(b) Show that in each example in (a), $n^4 + 4$ always can be factored as $a \times b$, where $a - b = 4n$.
(c) Write $a = x + 2n$ and $b = x - 2n$ for some x. Use $n^4 + 4 = ab$ to find x and then find the numbers a and b.

1.13.4 Answers to "CHECK YOUR UNDERSTANDING"

1. Since $1001 = 7 \times 143$, we have $7 \mid 1001$.

2. Since $1005 = 7 \times 143 + 4$, 1005 is not a multiple of 7.

3. Suppose $5 \mid 2 \cdot 3 \cdot 5 \cdot 7 + 1$. Since $5 \mid 2 \cdot 3 \cdot 5 \cdot 7$, Corollary 1.4 says that $5 \mid (2 \cdot 3 \cdot 5 \cdot 7 + 1) - (2 \cdot 3 \cdot 5 \cdot 7) = 1$, which is not true. Therefore, $5 \nmid 2 \cdot 3 \cdot 5 \cdot 7 + 1$.

4. We have to use only the primes less than $\sqrt{20} \approx 4.5$, so 2 and 3 suffice. After crossing out 1 and the multiples of 2, the numbers that remain are 2, 3, 5, 7, 9, 11, 13, 15, 17, 19. Of these, 3 crosses out 9 and 15. The numbers 2, 3, 5, 7, 11, 13, 17, 19 remain and are the primes less than 20.

5. Divide 7 into 200. The quotient is $q = 28$ and the remainder is $r = 4$, so $200 = 7 \cdot 28 + 4$.

6. We get $-200 = 7 \cdot (-28) - 4$, but we want $0 \leq r < 7$. Therefore, we write $-200 = 7 \cdot (-29) + 3$, so $q = -29$ and $r = 3$.

7. The divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24. The largest of these that divides 42 is 6, so $\gcd(24, 42) = 6$.

8. Since $60 = 2^2 \cdot 3 \cdot 5$, we need n to be odd and not a multiple of 3 or 5. The only n between 1 and 10 that satisfies these requirements is $n = 7$.

9. If $d \mid n$ and $d \mid n+3$, then $d \mid (n+3)-n=3$. Therefore, $d=1$ or 3, so any common divisor is either 1 or 3. If $n=1$, then $\gcd(1,4)=1$, so $d=1$ occurs. If $n=3$, then $\gcd(3,6)=3$, so $d=3$ occurs.
10. Use the Euclidean Algorithm:

$$\begin{aligned} 654 &= 2 \cdot 321 + 12 \\ 321 &= 26 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Therefore, $3 = \gcd(654, 321)$.

11. Use the Extended Euclidean Algorithm:

	x	y	
17	1	0	
12	0	1	
5	1	-1	(1st row) $-$(2nd row)
2	-2	3	(2nd row) $-$ 2$\cdot$(3rd row)
1	5	-7	(3rd row) $-$ 2$\cdot$(4th row).

The end result is $1 = 17 \cdot 5 - 12 \cdot 7$, so $x=5$ and $y=-7$.

12. Use the Division Algorithm:

$$\begin{array}{rcll} 1234 & = & 176 \cdot 7 & + \ 2 \\ 176 & = & 25 \cdot 7 & + \ 1 \\ 25 & = & 3 \cdot 7 & + \ 4 \\ 3 & = & 0 \cdot 7 & + \ 3. \end{array}$$

Therefore, $1234_{10} = 3412_7$.

13. $321_5 = 3 \cdot 5^2 + 2 \cdot 5 + 1 = 75 + 10 + 1 = 86$.
14. Use Theorem 1.14. Trial and error, for example, yields the solution $(x_0, y_0) = (-2, 2)$. Since $b/\gcd(a,b) = 8/2 = 4$ and $a/\gcd(a,b) = 6/2 = 3$, all solutions are given by

$$x = -2 + 4t, \qquad y = 2 - 3t,$$

where t is an integer (there are similar solutions corresponding to other choices of (x_0, y_0)).

Appendix B

Answers and Hints for Odd-Numbered Exercises

Chapter 1

1. These use the definition of divisibility: $120 = 5 \cdot 24$, $165 = 11 \cdot 15$, $98 = 14 \cdot 7$.
3. (a) 1, 2, 4, 5, 10, 20
   (b) 1, 2, 4, 13, 26, 52
   (c) 1, 3, 5, 13, 15, 39, 65, 195
   (d) 1, 7, 29, 203
5. (a) True: If $c \mid a$ then there exists j with $a = cj$. Therefore, $ab = c(jb)$, which says that $c \mid ab$.
   (b) True: If $c \mid a$ and $c \mid b$, there exist j and k with $a = cj$ and $b = ck$. Therefore, $ab = c^2(jk)$, which means that $c^2 \mid ab$.
   (c) False: Let $c = 4$, $a = 1$, $b = 7$. Then $c \nmid a$, $c \nmid b$, but $c \mid a + b$.
7. Note that $n^2 - n = n(n-1)$. If this is a prime, we must have $n = \pm 1$ or $n - 1 = \pm 1$. These give $n^2 - n = 0, 2, 2, 0$. Therefore, $n = -1$ and $n = 2$ make $n^2 - n$ prime.
9. (a) $p = 5$, (b) $p = 3, 7$, (c) $p = 31$, (d) $|p - q| = 2$
11. (a) All odd primes, (b) None
13. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$, $\quad 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 19 \cdot 97 \cdot 277$
15. For each prime p, there is an n with $n^2 < p < (n+1)^2$. Suppose there is a largest such n, call it N. Then all primes are less than $(N+1)^2$, which contradicts Euclid's theorem. Therefore, there are infinitely many such n.
17. (a) quotient = 1, remainder = 0, (b) quotient = 0, remainder = 9, (c) quotient = 24, remainder = 6, (d) quotient = 6, remainder = 0
19. $n = -3, -2, 0, 1$
21. Expand the final number in base 20: $a_0 + a_1 20 + a_2 20^2 + \cdots$. Then a_i is the number of people worth i billion.
23. (a) 12, (b) 3, (c) 1
25. Let $d = \gcd(2n-1, 2n+1)$. Then $d \mid (2n+1) - (2n-1)$.
27. Let $d = \gcd(b, c)$. Then $d \mid c$, so $d \mid a$. Also, $d \mid b$.

29. $(n+1)(n!+1) - ((n+1)!+1) = n$, so $\gcd(n!+1, (n+1)!+1)$ divides n and $n!+1$.

31. (a) $2 = 14\cdot(-7)+100$, (b) $6 = 6\cdot 1+84\cdot 0$, (c) $14 = 630\cdot(-2)+182\cdot 7$, (d) $24 = 1848\cdot 25+1776\cdot(-26)$

33. Let $d = \gcd(n^2, n^2+n+1)$. Then $d \mid (n^2+n+1)^2_n$, so $d \mid n+1$ and therefore $d \mid (n+1)(n-1) = n^2-1$.

35. (a) $13 = 2\cdot 5+3$, $5 = 1\cdot 3+2$, $3 = 1\cdot 2+1$, $2 = 2\cdot 1+0$
(b) $1111111111111 = 100001000\cdot 11111+111$, $11111 = 100\cdot 111+11$, $111 = 10\cdot 11+1$, $11 = 11\cdot 1+0$
(c) If $a = bq+r$ with $r > 0$, then $c = dQ+R$, where Q is q ones, each separated by $b-1$ zeros, and the last 1 is followed by r zeros; and R is r ones.

37. (a) 194, (b) 21, (c) 133

39. (a) $x = 2+4t, y = 1-3t$, (b) $x = 6-7t, y = 3-5t$,
(c) $x = -5+23t, y = 2-9t$, (d) No solutions

41. (horses, oxen) = (51, 9), or (30, 40), or (9, 71)

43. Because $\gcd(a,b) = 1$, there is a solution x_0, y_0 with integers that are not necessarily positive. The general solution of $ax - by = c$ is $x = x_0 - bt, y = y_0 - at$. Let t be a large negative number.

45. largest = 38, smallest = 34.

47. (a) (i) Use the solution for 10 and then add thirty 3-cent stamps
(ii) Use the solution for 8 and then add eighty-four 3-cent stamps.
(iii) Use the solution for 8 and then add ninety-eight 3-cent stamps.
(b) Every number greater than $k+a-1$ differs from a number on the list by a positive multiple of a.

49. If $n = rs$ with an odd number $r > 1$, then a^n+1 has a^s+1 as a factor.

Chapter 2

1. (a) $3^2\cdot 5^4$, (b) 5625 is a square

3. Use Theorem 2.2 with $a = b$.

5. (a) Write $a = 2^{a_2}3^{a_3}\cdots$ and $b = 2^{b_2}3^{b_3}\cdots$. By Proposition 2.6, $na_p \le nb_p$ for each p. Use Proposition 2.6 again to get $a \mid b$.
(b) Write $a = 2^{a_2}3^{a_3}\cdots$ and $b = 2^{b_2}3^{b_3}\cdots$. Proposition 2.6 says that $ma_p \le nb_p$ for each p. Use Proposition 2.6 again to get $a \mid b$.
(c) Let $a = 4, b = 2, m = 1, n = 2$.

7. $d \mid c$, so $d \mid a+b$. Since $d \mid a$, we have $d \mid b$.

9. The answer is 3: If we have four consecutive integers, one of them is divisible by 4. An example of three consecutive squarefree integers is 1, 2, 3.

11. Let $n = 2^{n_2}3^{n_3}\cdots$. Then $r = n_2$ and $m = 3^{n_3}\cdots$.

13. (a) p^3, (b) p