

Introduction to Higher Mathematics
Unit #4: Number Theory

Joseph H. Silverman

Version Date: January 2, 2020

Contents

| | | |
|----------|--|-----------|
| 1 | Number Theory — Lecture #1 | 1 |
| 1.1 | What is Number Theory? | 1 |
| 1.2 | Square Numbers and Triangle Numbers | 5 |
| | Exercises | 10 |
| 2 | Number Theory — Lecture #2 | 13 |
| 2.1 | Pythagorean Triples | 13 |
| 2.2 | Pythagorean Triples and the Unit Circle | 18 |
| | Exercises | 20 |
| 3 | Number Theory — Lecture #3 | 23 |
| 3.1 | Divisibility and the Greatest Common Divisor | 23 |
| 3.2 | Linear Equations and Greatest Common Divisors | 27 |
| | Exercises | 32 |
| 4 | Number Theory — Lecture #4 | 37 |
| 4.1 | Primes and Divisibility | 37 |
| 4.2 | The Fundamental Theorem of Arithmetic | 40 |
| | Exercises | 43 |
| 5 | Number Theory — Lecture #5 | 45 |
| 5.1 | Congruences | 45 |
| 5.2 | Congruences, Powers, and Fermat's Little Theorem | 49 |
| | Exercises | 54 |
| 6 | Number Theory — Lecture #6 | 57 |
| 6.1 | Prime Numbers | 57 |
| 6.2 | Counting Primes | 61 |
| | Exercises | 65 |
| 7 | Number Theory — Lecture #7 | 69 |
| 7.1 | The Fibonacci Sequence | 69 |
| 7.2 | The Fibonacci Sequence Modulo m | 75 |
| 7.3 | The Fibonacci Sequence: Supplement | 76 |

| | |
|--|------------|
| CONTENTS | 3 |
| Exercises | 78 |
| 8 Number Theory — Lecture #8 | 83 |
| 8.1 Squares Modulo p | 83 |
| Exercises | 88 |
| 9 Number Theory — Lecture #9 | 91 |
| 9.1 Is -1 a Square Modulo p ? Is 2 ? | 91 |
| 9.2 Quadratic Reciprocity to the Rescue | 99 |
| 9.3 Proof that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ [Supplement] | 102 |
| Exercises | 105 |
| A Class Exercise: Lecture #1: Mix and Match Number Types | 107 |
| B Class Exercise: Lecture #2: Pythagorean-Like Triples | 108 |
| C Class Exercise: Lecture #3: Least Common Multiples | 109 |
| D Class Exercise: Lecture #4: Further Travels in the \mathbb{E}-Zone | 110 |
| E Class Exercise: Lecture #5: Polynomial Roots Modulo m | 111 |
| F Class Exercise: Lecture #6: Sums of Reciprocals | 112 |
| G Class Exercise: Lecture #7: The $3n + 1$ Problem | 113 |
| H Class Exercise: Lecture #8: Cubes Modulo p | 115 |
| I Class Exercise: Lecture #9: | 116 |

Chapter 1

Number Theory — Lecture #1

1.1 What is Number Theory?

Number theory is the study of the set of positive whole numbers

$$1, 2, 3, 4, 5, 6, 7, \dots,$$

which are often called the set of *natural numbers*. We will especially want to study the *relationships* between different sorts of numbers. Since ancient times, people have separated the natural numbers into a variety of different types. Here are some familiar and not-so-familiar examples:

| | |
|--------------|---|
| odd | 1, 3, 5, 7, 9, 11, ... |
| even | 2, 4, 6, 8, 10, ... |
| square | 1, 4, 9, 16, 25, 36, ... |
| cube | 1, 8, 27, 64, 125, ... |
| prime | 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... |
| composite | 4, 6, 8, 9, 10, 12, 14, 15, 16, ... |
| 1 (modulo 4) | 1, 5, 9, 13, 17, 21, 25, ... |
| 3 (modulo 4) | 3, 7, 11, 15, 19, 23, 27, ... |
| triangular | 1, 3, 6, 10, 15, 21, ... |
| perfect | 6, 28, 496, ... |
| Fibonacci | 1, 1, 2, 3, 5, 8, 13, 21, ... |

Many of these types of numbers are undoubtedly already known to you. Others, such as the “modulo 4” numbers, may not be familiar. A number is said to be congruent to 1 (modulo 4) if it leaves a remainder of 1 when divided by 4, and similarly for the 3 (modulo 4) numbers. A number is called triangular if that number of pebbles can be arranged in a triangle, with one pebble at the top, two pebbles in the next row, and so on. The Fibonacci numbers are created by starting with 1 and 1. Then, to get the next number in the list, just add the previous two. Finally, a number is perfect if the sum of all its divisors, other than itself, adds back up to the original number. Thus, the numbers dividing 6 are 1, 2, and 3, and $1 + 2 + 3 = 6$. Similarly,

the divisors of 28 are 1, 2, 4, 7, and 14, and

$$1 + 2 + 4 + 7 + 14 = 28.$$

We will encounter many of these types of numbers in our excursion through the Theory of Numbers.

Some Typical Number Theoretic Questions

The main goal of number theory is to discover interesting and unexpected relationships between different sorts of numbers and to prove that these relationships are true. In this section we describe a few typical number theoretic problems, some of which we will eventually solve, some of which have known solutions too difficult for us to include, and some of which remain unsolved to this day.

Sums of Squares I. Can the sum of two squares be a square? The answer is clearly “YES”; for example $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. These are examples of *Pythagorean triples*. We will describe all Pythagorean triples in Chapter 2.

Sums of Higher Powers. Can the sum of two cubes be a cube? Can the sum of two fourth powers be a fourth power? In general, can the sum of two n^{th} powers be an n^{th} power? The answer is “NO.” This famous problem, called *Fermat’s Last Theorem*, was first posed by Pierre de Fermat in the seventeenth century, but was not completely solved until 1994 by Andrew Wiles. Wiles’s proof uses sophisticated mathematical techniques far beyond what we will be able to cover.

Infinitude of Primes. A *prime number* is a number p whose only factors are 1 and p .

- Are there infinitely many prime numbers?
- Are there infinitely many primes that are 1 modulo 4 numbers?
- Are there infinitely many primes that are 3 modulo 4 numbers?

The answer to all these questions is “YES.” We will prove some of these facts in Chapter 6, as well as stating a much more general result proved by Lejeune Dirichlet in 1837.

Sums of Squares II. Which numbers are sums of two squares? It often turns out that questions of this sort are easier to answer first for primes, so we ask which (odd) prime numbers are a sum of two squares. For example,

$$\begin{array}{llll} 3 = \text{NO}, & 5 = 1^2 + 2^2, & 7 = \text{NO}, & 11 = \text{NO}, \\ 13 = 2^2 + 3^2, & 17 = 1^2 + 4^2, & 19 = \text{NO}, & 23 = \text{NO}, \\ 29 = 2^2 + 5^2, & 31 = \text{NO}, & 37 = 1^2 + 6^2, & \dots \end{array}$$

Do you see a pattern? Possibly not, since this is only a short list, but a longer list leads to the conjecture that p is a sum of two squares if it is congruent to 1

(modulo 4). In other words, p is a sum of two squares if it leaves a remainder of 1 when divided by 4, and it is not a sum of two squares if it leaves a remainder of 3.

Number Shapes. The square numbers are the numbers 1, 4, 9, 16, ... that can be arranged in the shape of a square. The triangular numbers are the numbers 1, 3, 6, 10, ... that can be arranged in the shape of a triangle. The first few triangular and square numbers are illustrated in Figure 1.1.

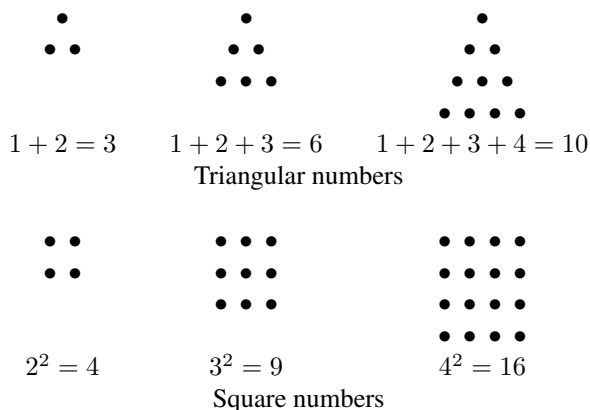


Figure 1.1: Numbers That Form Interesting Shapes

A natural question to ask is whether there are any triangular numbers that are also square numbers (other than 1). The answer is “YES,” the smallest example being

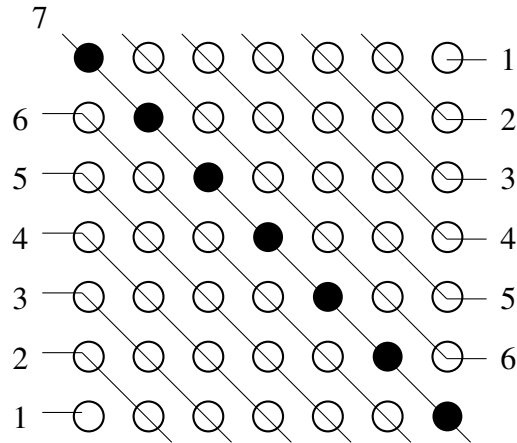
$$36 = 6^2 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8.$$

So we might ask whether there are more examples and, if so, are there infinitely many? To search for examples, the following formula is helpful:

$$1 + 2 + 3 + \cdots + (n - 1) + n = \frac{n(n + 1)}{2}. \quad (1.1)$$

There is an amusing anecdote associated with this formula. One day when the young Carl Friedrich Gauss (1777–1855) was in grade school, his teacher became so incensed with the class that he set them the task of adding up all the numbers from 1 to 100. As Gauss’s classmates dutifully began to add, Gauss walked up to the teacher and presented the answer, 5050. The story goes that the teacher was neither impressed nor amused, but there’s no record of what the next make-work assignment was!

Here is an easy geometric way to verify Gauss’s formula, which might be the way that he discovered it himself. The idea is to take two triangles consisting of $1 + 2 + \cdots + n$ pebbles and fit them together with one additional diagonal of $n + 1$ pebbles. Figure 1.2 illustrates this idea for $n = 6$.



$$(1 + 2 + 3 + 4 + 5 + 6) + 7 + (6 + 5 + 4 + 3 + 2 + 1) = 7^2$$

Figure 1.2: The Sum of the First n Integers

In Figure 1.2, we have marked the extra $n + 1 = 7$ pebbles on the diagonal with black dots. The resulting square has sides consisting of $n + 1$ pebbles, so in mathematical terms we obtain the formula

$$\begin{array}{ccc} 2(1 + 2 + 3 + \cdots + n) + (n + 1) & = & (n + 1)^2, \\ \text{two triangles} & + \text{diagonal} = & \text{square.} \end{array}$$

Now we can subtract $n + 1$ from each side and divide by 2 to get Gauss's formula.

Twin Primes. In the list of primes it is sometimes true that consecutive odd numbers are both prime. We have boxed these *twin primes* in the following list of primes less than 100:

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

Are there infinitely many twin primes? That is, are there infinitely many prime numbers p such that $p + 2$ is also a prime? At present, no one knows the answer to this question.

Primes of the Form $N^2 + 1$. If we list the numbers of the form $N^2 + 1$ taking $N = 1, 2, 3, \dots$, we find that some of them are prime. Of course, if N is odd, then $N^2 + 1$ is even, so it won't be prime unless $N = 1$. So it's really only interesting to take even values of N . We've highlighted the primes in the following list:

$$\begin{array}{llll}
2^2 + 1 = \mathbf{5} & 4^2 + 1 = \mathbf{17} & 6^2 + 1 = \mathbf{37} & 8^2 + 1 = 65 = 5 \cdot 13 \\
10^2 + 1 = \mathbf{101} & 12^2 + 1 = 145 = 5 \cdot 29 & 14^2 + 1 = \mathbf{197} & \\
16^2 + 1 = \mathbf{257} & 18^2 + 1 = 325 = 5^2 \cdot 13 & 20^2 + 1 = \mathbf{401} &
\end{array}$$

It looks like there are quite a few prime values, but if you take larger values of N you will find that they become much rarer. So we ask whether there are infinitely many primes of the form $N^2 + 1$. Again, no one presently knows the answer to this question.

We have now seen some of the types of questions that are studied in the Theory of Numbers. How does one attempt to answer these questions? The answer is that Number Theory is partly experimental and partly theoretical. The experimental part normally comes first; it leads to questions and suggests ways to answer them. The theoretical part follows; in this part one tries to devise an argument that gives a conclusive answer to the questions. In summary, here are the steps to follow:

1. Accumulate data, usually numerical, but sometimes more abstract in nature.
2. Examine the data and try to find patterns and relationships.
3. Formulate conjectures (i.e., guesses) that explain the patterns and relationships. These are frequently given by formulas.
4. Test your conjectures by collecting additional data and checking whether the new information fits your conjectures.
5. Devise an argument (i.e., a proof) that your conjectures are correct.

All five steps are important in number theory and in mathematics. More generally, the scientific method always involves at least the first four steps. Be wary of any purported “scientist” who claims to have “proved” something using only the first three. Given any collection of data, it’s generally not too difficult to devise numerous explanations. The true test of a scientific theory is its ability to predict the outcome of experiments that have not yet taken place. In other words, a scientific theory only becomes plausible when it has been tested against new data. This is true of all real science. In mathematics one requires the further step of a proof, that is, a logical sequence of assertions, starting from known facts and ending at the desired statement.

1.2 Square Numbers and Triangle Numbers

Some numbers are “shapely” in that they can be laid out in some sort of regular shape. For example, a *square number* n^2 can be arranged in the shape of an n -by- n square. Similarly, a *triangular number* is a number that can be arranged in the shape of a triangle. Figure 1.1 on page 3 illustrates the first few triangular and square numbers (other than 1). Triangular numbers are formed by adding

$$1 + 2 + 3 + \cdots + m$$

for different values of m , and we already found a formula for the m^{th} triangular number,

$$1 + 2 + 3 + \cdots + m = \frac{m(m+1)}{2}.$$

Here's a list of the first few triangular and square numbers.

Triangular Numbers 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105

Square Numbers 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169

We earlier posed the problem of trying to

“Square the Triangle”

In other words, can we find square numbers that are also triangular numbers. Even our short list reveals two examples, 1 (which isn't very interesting) and 36. This means that 36 pebbles can be arranged in the shape of a 6-by-6 square, and they can also be arranged in the shape of a triangle with 8 rows. A further search reveals some additional examples of square-triangular numbers, and we might ask how many there are. How might we find all of them?

Triangular numbers look like $m(m+1)/2$ and square numbers look like n^2 , so square-triangular numbers come from solutions to the equation

$$n^2 = \frac{m(m+1)}{2}$$

with positive integers n and m . If we multiply both sides by 8, we get

$$8n^2 = 4m^2 + 4m. \quad (1.2)$$

Do you remember the process of “completing the square” that is used to derive the quadratic formula? We're going to use that on the right-hand side of our equation. What number do we have to add to $4m^2 + 4m$ to make it a perfect square? Well, $4m^2 + 4m$ looks a lot like $(2m+1)^2$, so adding 1 to both sides of (1.2) gives

$$8n^2 + 1 = 4m^2 + 4m + 1 = (2m+1)^2.$$

Since $8n^2 = 2(2n)^2$, this suggests that we make the substitution

$$x = 2m+1 \quad \text{and} \quad y = 2n,$$

which gives the equation

$$2y^2 + 1 = x^2.$$

It is convenient to rearrange this into the form

$$x^2 - 2y^2 = 1. \quad (1.3)$$

To recapitulate, positive integer solutions (x, y) to the equation (1.3) give square–triangular numbers by taking¹

$$m = \frac{x-1}{2} \quad \text{and} \quad n = \frac{y}{2}.$$

By trial and error we notice one solution, $(x, y) = (3, 2)$, which gives the square–triangular number 1 coming from $(m, n) = (1, 1)$. With a little more experimentation, or using the fact that we know that 36 is square–triangular, we find another solution $(x, y) = (17, 12)$ corresponding to $(m, n) = (8, 6)$. Using a computer, we can search for more solutions by substituting $y = 1, 2, 3, \dots$ and checking if $1 + 2y^2$ is a square. The next solution found is $(x, y) = (99, 70)$, which gives us a new square–triangular number with $(m, n) = (49, 35)$. In other words, 1225 is a square–triangular number, since

$$35^2 = 1225 = 1 + 2 + 3 + \dots + 48 + 49.$$

1.2.1 Solving $x^2 - 2y^2 = 1$ by Factorization [Supplement]

What tools can we use to solve the equation

$$x^2 - 2y^2 = 1?$$

Here is an idea based on factorization. Unfortunately, $x^2 - 2y^2$ does not factor if we stay within the realm of whole numbers; but if we expand our horizons a little, it does factor as

$$x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2}).$$

For example, our solution $(x, y) = (3, 2)$ can be written as

$$1 = 3^2 - 2 \cdot 2^2 = (3 + 2\sqrt{2})(3 - 2\sqrt{2}).$$

Now see what happens if we square the left-hand and right-hand sides of this equation.

$$\begin{aligned} 1 = 1^2 &= (3 + 2\sqrt{2})^2 (3 - 2\sqrt{2})^2 \\ &= (17 + 12\sqrt{2})(17 - 12\sqrt{2}) \\ &= 17^2 - 2 \cdot 12^2 \end{aligned}$$

So by “squaring” the solution $(x, y) = (3, 2)$, we have constructed the next solution $(x, y) = (17, 12)$.

This process can be repeated to find more solutions. Thus, cubing the $(x, y) = (3, 2)$ solution gives

¹Wait, you may object, if y is odd or x is even, then m or n won’t be an integer. However, it turns out that this cannot happen, a fact that you will verify in Exercise 1.6.

$$\begin{aligned}
1 &= 1^3 = (3 + 2\sqrt{2})^3 (3 - 2\sqrt{2})^3 \\
&= (99 + 70\sqrt{2}) (99 - 70\sqrt{2}) \\
&= 99^2 - 2 \cdot 70^2,
\end{aligned}$$

and taking the fourth power gives

$$\begin{aligned}
1 &= 1^4 = (3 + 2\sqrt{2})^4 (3 - 2\sqrt{2})^4 \\
&= (577 + 408\sqrt{2}) (577 - 408\sqrt{2}) \\
&= 577^2 - 2 \cdot 408^2.
\end{aligned}$$

Notice that the fourth power gives us a new square–triangular number, $(m, n) = (288, 204)$. When doing computations of this sort, it's not necessary to raise the original solution to a large power. Instead, we can just multiply the original solution by the current one to get the next one. Thus, to find the fifth-power solution, we multiply the original solution $3 + 2\sqrt{2}$ by the fourth-power solution $577 + 408\sqrt{2}$. This gives

$$(3 + 2\sqrt{2}) (577 + 408\sqrt{2}) = 3363 + 2378\sqrt{2},$$

and from this we read off the fifth-power solution $(x, y) = (3363, 2378)$. Continuing in this fashion, we can construct a list of square–triangular numbers.

| x | y | $m = \frac{x-1}{2}$ | $n = \frac{y}{2}$ | $n^2 = \frac{m(m+1)}{2}$ |
|--------|--------|---------------------|-------------------|--------------------------|
| 3 | 2 | 1 | 1 | 1 |
| 17 | 12 | 8 | 6 | 36 |
| 99 | 70 | 49 | 35 | 1225 |
| 577 | 408 | 288 | 204 | 41616 |
| 3363 | 2378 | 1681 | 1189 | 1413721 |
| 19601 | 13860 | 9800 | 6930 | 48024900 |
| 114243 | 80782 | 57121 | 40391 | 1631432881 |
| 665857 | 470832 | 332928 | 235416 | 55420693056 |

As you see, these square–triangular numbers get quite large.

By raising $3 + 2\sqrt{2}$ to higher and higher powers, we can find more and more solutions to the equation

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

which gives us an inexhaustable supply of square–triangular numbers. We have proven:

Theorem 1.1. *There are infinitely many square–triangular numbers.*

This answers our original question, but raises a new question.² Do we get all square-triangular numbers by taking powers of $3 + 2\sqrt{2}$. The answer is yes.

Theorem 1.2 (Square–Triangular Number Theorem). **(a)** *Every solution in positive integers to the equation*

$$x^2 - 2y^2 = 1$$

is obtained by raising $3 + 2\sqrt{2}$ to powers. That is, the solutions (x_k, y_k) can all be found by multiplying out

$$x_k + y_k\sqrt{2} = \left(3 + 2\sqrt{2}\right)^k \quad \text{for } k = 1, 2, 3, \dots$$

(b) *Every square–triangular number $n^2 = \frac{1}{2}m(m+1)$ is given by*

$$m = \frac{x_k - 1}{2} \quad n = \frac{y_k}{2} \quad \text{for } k = 1, 2, 3, \dots,$$

where the (x_k, y_k) 's are the solutions from (a).

Proof. Unfortunately, we won't have time to do the proof, which is fairly intricate. But if you're interested, you can find a proof in most elementary number theory textbooks of a more general result for the equation $x^2 - Dy^2 = 1$, which is called Pell's equation. \square

1.2.2 How Big are Square-Triangular Numbers? [Supplement]

The Square–Triangular Number Theorem says that every solution (x_k, y_k) in positive integers to the equation

$$x^2 - 2y^2 = 1$$

can be obtained by multiplying out

$$x_k + y_k\sqrt{2} = \left(3 + 2\sqrt{2}\right)^k \quad \text{for } k = 1, 2, 3, \dots$$

The table at the beginning of this chapter makes it clear that the size of the solutions grows very rapidly as k increases. We'd like to get a more precise idea of just how large the k^{th} solution is. To do this, we note that the preceding formula is still correct if we replace $\sqrt{2}$ by $-\sqrt{2}$. In other words, it's also true that

$$x_k - y_k\sqrt{2} = \left(3 - 2\sqrt{2}\right)^k \quad \text{for } k = 1, 2, 3, \dots$$

Now if we add these two formulas together and divide by 2, we obtain a formula for x_k :

$$x_k = \frac{\left(3 + 2\sqrt{2}\right)^k + \left(3 - 2\sqrt{2}\right)^k}{2}.$$

²That's a hallmark of good mathematics: Solving the original problems raises new, and often even more interesting, problems to investigate!

Similarly, if we subtract the second formula from the first and divide by $2\sqrt{2}$, we get a formula for y_k :

$$y_k = \frac{(3 + 2\sqrt{2})^k - (3 - 2\sqrt{2})^k}{2\sqrt{2}}.$$

These formulas for x_k and y_k are useful because

$$3 + 2\sqrt{2} \approx 5.82843 \quad \text{and} \quad 3 - 2\sqrt{2} \approx 0.17157.$$

The fact that $3 - 2\sqrt{2}$ is less than 1 means that when we take a large power of $3 - 2\sqrt{2}$, we'll get a very tiny number. For example,

$$(3 - 2\sqrt{2})^{10} \approx 0.0000000221,$$

so

$$\begin{aligned} x_{10} &\approx \frac{(3 + 2\sqrt{2})^{10}}{2} \approx 22619536.99999998895 \quad \text{and} \\ y_{10} &\approx \frac{(3 + 2\sqrt{2})^{10}}{2\sqrt{2}} \approx 15994428.000000007815. \end{aligned}$$

But we know that x_{10} and y_{10} are integers, so the 10th solution is

$$(x_{10}, y_{10}) = (22619537, 15994428).$$

Using this we find that the 10th square-triangular number $n^2 = m(m + 1)/2$ is given by

$$n = 7997214 \quad \text{and} \quad m = 11309768.$$

It's also apparent from the formulas for x_k and y_k why the solutions grow so rapidly, since

$$x_k \approx \frac{1}{2}(5.82843)^k \quad \text{and} \quad y_k \approx \frac{1}{2\sqrt{2}}(5.82843)^k.$$

Thus, each successive solution is more than five times as large as the previous one. Mathematically, we say that the size of the solutions grows *exponentially*. Later we'll see a similar growth rate for the Fibonacci sequence.

Exercises

1.1. Try adding up the first few odd numbers and see if the numbers you get satisfy some sort of pattern. Once you find the pattern, express it as a formula. Give a geometric verification that your formula is correct.

1.2. The consecutive odd numbers 3, 5, and 7 are all primes. Are there infinitely many such "prime triplets"? That is, are there infinitely many prime numbers p such that $p + 2$ and $p + 4$ are also primes?

1.3. It is generally believed that infinitely many primes have the form $N^2 + 1$, although no one knows for sure.

- (a) Do you think that there are infinitely many primes of the form $N^2 - 1$?
- (b) Do you think that there are infinitely many primes of the form $N^2 - 2$?
- (c) How about of the form $N^2 - 3$? How about $N^2 - 4$?
- (d) Which values of a do you think give infinitely many primes of the form $N^2 - a$?

1.4. The following two lines indicate another way to derive the formula for the sum of the first n integers by rearranging the terms in the sum. Fill in the details.

$$\begin{aligned} 1 + 2 + 3 + \cdots + n &= (1 + n) + (2 + (n - 1)) + (3 + (n - 2)) + \cdots \\ &= (1 + n) + (1 + n) + (1 + n) + \cdots \end{aligned}$$

How many copies of $n + 1$ are in there in the second line? You may need to consider the cases of odd n and even n separately. If that's not clear, first try writing it out explicitly for $n = 6$ and $n = 7$.

1.5. For each of the following statements, fill in the blank with an easy-to-check criterion:

- (a) M is a triangular number if and only if _____ is an odd square.
- (b) N is an odd square if and only if _____ is a triangular number.
- (c) Prove that your criteria in (a) and (b) are correct.

1.6. Suppose that x and y are integers that satisfy the equation

$$x^2 - 2y^2 = 1.$$

Prove that x must be odd and that y must be even.

1.7. Find four solutions in positive integers to the equation

$$x^2 - 5y^2 = 1.$$

[Hint. Use trial and error to find a small solution (a, b) and then take powers of $a + b\sqrt{5}$.]

1.8. (a) In this problem we investigate which numbers can be written as a sum of two triangular numbers. It is convenient to allow 0 to be triangular number, so for example 3, 7, and 20 are each sums of two triangular numbers, since

$$3 = 0 + 3, \quad 7 = 1 + 6, \quad \text{and} \quad 20 = 10 + 10.$$

On the other hand, 19 is not a sum of two triangular numbers. Make a table of the numbers from 1 to 30 and determine which of them can be written as a sum of two triangular numbers

- (b) Fill in the blank with a formula involving B and then prove that your statement is correct:

B is a sum of two triangular numbers if and only if _____ is a sum of two squares.

- (c) Compile some data and make a conjecture about which numbers can be written as sums of three triangular numbers?

1.9. A number n is called a *pentagonal number* if n pebbles can be arranged in the shape of a (filled in) pentagon. The first four pentagonal numbers are 1, 5, 12, and 22, as illustrated in Figure 1.3. You should visualize each pentagon as sitting inside the next larger pentagon. The n^{th} pentagonal number is formed using an outer pentagon whose sides have n pebbles.

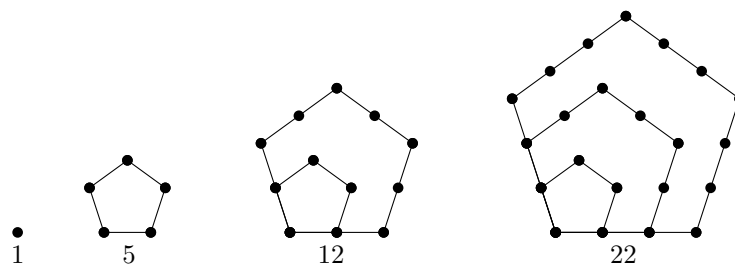


Figure 1.3: The First Four Pentagonal Numbers

- (a) Draw a picture for the fifth pentagonal number.
- (b) Figure out the pattern and find a simple formula for the n^{th} pentagonal number.
- (c) What is the 10^{th} pentagonal number? What is the 100^{th} pentagonal number?

1.10. (a) Bonus Problem: Let (x_k, y_k) for $k = 0, 1, 2, 3, \dots$ be the solutions to $x^2 - 2y^2 = 1$ described in Theorem 1.2. Fill in the blanks with positive numbers such that the following formulas are true. Then prove that the formulas are correct.

$$x_{k+1} = ______ x_k + ______ y_k \quad \text{and} \quad y_{k+1} = ______ x_k + ______ y_k.$$

- (b) Fill in the blanks with positive numbers such that the following statement is true: If (m, n) gives a square-triangular number, that is, if the pair (m, n) satisfies the formula $n^2 = m(m+1)/2$, then

$$(1 + ______ m + ______ n, 1 + ______ m + ______ n)$$

also gives a square-triangular number.

- (c) If L is a square-triangular number, explain why $1 + 17L + 6\sqrt{L + 8L^2}$ is the next largest square-triangular number.

Chapter 2

Number Theory — Lecture #2

2.1 Pythagorean Triples

The Pythagorean Theorem, that formula loved (or loathed?) by all high school geometry students, says that the sum of the squares of the sides of a right triangle equals the square of the hypotenuse. In symbols,

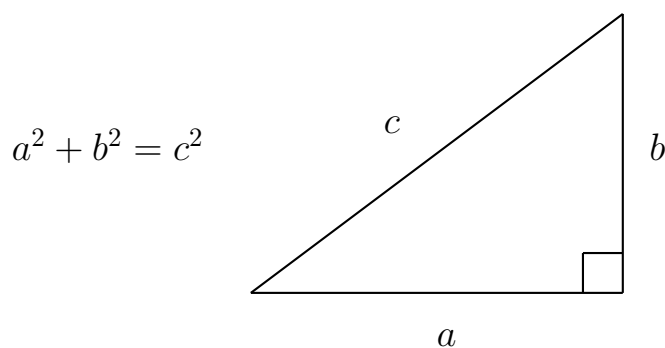


Figure 2.1: A Pythagorean Triangle

Since we're interested in number theory, that is, the theory of the whole numbers, we will ask whether there are any Pythagorean triangles all of whose sides are positive integers. There are many such triangles, the most famous being 3, 4, and 5. Here are the first few examples:

| | | | |
|-------------------|---------------------|---------------------|----------------------|
| $3^2 + 4^2 = 5^2$ | $5^2 + 12^2 = 13^2$ | $8^2 + 15^2 = 17^2$ | $28^2 + 45^2 = 53^2$ |
|-------------------|---------------------|---------------------|----------------------|

The study of these *Pythagorean triples* began long before the time of Pythagoras. There are Babylonian tablets that contain lists of parts of such triples, including quite large ones, indicating that the Babylonians probably had a systematic method

for producing them. Even more amazing is the fact that the Babylonians may have used their lists of Pythagorean triples as primitive trigonometric tables. Pythagorean triples were also used in ancient Egypt. For example, a rough-and-ready way to produce a right angle is to take a piece of string, mark it into 12 equal segments, tie it into a loop, and hold it taut in the form of a 3-4-5 triangle, as illustrated in Figure 2.2. This provides an inexpensive right angle tool for use on small construction projects, such as marking property boundaries or building pyramids.

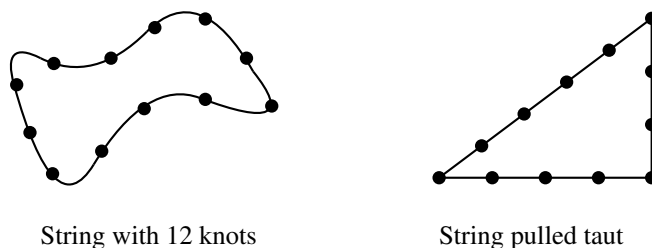


Figure 2.2: Using a knotted string to create a right triangle

The Babylonians and Egyptians had practical reasons for studying Pythagorean triples. Do such practical reasons still exist? For this particular problem, the answer is “probably not.” However, there is at least one good reason to study Pythagorean triples, and it’s the same reason why it is worthwhile studying the art of Rembrandt and the music of Beethoven. There is a beauty to the ways in which numbers interact with one another, just as there is a beauty in the composition of a painting or a symphony. To appreciate this beauty, one has to be willing to expend a certain amount of mental energy. But the end result is well worth the effort. Our goal is to understand and appreciate some truly beautiful mathematics, to learn how this mathematics was discovered and proved, and maybe even to make some original contributions of our own.

Enough blathering, you are undoubtedly thinking. Let’s get to the real stuff. Our first naive question is whether there are infinitely many *Pythagorean triples*, that is, triples of natural numbers (a, b, c) satisfying the equation $a^2 + b^2 = c^2$. The answer is “YES” for a very silly reason. If we take a Pythagorean triple (a, b, c) and multiply it by some other number d , then we obtain a new Pythagorean triple (da, db, dc) . This is true because

$$(da)^2 + (db)^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2.$$

Clearly these new Pythagorean triples are not very interesting. So we will concentrate our attention on triples with no common factors. We will even give them a name:

A *primitive Pythagorean triple* (or PPT for short) is a triple of numbers (a, b, c) such that a , b , and c have no common factors¹ and satisfy

¹A *common factor* of a , b , and c is a number d such that each of a , b , and c is a multiple of d . For example, 3 is a common factor of 30, 42, and 105, since $30 = 3 \cdot 10$, $42 = 3 \cdot 14$, and $105 = 3 \cdot 35$, and

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

Recall our checklist from the end of Section 1.1. The first step is to accumulate some data. I used a computer to substitute in values for a and b and checked if $a^2 + b^2$ is a square. Here are some primitive Pythagorean triples that I found:

$$\begin{array}{cccc} (3, 4, 5), & (5, 12, 13), & (8, 15, 17), & (7, 24, 25), \\ (20, 21, 29), & (9, 40, 41), & (12, 35, 37), & (11, 60, 61), \\ (28, 45, 53), & (33, 56, 65), & (16, 63, 65). \end{array}$$

A few conclusions can easily be drawn even from such a short list. For example, it certainly looks like one of a and b is odd and the other even. It also seems that c is always odd.

It's not hard to prove that these conjectures are correct. First, if a and b are both even, then c would also be even. This means that a , b , and c would have a common factor of 2, so the triple would not be primitive. Next, suppose that a and b are both odd, which means that c would have to be even. This means that there are numbers x , y , and z such that

$$a = 2x + 1, \quad b = 2y + 1, \quad \text{and} \quad c = 2z.$$

We can substitute these into the equation $a^2 + b^2 = c^2$ to get

$$\begin{aligned} (2x + 1)^2 + (2y + 1)^2 &= (2z)^2, \\ 4x^2 + 4x + 4y^2 + 4y + 2 &= 4z^2. \end{aligned}$$

Now divide by 2,

$$2x^2 + 2x + 2y^2 + 2y + 1 = 2z^2.$$

This last equation says that the odd number on the left is equal to the even number on the right, which is impossible, so a and b cannot both be odd. Since we've also checked that they cannot both be even and cannot both be odd, it must be true that one is even and the other is odd. It's then obvious from the equation $a^2 + b^2 = c^2$ that c is also odd.

We can always switch a and b , so our problem now is to find all solutions in natural numbers to the equation

$$a^2 + b^2 = c^2 \quad \text{with} \quad \begin{cases} a \text{ odd,} \\ b \text{ even,} \\ a, b, c \text{ have no common factors.} \end{cases}$$

The tools that we use are *factorization* and *divisibility*.

Our first observation is that if (a, b, c) is a primitive Pythagorean triple, then we can factor

indeed it is their largest common factor. On the other hand, the numbers 10, 12, and 15 have no common factor (other than 1). Since our current goal is to explore some interesting and beautiful number theory without getting bogged down in formalities, we will use common factors and divisibility informally and trust our intuition. Later we will return to these questions and develop the theory of divisibility more carefully.

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

Here are a few examples from the list given earlier, where note that we always take a to be odd and b to be even:

$$\begin{aligned} 3^2 &= 5^2 - 4^2 = (5 - 4)(5 + 4) = 1 \cdot 9, \\ 15^2 &= 17^2 - 8^2 = (17 - 8)(17 + 8) = 9 \cdot 25, \\ 35^2 &= 37^2 - 12^2 = (37 - 12)(37 + 12) = 25 \cdot 49, \\ 33^2 &= 65^2 - 56^2 = (65 - 56)(65 + 56) = 9 \cdot 121. \end{aligned}$$

It looks like $c - b$ and $c + b$ are themselves always squares. We check this observation with a couple more examples:

$$\begin{aligned} 21^2 &= 29^2 - 20^2 = (29 - 20)(29 + 20) = 9 \cdot 49, \\ 63^2 &= 65^2 - 16^2 = (65 - 16)(65 + 16) = 49 \cdot 81. \end{aligned}$$

How can we prove that $c - b$ and $c + b$ are squares? Another observation apparent from our list of examples is that $c - b$ and $c + b$ seem to have no common factors. We can prove this last assertion as follows. Suppose that d is a common factor of $c - b$ and $c + b$; that is, d divides both $c - b$ and $c + b$. Then d also divides

$$(c + b) + (c - b) = 2c \quad \text{and} \quad (c + b) - (c - b) = 2b.$$

Thus, d divides $2b$ and $2c$. But b and c have no common factor because we are assuming that (a, b, c) is a primitive Pythagorean triple. So d must equal 1 or 2. But d also divides $(c - b)(c + b) = a^2$, and a is odd, so d must be 1. In other words, the only number dividing both $c - b$ and $c + b$ is 1, so $c - b$ and $c + b$ have no common factor.

We now know that $c - b$ and $c + b$ are positive integers having no common factor, that their product is a square since $(c - b)(c + b) = a^2$. The only way that this can happen is if $c - b$ and $c + b$ are themselves squares.² So we can write

$$c + b = s^2 \quad \text{and} \quad c - b = t^2,$$

where $s > t \geq 1$ are odd integers with no common factors. Solving these two equations for b and c yields

$$c = \frac{s^2 + t^2}{2} \quad \text{and} \quad b = \frac{s^2 - t^2}{2},$$

and then

$$a = \sqrt{(c - b)(c + b)} = \sqrt{t^2 \cdot s^2} = st.$$

We have (almost) finished our first serious proof! The following theorem records our accomplishment.

²This is intuitively clear if you consider the factorization of $c - b$ and $c + b$ into primes, since the primes in the factorization of $c - b$ will be distinct from the primes in the factorization of $c + b$. However, the existence and uniqueness of the factorization into primes is by no means as obvious as it appears. Later we will prove this unique factorization property.

Theorem 2.1 (Pythagorean Triples Theorem). *We can find every primitive Pythagorean triple (a, b, c) with a odd and b even by using the formulas*

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where $s > t \geq 1$ are chosen to be any odd integers with no common factors.

Why did we say that we have “almost” finished the proof? We have shown that if (a, b, c) is a PPT with a odd, then there are odd integers $s > t \geq 1$ with no common factors so that a , b , and c are given by the stated formulas. But we still need to check that these formulas always give a PPT. We first use a little bit of algebra to show that the formulas give a Pythagorean triple. Thus

$$(st)^2 + \left(\frac{s^2 - t^2}{2}\right)^2 = s^2t^2 + \frac{s^4 - 2s^2t^2 + t^4}{4} = \frac{s^4 + 2s^2t^2 + t^4}{4} = \left(\frac{s^2 + t^2}{2}\right)^2.$$

We also need to check that st , $\frac{s^2 - t^2}{2}$, and $\frac{s^2 + t^2}{2}$ have no common factors. This requires a fact about prime numbers that we don’t yet know, so we postpone the proof until later, where you will get to finish the argument in Exercise 4.3.

For example, taking $t = 1$ in Theorem 2.1 gives a triple $\left(s, \frac{s^2 - 1}{2}, \frac{s^2 + 1}{2}\right)$ whose b and c entries differ by 1. This explains many of the examples that we listed. Table 2.1 gives all possible triples with $s \leq 9$.

| s | t | $a = st$ | $b = \frac{s^2 - t^2}{2}$ | $c = \frac{s^2 + t^2}{2}$ |
|-----|-----|----------|---------------------------|---------------------------|
| 3 | 1 | 3 | 4 | 5 |
| 5 | 1 | 5 | 12 | 13 |
| 7 | 1 | 7 | 24 | 25 |
| 9 | 1 | 9 | 40 | 41 |
| 5 | 3 | 15 | 8 | 17 |
| 7 | 3 | 21 | 20 | 29 |
| 7 | 5 | 35 | 12 | 37 |
| 9 | 5 | 45 | 28 | 53 |
| 9 | 7 | 63 | 16 | 65 |

Table 2.1: Primitive Pythagorean Triples with $9 \geq s > t$

A Notational Interlude

Mathematicians have created certain standard notation as a shorthand for various quantities. We will keep our use of such notation to a minimum, but there are a few symbols that are so commonly used and are so useful that it is worthwhile to introduce them here. They are

\mathbb{N} = the set of natural numbers = $1, 2, 3, 4, \dots$,

\mathbb{Z} = the set of integers = $\dots - 3, -2, -1, 0, 1, 2, 3, \dots$,

\mathbb{Q} = the set of rational numbers (i.e., fractions).

In addition, mathematicians often use \mathbb{R} to denote the real numbers and \mathbb{C} for the complex numbers, but we will not need these. Why were these letters chosen? The choice of \mathbb{N} , \mathbb{R} , and \mathbb{C} needs no explanation. The letter \mathbb{Z} for the set of integers comes from the German word “Zahlen,” which means numbers. Similarly, \mathbb{Q} comes from the German “Quotient” (which is the same as the English word). We will also use the standard mathematical symbol \in to mean “is an element of the set.” So, for example, $a \in \mathbb{N}$ means that a is a natural number, and $x \in \mathbb{Q}$ means that x is a rational number.

2.2 Pythagorean Triples and the Unit Circle

In the previous section we described all solutions to

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

in whole numbers a, b, c . If we divide this equation by c^2 , we obtain

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

So the pair of rational numbers $(a/c, b/c)$ is a solution to the equation

$$x^2 + y^2 = 1.$$

Everyone knows what the equation $x^2 + y^2 = 1$ looks like: It is a circle C of radius 1 with center at $(0, 0)$. We are going to use the geometry of the circle C to find all the points on C whose xy -coordinates are rational numbers. Notice that the circle has four obvious points with rational coordinates, $(\pm 1, 0)$ and $(0, \pm 1)$. Suppose that we take any (rational) number m and look at the line L going through the point $(-1, 0)$ and having slope m , as illustrated in Figure 2.3. The line L is given by the equation

$$L : y = m(x + 1) \quad (\text{point-slope formula}).$$

It is clear from the picture that the intersection $C \cap L$ consists of exactly two points, and one of those points is $(-1, 0)$. We want to find the other one.

To find the intersection of C and L , we need to solve the equations

$$x^2 + y^2 = 1 \quad \text{and} \quad y = m(x + 1)$$

for x and y . Substituting the second equation into the first and simplifying, we need to solve

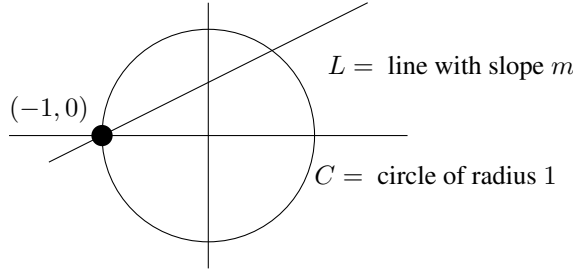


Figure 2.3: The Intersection of a Circle and a Line

$$\begin{aligned}
 x^2 + (m(x+1))^2 &= 1 \\
 x^2 + m^2(x^2 + 2x + 1) &= 1 \\
 (m^2 + 1)x^2 + 2m^2x + (m^2 - 1) &= 0.
 \end{aligned}$$

This is just a quadratic equation, so we could use the quadratic formula to solve for x . But there is a much easier way to find the solution. We know that $x = -1$ must be a solution, since the point $(-1, 0)$ is on both C and L . This means that we can divide the quadratic polynomial by $x + 1$ to find the other root:

$$\begin{array}{r}
 (m^2 + 1)x + (m^2 - 1) \\
 x + 1 \overline{) (m^2 + 1)x^2 + 2m^2x + (m^2 - 1)}
 \end{array}$$

So the other root is the solution of $(m^2 + 1)x + (m^2 - 1) = 0$, which means that

$$x = \frac{1 - m^2}{1 + m^2}.$$

Then we substitute this value of x into the equation $y = m(x + 1)$ of the line L to find the y -coordinate,

$$y = m(x + 1) = m \left(\frac{1 - m^2}{1 + m^2} + 1 \right) = \frac{2m}{1 + m^2}.$$

Thus, for every rational number m we get a solution in rational numbers

$$\left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right) \text{ to the equation } x^2 + y^2 = 1.$$

On the other hand, if we have a solution (x_1, y_1) in rational numbers, then the slope of the line through (x_1, y_1) and $(-1, 0)$ will be a rational number. So by taking all possible values for m , the process we have described will yield every solution to $x^2 + y^2 = 1$ in rational numbers [except for $(-1, 0)$, which corresponds to a vertical line having slope “ $m = \infty$ ”]. We summarize our results in the following theorem.

Theorem 2.2. *Every point on the circle*

$$x^2 + y^2 = 1$$

whose coordinates are rational numbers can be obtained from the formula

$$(x, y) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right)$$

*by substituting in rational numbers for m .*³

How is this formula for rational points on a circle related to our formula for Pythagorean triples? If we write the rational number m as a fraction v/u , then our formula becomes

$$(x, y) = \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right),$$

and clearing denominators gives the Pythagorean triple

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2).$$

This is another way of describing Pythagorean triples, although to describe only the primitive ones would require some restrictions on u and v . You can relate this description to the formula in Theorem 2.1 by setting

$$u = \frac{s+t}{2} \quad \text{and} \quad v = \frac{s-t}{2}.$$

Exercises

- 2.1.** (a) We showed that in any primitive Pythagorean triple (a, b, c) , either a or b is even. Use the same sort of argument to show that either a or b must be a multiple of 3.
 (b) By examining the primitive Pythagorean triples in Table 2.1, make a guess about when a , b , or c is a multiple of 5. Try to show that your guess is correct.
- 2.2.** A nonzero integer d is said to *divide* an integer m if $m = dk$ for some number k . Show that if d divides both m and n , then d also divides $m - n$ and $m + n$.
- 2.3.** For each of the following questions, begin by compiling some data; next examine the data and formulate a conjecture; and finally try to prove that your conjecture is correct. (But don't worry if you can't solve every part of this problem; some parts are quite difficult.)
 (a) Which odd numbers a can appear in a primitive Pythagorean triple (a, b, c) ?
 (b) Which even numbers b can appear in a primitive Pythagorean triple (a, b, c) ?
 (c) Which numbers c can appear in a primitive Pythagorean triple (a, b, c) ?

³We've cheated a little bit. In order to get the point $(-1, 0)$, we need to take the limiting value as $m \rightarrow \infty$

2.4. Our list of examples includes the two primitive Pythagorean triples

$$33^2 + 56^2 = 65^2 \quad \text{and} \quad 16^2 + 63^2 = 65^2.$$

Find at least one more example of two primitive Pythagorean triples with the same value of c . Can you find three primitive Pythagorean triples with the same c ? Can you find more than three?

2.5. We recall that the n^{th} triangular number T_n is given by the formula

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

The first few triangular numbers are 1, 3, 6, and 10. In the list of the first few Pythagorean triples (a, b, c) , we find $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, and $(9, 40, 41)$. Notice that in each case, the value of b is four times a triangular number.

- Find a primitive Pythagorean triple (a, b, c) with $b = 4T_5$. Do the same for $b = 4T_6$ and for $b = 4T_7$.
- Do you think that for every triangular number T_n , there is a primitive Pythagorean triple (a, b, c) with $b = 4T_n$? If you believe that this is true, then prove it. Otherwise, find some triangular number for which it is not true.

2.6. If you look at a list of primitive Pythagorean triples such as Table 2.1, you will see many triples in which c is 2 greater than a . For example, the triples

$$(3, 4, 5), (15, 8, 17), (35, 12, 37), \text{ and } (63, 16, 65)$$

all have this property.

- Find two more primitive Pythagorean triples (a, b, c) having $c = a + 2$.
- Find a primitive Pythagorean triple (a, b, c) having $c = a + 2$ and $c > 1000$.
- Try to find a formula that describes all primitive Pythagorean triples (a, b, c) having $c = a + 2$.

2.7. For each primitive Pythagorean triple (a, b, c) in Table 2.1, compute the quantity $2c - 2a$. Do these values seem to have some special form? Try to prove that your observation is true for all primitive Pythagorean triples.

2.8. Let m and n be numbers that differ by 2, and write the sum $\frac{1}{m} + \frac{1}{n}$ as a fraction in lowest terms. For example, $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ and $\frac{1}{3} + \frac{1}{5} = \frac{8}{15}$.

- Compute the next three examples.
- Examine the numerators and denominators of the fractions in (a) and compare them with the Pythagorean triples in Table 2.1. Formulate a conjecture about such fractions.
- Prove that your conjecture is correct.

2.9. (a) Read about the Babylonian number system and write a short description, including the symbols for the numbers 1 to 10 and the multiples of 10 from 20 to 50.
 (b) Read about the Babylonian tablet called Plimpton 322 and write a brief report, including its approximate date of origin.
 (c) The second and third columns of Plimpton 322 give pairs of integers (a, c) having the property that $c^2 - a^2$ is a perfect square. Convert some of these pairs from Babylonian numbers to decimal numbers and compute the value of b so that (a, b, c) is a Pythagorean triple.

2.10. As we have just seen, we get every Pythagorean triple (a, b, c) with b even from the formula

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$$

by substituting in different integers for u and v . For example, $(u, v) = (2, 1)$ gives the smallest triple $(3, 4, 5)$.

- If u and v have a common factor, explain why (a, b, c) will not be a primitive Pythagorean triple.
- Find an example of integers $u > v > 0$ that do not have a common factor, yet the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is not primitive.
- Make a table of the Pythagorean triples that arise when you substitute in all values of u and v with $1 \leq v < u \leq 10$.
- Using your table from (c), find some simple conditions on u and v that ensure that the Pythagorean triple $(u^2 - v^2, 2uv, u^2 + v^2)$ is primitive.
- Prove that your conditions in (d) really work.

2.11. (a) Use the lines through the point $(1, 1)$ to describe all the points on the circle

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

whose coordinates are rational numbers.

- What goes wrong if you try to apply the same procedure to find all the points on the circle $x^2 + y^2 = 3$ with rational coordinates?

2.12. Find a formula for all the points on the hyperbola

$$x^2 - y^2 = 1$$

whose coordinates are rational numbers. [*Hint.* Take the line through the point $(-1, 0)$ having rational slope m and find a formula in terms of m for the second point where the line intersects the hyperbola.]

2.13. The curve

$$y^2 = x^3 + 8$$

contains the points $(1, -3)$ and $(-7/4, 13/8)$. The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?

2.14. In Section 1.2 we saw that square-triangular numbers have the form $m^2 = \frac{1}{2}(n^2 + n)$, and that we can find all of them by solving the equation

$$x^2 - 2y^2 = 1$$

and setting $m = \frac{1}{2}(x - 1)$ and $n = \frac{1}{2}y$.

- The curve $x^2 - 2y^2 = 1$ includes the point $(1, 0)$. Let L be the line through $(1, 0)$ having slope m . Find the other point where L intersects the curve.
- Suppose that you take m to equal $m = v/u$, where (u, v) is a solution to $u^2 - 2v^2 = 1$. Show that the other point that you found in (b) has integer coordinates. Further, changing the signs of the coordinates if necessary, show that you get a solution to $x^2 - 2y^2 = 1$ in positive integers.
- Starting with the solution $(3, 2)$ to $x^2 - 2y^2 = 1$, apply (b) and (c) repeatedly to find several more solutions to $x^2 - 2y^2 = 1$. Then use those solutions to find additional examples of square-triangular numbers.
- Prove that this procedure leads to infinitely many different square-triangular numbers.

Chapter 3

Number Theory — Lecture #3

3.1 Divisibility and the Greatest Common Divisor

As we have already seen in our study of Pythagorean triples, the notions of divisibility and factorizations are important tools in number theory. In this chapter we will look at these ideas more closely.

Suppose that m and n are integers with $m \neq 0$. We say that m *divides* n if n is a multiple of m , that is, if there is an integer k such that $n = mk$. If m divides n , we write $m|n$. Similarly, if m does not divide n , then we write $m \nmid n$. For example,

$$3|6 \quad \text{and} \quad 12|132, \quad \text{since} \quad 6 = 3 \cdot 2 \quad \text{and} \quad 132 = 12 \cdot 11.$$

The divisors of 6 are 1, 2, 3, and 6. On the other hand, $5 \nmid 7$, since no integer multiple of 5 is equal to 7. A number that divides n is called a *divisor of n* .

If we are given two numbers, we can look for common divisors, that is, numbers that divide both of them. For example, 4 is a common divisor of 12 and 20, since $4|12$ and $4|20$. Notice that 4 is the largest common divisor of 12 and 20. Similarly, 3 is a common divisor of 18 and 30, but it is not the largest, since 6 is also a common divisor. The largest common divisor of two numbers is an extremely important quantity that will frequently appear during our number theoretic excursions.

The *greatest common divisor* of two numbers a and b (not both zero) is the largest number that divides both of them. It is denoted by $\gcd(a, b)$.

If $\gcd(a, b) = 1$, we say that a and b are *relatively prime*.

Two examples that we mentioned above are

$$\gcd(12, 20) = 4 \quad \text{and} \quad \gcd(18, 30) = 6.$$

Another example is

$$\gcd(225, 120) = 15.$$

We can check that this answer is correct by factoring $225 = 3^2 \cdot 5^2$ and $120 = 2^3 \cdot 3 \cdot 5$, but, in general, factoring a and b is not an efficient way to compute their greatest common divisor.¹

The most efficient method known for finding the greatest common divisors of two numbers is called the *Euclidean algorithm*. It consists of doing a sequence of divisions with remainder until the remainder is zero. We will illustrate with two examples before describing the general method.

As our first example, we will compute $\gcd(36, 132)$. The first step is to divide 132 by 36, which gives a quotient of 3 and a remainder of 24. We write this as

$$132 = 3 \times 36 + 24.$$

The next step is to take 36 and divide it by the remainder 24 from the previous step. This gives

$$36 = 1 \times 24 + 12.$$

Next we divide 24 by 12, and we find a remainder of 0,

$$24 = 2 \times 12 + 0.$$

The Euclidean algorithm says that as soon as you get a remainder of 0, the remainder from the previous step is the greatest common divisor of the original two numbers. So in this case we find that $\gcd(132, 36) = 12$.

Let's do a larger example. We will compute

$$\gcd(1160718174, 316258250).$$

Our reason for doing a large example like this is to help convince you that the Euclidean algorithm gives a far more efficient way to compute gcd's than factorization. We begin by dividing 1160718174 by 316258250, which gives 3 with a remainder of 211943424. Next we take 316258250 and divide it by 211943424. This process continues until we get a remainder of 0. The calculations are given in the following table:

$$\begin{array}{rcl} 1160718174 & = & 3 \times 316258250 + 211943424 \\ 316258250 & = & 1 \times 211943424 + 104314826 \\ 211943424 & = & 2 \times 104314826 + 3313772 \\ 104314826 & = & 31 \times 3313772 + 1587894 \\ 3313772 & = & 2 \times 1587894 + 137984 \\ 1587894 & = & 11 \times 137984 + 70070 \\ 137984 & = & 1 \times 70070 + 67914 \\ 70070 & = & 1 \times 67914 + 2156 \\ 67914 & = & 31 \times 2156 + 1078 \\ 2156 & = & 2 \times 1078 + 0 \end{array} \quad \leftarrow \gcd$$

Notice how at each step we divide a number A by a number B to get a quotient Q and a remainder R . In other words,

¹An even less efficient way to compute the greatest common divisor of a and b is the method taught to my daughter by her fourth grade teacher, who recommended that the students make complete lists of all the divisors of a and b and then pick out the largest number that appears on both lists!

$$A = Q \times B + R.$$

Then at the next step we replace our old A and B with the numbers B and R and continue the process until we get a remainder of 0. At that point, the remainder R from the previous step is the greatest common divisor of our original two numbers. So the above calculation shows that

$$\gcd(1160718174, 316258250) = 1078.$$

We can partly check our calculation (always a good idea) by verifying that 1078 is indeed a common divisor. Thus

$$1160718174 = 1078 \times 1076733 \quad \text{and} \quad 316258250 = 1078 \times 293375.$$

There is one more practical matter to be mentioned before we undertake a theoretical analysis of the Euclidean algorithm. If we are given A and B , how can we find the quotient Q and the remainder R ? Of course, you can always use long division, but that can be time consuming and subject to arithmetic errors if A and B are large. A pleasant alternative is to find a calculator or computer program that will automatically compute Q and R for you. However, even if you are only equipped with an inexpensive calculator, there is an easy three-step method to find Q and R .

Method to Compute Q and R on a Calculator So That $A = B \times Q + R$

1. Use the calculator to divide A by B . You get a number with decimals.
2. Discard all the digits to the right of the decimal point. This gives Q .
3. To find R , use the formula $R = A - B \times Q$.

For example, suppose that $A = 12345$ and $B = 417$. Then $A/B = 29.6043\dots$, so $Q = 29$ and $R = 12345 - 417 \cdot 29 = 252$.

We're now ready to analyze the Euclidean algorithm. The general method looks like

$$\begin{aligned} a &= q_1 \times b &+& r_1 \\ b &= q_2 \times r_1 &+& r_2 \\ r_1 &= q_3 \times r_2 &+& r_3 \\ r_2 &= q_4 \times r_3 &+& r_4 \\ &\vdots \\ r_{n-3} &= q_{n-1} \times r_{n-2} &+& r_{n-1} \\ r_{n-2} &= q_n \times r_{n-1} &+& \boxed{r_n} \leftarrow \gcd \\ r_{n-1} &= q_{n+1} r_n &+& 0 \end{aligned}$$

If we let $r_0 = b$ and $r_{-1} = a$, then every line looks like

$$r_{i-1} = q_{i+1} \times r_i + r_{i+1}.$$

Why is the last nonzero remainder r_n a common divisor of a and b ? We start from the bottom and work our way up. The last line $r_{n-1} = q_{n+1} r_n$ shows that r_n divides r_{n-1} . Then the previous line

$$r_{n-2} = q_n \times r_{n-1} + r_n$$

shows that r_n divides r_{n-2} , since it divides both r_{n-1} and r_n . Now looking at the line above that, we already know that r_n divides both r_{n-1} and r_{n-2} , so we find that r_n also divides r_{n-3} . Moving up line by line, when we reach the second line we will already know that r_n divides r_2 and r_1 . Then the second line $b = q_2 \times r_1 + r_2$ tells us that r_n divides b . Finally, we move up to the top line and use the fact that r_n divides both r_1 and b to conclude that r_n also divides a . This completes our verification that the last nonzero remainder r_n is a common divisor of a and b .

But why is r_n the *greatest* common divisor of a and b ? Suppose that d is any common divisor of a and b . We will work our way back down the list of equations. So from the first equation $a = q_1 \times b + r_1$ and the fact that d divides both a and b , we see that d also divides r_1 . Then the second equation $b = q_2 r_1 + r_2$ shows us that d must divide r_2 . Continuing down line by line, at each stage we will know that d divides the previous two remainders r_{i-1} and r_i , and then the current line $r_{i-1} = q_{i+1} \times r_i + r_{i+1}$ will tell us that d also divides the next remainder r_{i+1} . Eventually, we reach the penultimate line $r_{n-2} = q_n \times r_{n-1} + r_n$, at which point we conclude that d divides r_n . So we have shown that if d is any common divisor of a and b then d will divide r_n . Therefore, r_n must be the greatest common divisor of a and b .

This completes our verification that the Euclidean algorithm actually computes the greatest common divisor, a fact of sufficient importance to be officially recorded.

Theorem 3.1 (Euclidean Algorithm). *To compute the greatest common divisor of two numbers a and b , let $r_{-1} = a$, let $r_0 = b$, and compute successive quotients and remainders*

$$r_{i-1} = q_{i+1} \times r_i + r_{i+1}$$

for $i = 0, 1, 2, \dots$ until some remainder r_{n+1} is 0. The last nonzero remainder r_n is then the greatest common divisor of a and b .

There remains the question of why the Euclidean algorithm always finishes. In other words, we know that the last nonzero remainder will be the desired gcd, but how do we know that we ever get a remainder that does equal 0? This is not a silly question, since it is easy to give algorithms that do not terminate; and there are even very simple algorithms for which it is not known whether or not they always terminate. Fortunately, it is easy to see that the Euclidean algorithm always terminates. The reason is simple. Each time we compute a quotient with remainder,

$$A = Q \times B + R,$$

the remainder will be between 0 and $B - 1$. This is clear, since if $R \geq B$, then we can add one more onto the quotient Q and subtract B from R . So the successive remainders in the Euclidean algorithm continually decrease:

$$b = r_0 > r_1 > r_2 > r_3 > \dots$$

But all the remainders are greater than or equal to 0, so we have a strictly decreasing sequence of nonnegative integers. Eventually, we must reach a remainder that equals 0; in fact, it is clear that we will reach a remainder of 0 in at most b steps. Fortunately, the Euclidean algorithm is far more efficient than this. You will show in the exercises that the number of steps in the Euclidean algorithm is at most seven times the *number of digits* in b . So, on a computer, it is quite feasible to compute $\gcd(a, b)$ when a and b have hundreds or even thousands of digits!

3.2 Linear Equations and Greatest Common Divisors

Given two whole numbers a and b , we are going to look at all the possible numbers we can get by adding a multiple of a to a multiple of b . In other words, we will consider all numbers obtained from the formula

$$ax + by$$

when we substitute all possible integers for x and y . Note that we are going to allow both positive and negative values for x and y . For example, we could take $a = 42$ and $b = 30$. Some of the values of $ax + by$ for this a and b are given in the following table:

| | $x = -3$ | $x = -2$ | $x = -1$ | $x = 0$ | $x = 1$ | $x = 2$ | $x = 3$ |
|----------|----------|----------|----------|---------|---------|---------|---------|
| $y = -3$ | -216 | -174 | -132 | -90 | -48 | -6 | 36 |
| $y = -2$ | -186 | -144 | -102 | -60 | -18 | 24 | 66 |
| $y = -1$ | -156 | -114 | -72 | -30 | 12 | 54 | 96 |
| $y = 0$ | -126 | -84 | -42 | 0 | 42 | 84 | 126 |
| $y = 1$ | -96 | -54 | -12 | 30 | 72 | 114 | 156 |
| $y = 2$ | -66 | -24 | 18 | 60 | 102 | 144 | 186 |
| $y = 3$ | -36 | 6 | 48 | 90 | 132 | 174 | 216 |

Table of Values of $42x + 30y$

Our first observation is that every entry in the table is divisible by 6. This is not surprising, since both 42 and 30 are divisible by 6, so every number of the form $42x + 30y = 6(7x + 5y)$ is a multiple of 6. More generally, it is clear that every number of the form $ax + by$ is divisible by $\gcd(a, b)$, since both a and b are divisible by $\gcd(a, b)$.

A second observation, which is somewhat more surprising, is that the greatest common divisor of 42 and 30, which is 6, actually appears in our table. Thus from the table we see that

$$42 \cdot (-2) + 30 \cdot 3 = 6 = \gcd(42, 30).$$

Further examples suggest the following conclusion:

The smallest positive value of
 $ax + by$
 is equal to $\gcd(a, b)$.

There are many ways to prove that this is true. We will take a constructive approach, via the Euclidean algorithm, which has the advantage of giving a procedure for finding the appropriate values of x and y . In other words, we are going to describe a method of finding integers x and y that are solutions to the equation

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

Since, as we have already observed, every number $ax + by$ is divisible by $\gcd(a, b)$, it will follow that the smallest positive value of $ax + by$ is precisely $\gcd(a, b)$.

How might we solve the equation $ax + by = \gcd(a, b)$? If a and b are small, we might be able to guess a solution. For example, the equation

$$10x + 35y = 5$$

has the solution $x = -3$ and $y = 1$, and the equation

$$7x + 11y = 1$$

has the solution $x = -3$ and $y = 2$. We also notice that there can be more than one solution, since $x = 8$ and $y = -5$ is also a solution to $7x + 11y = 1$.

However, if a and b are large, neither guesswork nor trial and error is going to be helpful. We are going to start by illustrating the Euclidean algorithm method for solving $ax + by = \gcd(a, b)$ with a particular example. So we are going to try to solve

$$22x + 60y = \gcd(22, 60).$$

The first step is to perform the Euclidean algorithm to compute the gcd. We find

$$\begin{aligned} 60 &= 2 \times 22 + 16 \\ 22 &= 1 \times 16 + 6 \\ 16 &= 2 \times 6 + 4 \\ 6 &= 1 \times 4 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

This shows that $\gcd(22, 60) = 2$, a fact that is clear without recourse to the Euclidean algorithm. However, the Euclidean algorithm computation is important because we're going to use the intermediate quotients and remainders to solve the equation $22x + 60y = 2$. The first step is to rewrite the first equation as

$$16 = a - 2b, \quad \text{where we let } a = 60 \text{ and } b = 22.$$

We next substitute this value into the 16 appearing in the second equation. This gives (remember that $b = 22$)

$$b = 1 \times 16 + 6 = 1 \times (a - 2b) + 6.$$

Rearranging this equation to isolate the remainder 6 yields

$$6 = b - (a - 2b) = -a + 3b.$$

Now substitute the values 16 and 6 into the next equation, $16 = 2 \times 6 + 4$:

$$a - 2b = 16 = 2 \times 6 + 4 = 2(-a + 3b) + 4.$$

Again we isolate the remainder 4, yielding

$$4 = (a - 2b) - 2(-a + 3b) = 3a - 8b.$$

Finally, we use the equation $6 = 1 \times 4 + 2$ to get

$$-a + 3b = 6 = 1 \times 4 + 2 = 1 \times (3a - 8b) + 2.$$

Rearranging this equation gives the desired solution

$$-4a + 11b = 2.$$

(We should check our solution: $-4 \times 60 + 11 \times 22 = -240 + 242 = 2$.)

We can summarize the above computation in the following efficient tabular form. Note that the left-hand equations are the Euclidean algorithm, and the right-hand equations compute the solution to $ax + by = \gcd(a, b)$.

| | |
|-----------------------|------------------------------------|
| $a = 2 \times b + 16$ | $16 = a - 2b$ |
| $b = 1 \times 16 + 6$ | $6 = b - 1 \times 16$ |
| | $= b - 1 \times (a - 2b)$ |
| | $= -a + 3b$ |
| $16 = 2 \times 6 + 4$ | $4 = 16 - 2 \times 6$ |
| | $= (a - 2b) - 2 \times (-a + 3b)$ |
| | $= 3a - 8b$ |
| $6 = 1 \times 4 + 2$ | $2 = 6 - 1 \times 4$ |
| | $= (-a + 3b) - 1 \times (3a - 8b)$ |
| | $= -4a + 11b$ |
| $4 = 2 \times 2 + 0$ | |

Why does this method work? As the following table makes clear, we start with the first two lines of the Euclidean algorithm, which involve the quantities a and b , and work our way down.

| | |
|-----------------------|---|
| $a = q_1 b + r_1$ | $r_1 = a - q_1 b$ |
| $b = q_2 r_1 + r_2$ | $r_2 = b - q_2 r_1$ |
| | $= b - q_2(a - q_1 b)$ |
| | $= -q_2 a + (1 + q_1 q_2)b$ |
| $r_1 = q_3 r_2 + r_3$ | $r_3 = r_1 - q_3 r_2$ |
| | $= (a - q_1 b) - q_3(-q_2 a + (1 + q_1 q_2)b)$ |
| | $= (1 + q_2 q_3)a - (q_1 + q_3 + q_1 q_2 q_3)b$ |
| \vdots | \vdots |

As we move from line to line, we will continually be forming equations that look like

latest remainder = some multiple of a plus some multiple of b .

Eventually, we get down to the last nonzero remainder, which we know is equal to $\gcd(a, b)$, and this gives the desired solution to the equation $\gcd(a, b) = ax + by$.

A larger example with $a = 12453$ and $b = 2347$ is given in tabular form in Figure 3.1. As before, the left-hand side is the Euclidean algorithm and the right-hand side solves $ax + by = \gcd(a, b)$. We see that $\gcd(12453, 2347) = 1$ and that the equation $12453x + 2347y = 1$ has the solution $(x, y) = (304, -1613)$.

We now know that the equation

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

always has a solution in integers x and y . The final topic we discuss in this section is the question of how many solutions it has, and how to describe all the solutions. Let's start with the case that a and b are relatively prime, that is, $\gcd(a, b) = 1$, and suppose that (x_1, y_1) is a solution to the equation

$$ax + by = 1.$$

We can create additional solutions by subtracting a multiple of b from x_1 and adding the same multiple of a onto y_1 . In other words, for any integer k we obtain a new solution $(x_1 + kb, y_1 - ka)$.² We can check that this is indeed a solution by computing

$$a(x_1 + kb) + b(y_1 - ka) = ax_1 + akb + by_1 - bka = ax_1 + by_1 = 1.$$

So, for example, if we start with the solution $(-1, 2)$ to $5x + 3y = 1$, we obtain new solutions $(-1 + 3k, 2 - 5k)$. Note that the integer k is allowed to be positive, negative, or zero. Putting in particular values of k gives the solutions

$$\begin{aligned} \dots (-13, 22), (-10, 17), (-7, 12), (-4, 7), (-1, 2), \\ (2, -3), (5, -8), (8, -13), (11, -18) \dots \end{aligned}$$

Still looking at the case that $\gcd(a, b) = 1$, we can show that this procedure gives all possible solutions. Suppose that we are given two solutions (x_1, y_1) and (x_2, y_2) to the equation $ax + by = 1$. In other words,

$$ax_1 + by_1 = 1 \quad \text{and} \quad ax_2 + by_2 = 1.$$

We are going to multiply the first equation by y_2 , multiply the second equation by y_1 , and subtract. This will eliminate b and, after a little bit of algebra, we are left with

$$ax_1y_2 - ax_2y_1 = y_2 - y_1.$$

Similarly, if we multiply the first equation by x_2 , multiply the second equation by x_1 , and subtract, we find that

²Geometrically, we are starting from the known point (x_1, y_1) on the line $ax + by = 1$ and using the fact that the line has slope $-a/b$ to find new points $(x_1 + t, y_1 - (a/b)t)$. To get new points with integer coordinates, we need to let t be a multiple of b . Substituting $t = kb$ gives the new integer solution $(x_1 + kb, y_1 - ka)$.

| | |
|----------------------------|---|
| $a = 5 \times b + 718$ | $718 = a - 5b$ |
| $b = 3 \times 718 + 193$ | $193 = b - 3 \times 718$ |
| | $= b - 3 \times (a - 5b)$ |
| | $= -3a + 16b$ |
| $718 = 3 \times 193 + 139$ | $139 = 718 - 3 \times 193$ |
| | $= (a - 5b) - 3 \times (-3a + 16b)$ |
| | $= 10a - 53b$ |
| $193 = 1 \times 139 + 54$ | $54 = 193 - 139$ |
| | $= (-3a + 16b) - (10a - 53b)$ |
| | $= -13a + 69b$ |
| $139 = 2 \times 54 + 31$ | $31 = 139 - 2 \times 54$ |
| | $= (10a - 53b) - 2 \times (-13a + 69b)$ |
| | $= 36a - 191b$ |
| $54 = 1 \times 31 + 23$ | $23 = 54 - 31$ |
| | $= -13a + 69b - (36a - 191b)$ |
| | $= -49a + 260b$ |
| $31 = 1 \times 23 + 8$ | $8 = 31 - 23$ |
| | $= 36a - 191b - (-49a + 260b)$ |
| | $= 85a - 451b$ |
| $23 = 2 \times 8 + 7$ | $7 = 23 - 2 \times 8$ |
| | $= (-49a + 260b) - 2 \times (85a - 451b)$ |
| | $= -219a + 1162b$ |
| $8 = 1 \times 7 + 1$ | $1 = 8 - 7$ |
| | $= 85a - 451b - (-219a + 1162b)$ |
| | $= 304a - 1613b$ |
| $7 = 7 \times 1 + 0$ | |

Figure 3.1: Solving $ax + by = \gcd(a, b)$ for $a = 12453$ and $b = 2347$

$$bx_2y_1 - bx_1y_2 = x_2 - x_1.$$

So if we let $k = x_2y_1 - x_1y_2$, then we find that

$$x_2 = x_1 + kb \quad \text{and} \quad y_2 = y_1 - ka.$$

This means that the second solution (x_2, y_2) is obtained from the first solution (x_1, y_1) by adding a multiple of b onto x_1 and subtracting the same multiple of a from y_1 . So every solution to $ax + by = 1$ can be obtained from the initial solution (x_1, y_1) by substituting different values of k into $(x_1 + kb, y_1 - ka)$.

What happens if $\gcd(a, b) > 1$? To make the formulas look a little bit simpler, we will let $g = \gcd(a, b)$. We know from the Euclidean algorithm method that there is at least one solution (x_1, y_1) to the equation

$$ax + by = g.$$

But g divides both a and b , so (x_1, y_1) is a solution to the simpler equation

$$\frac{a}{g}x + \frac{b}{g}y = 1.$$

Now our earlier work applies, so we know that every other solution can be obtained by substituting values for k in the formula

$$\left(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g} \right).$$

This completes our description of the solutions to the equation $ax + by = g$, as summarized in the following theorem.

Theorem 3.2 (Linear Equation Theorem). *Let a and b be nonzero integers, and let $g = \gcd(a, b)$. The equation*

$$ax + by = g$$

always has a solution (x_1, y_1) in integers, and this solution can be found by the Euclidean algorithm method described earlier. Then every solution to the equation can be obtained by substituting integers k into the formula

$$\left(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g} \right).$$

For example, we saw that the equation

$$60x + 22y = \gcd(60, 22) = 2$$

has the solution $x = -4, y = 11$. Then our Linear Equation Theorem says that every solution is obtained from the formula

$$(-4 + 11k, 11 - 30k) \quad \text{with } k \text{ any integer.}$$

In particular, if we want a solution with x positive, then we can take $k = 1$, which gives the smallest such solution $(x, y) = (7, -19)$.

In this chapter we have shown that the equation

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

always has a solution. This fact is extremely important for both theoretical and practical reasons, and we will be using it repeatedly in our number theoretic investigations. For example, we will use this equation in our theoretical study of factorization of numbers into primes. And solving the equation $ax + by = 1$ is crucial in cryptography, although we will unfortunately not have time to discuss this topic.

Exercises

3.1. Use the Euclidean algorithm to compute each of the following gcd's.

- (a) $\gcd(12345, 67890)$ (b) $\gcd(54321, 9876)$

3.2 (Computer Exercise). Write a program to compute the greatest common divisor $\gcd(a, b)$ of two integers a and b . Your program should work even if one of a or b is zero. Make sure that you don't go into an infinite loop if a and b are both zero!

3.3. Let $b = r_0, r_1, r_2, \dots$ be the successive remainders in the Euclidean algorithm applied to a and b . Show that after every two steps, the remainder is reduced by at least one half. In other words, verify that

$$r_{i+2} < \frac{1}{2}r_i \quad \text{for every } i = 0, 1, 2, \dots$$

Conclude that the Euclidean algorithm terminates in at most $2 \log_2(b)$ steps, where \log_2 is the logarithm to the base 2. In particular, show that the number of steps is at most seven times the number of digits in b . [Hint. What is the value of $\log_2(10)$?]

3.4. The “ $3n + 1$ algorithm” works as follows. Start with any number n . If n is even, divide it by 2. If n is odd, replace it with $3n + 1$. Repeat. So, for example, if we start with 5, we get the list of numbers

$$5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \dots,$$

and if we start with 7, we get

$$7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \dots$$

Notice that if we ever get to 1 the list just continues to repeat with 4, 2, 1's. In general, one of the following two possibilities will occur:³

- (i) We may end up repeating some number a that appeared earlier in our list, in which case the block of numbers between the two a 's will repeat indefinitely. In this case we say that the algorithm *terminates* at the last nonrepeated value, and the number of distinct entries in the list is called the *length of the algorithm*. For example, the algorithm terminates at 1 for both 5 and 7. The length of the algorithm for 5 is 6, and the length of the algorithm for 7 is 17.
- (ii) We may never repeat the same number, in which case we say that the algorithm does not terminate.
- (a) Find the length and terminating value of the $3n + 1$ algorithm for each of the following starting values of n :

$$(i) n = 21 \quad (ii) n = 13 \quad (iii) n = 31$$

- (b) Do some further experimentation and try to decide whether the $3n + 1$ algorithm always terminates and, if so, at what value(s) it terminates.
- (c) Assuming that the algorithm terminates at 1, let $L(n)$ be the length of the algorithm for starting value n . For example, $L(5) = 6$ and $L(7) = 17$. Show that if $n = 8k + 4$ with $k \geq 1$, then $L(n) = L(n + 1)$. [Hint. What does the algorithm do to the starting values $8k + 4$ and $8k + 5$?]
- (d) Show that if $n = 128k + 28$ then $L(n) = L(n + 1) = L(n + 2)$.
- (e) Find some other conditions, similar to those in (c) and (d), for which consecutive values of n have the same length. (It might be helpful to begin by using the next exercise to accumulate some data.)

³There is, of course, a third possibility. We may get tired of computing and just stop working, in which case one might say that the algorithm terminates due to exhaustion of the computer!

3.5 (Computer Exercise). Write a program to implement the $3n + 1$ algorithm described in the previous exercise. The user will input n and your program should return the length $L(n)$ and the terminating value $T(n)$ of the $3n + 1$ algorithm. Use your program to create a table giving the length and terminating value for all starting values $1 \leq n \leq 100$.

3.6. (a) Find a solution in integers to the equation

$$12345x + 67890y = \gcd(12345, 67890).$$

(b) Find a solution in integers to the equation

$$54321x + 9876y = \gcd(54321, 9876).$$

3.7. Describe all integer solutions to each of the following equations.

- (a) $105x + 121y = 1$
- (b) $12345x + 67890y = \gcd(12345, 67890)$
- (c) $54321x + 9876y = \gcd(54321, 9876)$

3.8 (Computer Exercise). The method for solving $ax + by = \gcd(a, b)$ described in this chapter involves a considerable amount of manipulation and back substitution. This exercise describes an alternative way to compute x and y that is especially easy to implement on a computer.

- (a) Show that the algorithm described in Figure 3.2 computes the greatest common divisor g of the positive integers a and b , together with a solution (x, y) in integers to the equation $ax + by = \gcd(a, b)$.
- (b) Implement the algorithm on a computer using the computer language of your choice.
- (c) Use your program to compute $g = \gcd(a, b)$ and integer solutions to $ax + by = g$ for the following pairs (a, b) .
 - (i) (19789, 23548) (ii) (31875, 8387) (iii) (22241739, 19848039)
- (d) What happens to your program if $b = 0$? Fix the program so that it deals with this case correctly.
- (e) For later applications it is useful to have a solution with $x > 0$. Modify your program so that it always returns a solution with $x > 0$. [Hint. If (x, y) is a solution, then so is $(x + b, y - a)$.]

- (1) Set $x = 1$, $g = a$, $v = 0$, and $w = b$.
- (2) If $w = 0$ then set $y = (g - ax)/b$ and return the values (g, x, y) .
- (3) Divide g by w with remainder, $g = qw + t$, with $0 \leq t < w$.
- (4) Set $s = x - qv$.
- (5) Set $(x, g) = (v, w)$.
- (6) Set $(v, w) = (s, t)$.
- (7) Go to Step (2).

Figure 3.2: Efficient algorithm to solve $ax + by = \gcd(a, b)$

- 3.9. (a) Find integers x , y , and z that satisfy the equation

$$6x + 15y + 20z = 1.$$

- (b) Under what conditions on a , b , c is it true that the equation

$$ax + by + cz = 1$$

has a solution? Describe a general method of finding a solution when one exists.

- (c) Use your method from (b) to find a solution in integers to the equation

$$155x + 341y + 385z = 1.$$

- 3.10. Suppose that $\gcd(a, b) = 1$. Prove that for every integer c , the equation $ax + by = c$ has a solution in integers x and y . [*Hint.* Find a solution to $ax + by = 1$ and multiply by c .] Find a solution to $37x + 47y = 103$. Try to make x and y as small as possible.

- 3.11. Sometimes we are only interested in solutions to $ax + by = c$ using nonnegative values for x and y .

- (a) Explain why the equation $3x + 5y = 4$ has no solutions with $x \geq 0$ and $y \geq 0$.
 (b) Make a list of some of the numbers of the form $3x + 5y$ with $x \geq 0$ and $y \geq 0$. Make a conjecture as to which values are not possible. Then prove that your conjecture is correct.
 (c) For each of the following values of (a, b) , find the largest number that is not of the form $ax + by$ with $x \geq 0$ and $y \geq 0$.

$$(i) (a, b) = (3, 7) \qquad (ii) (a, b) = (5, 7) \qquad (iii) (a, b) = (4, 11).$$

- (d) Let $\gcd(a, b) = 1$. Using your results from (c), find a conjectural formula in terms of a and b for the largest number that is not of the form $ax + by$ with $x \geq 0$ and $y \geq 0$? Check your conjecture for at least two more values of (a, b) .
 (e) Prove that your conjectural formula in (d) is correct.
 (f) Try to generalize this problem to sums of three terms $ax + by + cz$ with $x \geq 0$, $y \geq 0$, and $z \geq 0$. For example, what is the largest number that is not of the form $6x + 10y + 15z$ with nonnegative x, y, z ?

Chapter 4

Number Theory — Lecture #4

4.1 Primes and Divisibility

A *prime number* is a number $p \geq 2$ whose only (positive) divisors are 1 and p . Numbers $m \geq 2$ that are not primes are called *composite numbers*. For example,

| | |
|-------------------|---|
| prime numbers | 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... |
| composite numbers | 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ... |

Prime numbers are characterized by the numbers by which they are divisible; that is, they are defined by the property that they are only divisible by 1 and by themselves. So it is not immediately clear that primes numbers should have special properties that involve the numbers that they divide. Thus the following fact concerning prime numbers is both nonobvious and important.¹

Lemma 4.1. *Let p be a prime number, and suppose that p divides the product ab . Then either p divides a or p divides b (or p divides both a and b).²*

Proof. We are given that p divides the product ab . If p divides a , we are done, so we may as well assume that p does not divide a . Now consider what $\gcd(p, a)$ can be. It divides p , so it is either 1 or p . It also divides a , so it isn't p , since we have assumed that p does not divide a . Thus, $\gcd(p, a)$ must equal 1.

Now we use the Linear Equation Theorem (Theorem 3.2) with the numbers p and a . The Linear Equation Theorem says that we can find integers x and y that solve the equation

$$px + ay = 1.$$

[Note that we are using the fact that $\gcd(p, a) = 1$.] Now multiply both sides of the equation by b . This gives

¹A *lemma* is a result that is used as a stepping stone for proving other results.

²You may say that this lemma is obvious if we look at the prime factorizations of a and b . However, the fact that a number can be factored into a product of primes in exactly one way is itself a nonobvious fact. We will discuss this further later in this chapter.

$$pbx + aby = b.$$

Certainly pbx is divisible by p , and also aby is divisible by p , since we know that p divides ab . It follows that p divides the sum

$$pbx + aby,$$

so p divides b . This completes the proof of the lemma.³ □

The lemma says that if a prime divides a product ab , it must divide one of the factors. Notice that this is a special property of prime numbers; it is not true for composite numbers. For example, 6 divides the product $15 \cdot 14$, but 6 divides neither 15 nor 14. It is not hard to extend the lemma to products with more than two factors.

Theorem 4.2 (Prime Divisibility Property). *Let p be a prime number, and suppose that p divides the product $a_1 a_2 \cdots a_r$. Then p divides at least one of the factors a_1, a_2, \dots, a_r .*

Proof. If p divides a_1 , we're done. If not, we apply the lemma to the product

$$a_1(a_2 a_3 \cdots a_r)$$

to conclude that p must divide $a_2 a_3 \cdots a_r$. In other words, we are applying the lemma with $a = a_1$ and $b = a_2 a_3 \cdots a_r$. We know that $p|ab$, so if $p \nmid a$, the lemma says that p must divide b .

So now we know that p divides $a_2 a_3 \cdots a_r$. If p divides a_2 , we're done. If not, we apply the lemma to the product $a_2(a_3 \cdots a_r)$ to conclude that p must divide $a_3 \cdots a_r$. Continuing in this fashion, we must eventually find some a_i that is divisible by p . □

Later in this chapter we are going to use the Prime Divisibility Property to *prove* that every positive integer can be factored as a product of prime numbers in essentially one way. Unfortunately, this important fact is so familiar to most readers that they will question why it requires a proof. So before giving the proof, I want to try to convince you that unique factorization into primes is far from being obvious. For this purpose, I invite you to leave the familiar behind and enter the⁴

Even Number World
(popularly known as the “ \mathbb{E} -Zone”)

Imagine yourself in a world where the only numbers that are known are the even numbers. So, in this world, the only numbers that exist are

³When we are proving a statement, we use a little box □ to indicate that we have completed the proof. Some books instead use QED to indicate the end of a proof. The letters QED stand for the Latin phrase *Quod erat demonstrandum*, which roughly means “that which was to be proved.” This in turn comes from the Greek phrase $\omega\pi\epsilon\rho\ \epsilon\delta\epsilon\iota\ \delta\epsilon\iota\chi\alpha\iota$, which appears in Euclid’s *Elements*.

⁴Since this book is not a multimedia product, you’ll have to use your imagination to supply the appropriate Twilight Zone music.

$$\mathbb{E} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, \dots\}.$$

Notice that in the \mathbb{E} -Zone we can add, subtract, and multiply numbers just as usual, since the sum, difference, and product of even numbers are again even numbers. We can also talk about divisibility. We say that a number m \mathbb{E} -divides a number n if there is a number k with $n = mk$. But remember that we're now in the \mathbb{E} -Zone, so the word “number” means an even number. For example, 6 \mathbb{E} -divides 12, since $12 = 6 \cdot 2$; but 6 does not \mathbb{E} -divide 18, since there is no (even) number k satisfying $18 = 6k$.

We can also talk about primes. We say that an (even) number p is an \mathbb{E} -prime if it is not divisible by any (even) numbers. (In the \mathbb{E} -Zone, a number is not divisible by itself!) For example, here are some \mathbb{E} -primes:

$$2, 6, 10, 14, 18, 22, 26, 30.$$

Recall the lemma we proved above for ordinary numbers. We showed that if a prime p divides a product ab then either p divides a or p divides b . Now move to the \mathbb{E} -Zone and consider the \mathbb{E} -prime 6 and the numbers $a = 10$ and $b = 18$. The number 6 \mathbb{E} -divides $ab = 180$, since $180 = 6 \cdot 30$; but 6 \mathbb{E} -divides neither 10 nor 18. So our “obvious” lemma is not true here in the \mathbb{E} -Zone!

There are other “self-evident facts” that are untrue in the \mathbb{E} -Zone. For example, consider the fact that every number can be factored as a product of primes in exactly one way. (Of course, rearranging the order of the factors is not considered a different factorization.) It's not hard to show, even in the \mathbb{E} -Zone, that every (even) number can be written as a product of \mathbb{E} -primes. But consider the following factorizations:

$$180 = 6 \cdot 30 = 10 \cdot 18.$$

Notice that all of the numbers 6, 30, 10, and 18 are \mathbb{E} -primes. This means that 180 can be written as a product of \mathbb{E} -primes in two fundamentally different ways! In fact, there is even a third way to write it as a product of \mathbb{E} -primes,

$$180 = 2 \cdot 90.$$

We are going to leave the \mathbb{E} -Zone now and return to the familiar world where odd and even numbers live together in peace and harmony. But we hope that our excursion into the \mathbb{E} -Zone has convinced you that facts that seem obvious require a healthy dose of skepticism. Especially, any “fact” that “must be true” because it is very familiar or because it is frequently proclaimed to be true is a fact that needs the most careful scrutiny.⁵

\mathbb{E} -Zone Border Crossing—Welcome Back Home

⁵The principle that well-known and frequently asserted “facts” should be carefully scrutinized also applies to endeavors far removed from mathematics. Politics and journalism come to mind, and the reader will undoubtedly be able to add many others to the list.

4.2 The Fundamental Theorem of Arithmetic

Everyone “knows” that a positive integer can be factored into a product of primes in exactly one way. But our visit to the \mathbb{E} -Zone provides convincing evidence that this obvious assertion requires a careful proof.

Theorem 4.3 (The Fundamental Theorem of Arithmetic). *Every integer $n \geq 2$ can be factored into a product of primes*

$$n = p_1 p_2 \cdots p_r$$

in exactly one way.

Before we commence the proof of the Fundamental Theorem of Arithmetic, a few comments are in order. First, if n itself is prime, then we just write $n = n$ and consider this to be a product consisting of a single number. Second, when we write $n = p_1 p_2 \cdots p_r$, we do not mean that p_1, p_2, \dots, p_r have to be different primes. For example, we would write $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$. Third, when we say that n can be written as a product in exactly one way, we do not consider rearrangement of the factors to be a new factorization. For example, $12 = 2 \cdot 2 \cdot 3$ and $12 = 2 \cdot 3 \cdot 2$ and $12 = 3 \cdot 2 \cdot 2$, but all these are treated as the same factorization.

Proof. The Fundamental Theorem of Arithmetic really contains two assertions.

Assertion 1. The number n can be factored into a product of primes in some way.

Assertion 2. There is only one such factorization (aside from rearranging the factors).

We begin with Assertion 1. We are going to give a proof by induction. More precisely, first we’ll verify the assertion for $n = 2$, and then for $n = 3$, and then for $n = 4$, and so on. We begin by observing that $2 = 2$ and $3 = 3$ and $4 = 2^2$, so each of these numbers can be written as a product of primes. This verifies Assertion 1 for $n = 2, 3, 4$. Now suppose that we’ve verified Assertion 1 for every n up to some number, call it N . This means we know that every number $n \leq N$ can be factored into a product of primes. Now we’ll check that the same is true of $N + 1$.

There are two possibilities. First, $N + 1$ may already be prime, in which case it is its own factorization into primes. Second, $N + 1$ may be composite, which means that it can be factored as $N + 1 = n_1 n_2$ with $2 \leq n_1, n_2 \leq N$. But we know Assertion 1 is true for n_1 and n_2 , since they are both less than or equal to N . This means that both n_1 and n_2 can be written as a product of primes, say

$$n_1 = p_1 p_2 \cdots p_r \quad \text{and} \quad n_2 = q_1 q_2 \cdots q_s.$$

Multiplying these two products together gives

$$N + 1 = n_1 n_2 = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s,$$

so $N + 1$ can be factored into a product of primes. This means that Assertion 1 is true for $N + 1$.

To recapitulate, we have shown that if Assertion 1 is true for all numbers less than or equal to N , then it is also true for $N + 1$. But we have checked it is true for 2, 3, and 4, so taking $N = 4$, we see that it is also true for 5. But then we can take $N = 5$ to conclude that it is true for 6. Taking $N = 6$, we see that it is true for $N = 7$, and so on. Since we can continue this process indefinitely, it follows that Assertion 1 is true for every integer.

Next we tackle Assertion 2. It is possible to give an induction proof for this assertion, too, but we will proceed more directly. Suppose that we are able to factor n as a product of primes in two ways, say

$$n = p_1 p_2 p_3 p_4 \cdots p_r = q_1 q_2 q_3 q_4 \cdots q_s.$$

We need to check that the factorizations are the same, possibly after rearranging the order of the factors. We first observe that $p_1 | n$, so $p_1 | q_1 q_2 \cdots q_s$. The Prime Divisibility Property proved earlier in this chapter tells us that p_1 must divide (at least) one of the q_i 's, so if we rearrange the q_i 's, we can arrange matters so that $p_1 | q_1$. But q_1 is also a prime number, so its only divisors are 1 and q_1 . Therefore, we must have $p_1 = q_1$.

Now we cancel p_1 (which is the same as q_1) from both sides of the equation. This gives the equation

$$p_2 p_3 p_4 \cdots p_r = q_2 q_3 q_4 \cdots q_s.$$

Briefly repeating the same argument, we note that p_2 divides the left-hand side of this equation, so p_2 divides the right-hand side, and hence by the Prime Divisibility Property, p_2 divides one of the q_i 's. After rearranging the factors, we get $p_2 | q_2$, and then the fact that q_2 is prime means that $p_2 = q_2$. This allows us to cancel p_2 (which equals q_2) to obtain the new equation

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

We can continue in this fashion until either all the p_i 's or all the q_i 's are gone. But if all the p_i 's are gone, then the left-hand side of the equation equals 1, so there cannot be any q_i 's left, either. Similarly, if the q_i 's are all gone, then the p_i 's must all be gone. In other words, the number of p_i 's must be the same as the number of q_i 's. To recapitulate, we have shown that if

$$n = p_1 p_2 p_3 p_4 \cdots p_r = q_1 q_2 q_3 q_4 \cdots q_s,$$

where all the p_i 's and q_i 's are primes, then $r = s$, and we can rearrange the q_i 's so that

$$p_1 = q_1 \quad \text{and} \quad p_2 = q_2 \quad \text{and} \quad p_3 = q_3 \quad \text{and} \quad \dots \quad \text{and} \quad p_r = q_s.$$

This completes the proof that there is only one way to write n as a product of primes. \square

The Fundamental Theorem of Arithmetic says that every integer $n \geq 2$ can be written as a product of prime numbers. Suppose we are given a particular integer n . As a practical matter, how can we write it as a product of primes? If n is fairly small (for example, $n = 180$) we can factor it by inspection,

$$180 = 2 \cdot 90 = 2 \cdot 2 \cdot 45 = 2 \cdot 2 \cdot 3 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5.$$

If n is larger (for example, $n = 9105293$) it may be more difficult to find a factorization. One method is to try dividing n by primes $2, 3, 5, 7, 11, \dots$ until we find a divisor. For $n = 9105293$, we find after some work that the smallest prime dividing n is 37. We factor out the 37,

$$9105293 = 37 \cdot 246089,$$

and continue checking $37, 41, 43, \dots$ to find a prime that divides 246089. We find that $43|246089$, since $246089 = 43 \cdot 5723$. And so on until we factor $5723 = 59 \cdot 97$, where we recognize that 59 and 97 are both primes. This gives the complete prime factorization

$$9105293 = 37 \cdot 43 \cdot 59 \cdot 97.$$

If n is not itself prime, then there must be a prime $p \leq \sqrt{n}$ that divides n . To see why this is true, we observe that if p is the smallest prime that divides n , then $n = pm$ with $m \geq p$, and hence $n = pm \geq p^2$. Taking the square root of both sides yields $\sqrt{n} \geq p$. This gives the following foolproof method for writing any number n as a product of primes:

To write n as a product of primes, try dividing it by every number (or just every prime number) $2, 3, \dots$ that is less than or equal to \sqrt{n} . If you find no numbers that divide n , then n itself is prime. Otherwise, the first divisor that you find will be a prime p . Factor $n = pm$ and repeat the process with m .

This procedure, although fairly inefficient, works fine on a computer for numbers that are moderately large, say up to 10 digits. But how about a number like $n = 10^{128} + 1$? If n turns out to be prime, we won't find out until we've checked $\sqrt{n} \approx 10^{64}$ possible divisors. This is completely infeasible. If we could check 1,000,000,000 (that's one billion) possible divisors each second, it would still take approximately $3 \cdot 10^{48}$ years! This leads to the following two closely related questions:

Question 1. How can we tell if a given number n is prime or composite?

Question 2. If n is composite, how can we factor it into primes?

Although it might seem that these questions are the same, it turns out that Question 1 is much easier to answer than Question 2. We will later see how to write down large numbers that we know are composite, even though we will be unable to write down any of their factors. In a similar fashion, we will be able to find very large

prime numbers p and q such that, if we were to send someone the value of the product $n = pq$, they would be unable to factor n to retrieve the numbers p and q . This curious fact, that it is very easy to multiply two numbers but very difficult to factor the product, lies at the heart of a remarkable application of number theory to the creation of some of the very secure codes such as RSA that are used to protect your internet transactions.

Exercises

4.1. Suppose that $\gcd(a, b) = 1$, and suppose further that a divides the product bc . Show that a must divide c . [Try to do this exercise by the same method that we used to prove Lemma 4.1, rather than using the fundamental theorem of arithmetic.]

4.2. Suppose that $\gcd(a, b) = 1$, and suppose further that a divides c and that b divides c . Show that the product ab must divide c . [Try to do this exercise by the same method that we used to prove Lemma 4.1, rather than using the fundamental theorem of arithmetic.]

4.3. Let s and t be odd integers with $s > t \geq 1$ and $\gcd(s, t) = 1$. Prove that the three numbers

$$st, \quad \frac{s^2 - t^2}{2}, \quad \text{and} \quad \frac{s^2 + t^2}{2}$$

are pairwise relatively prime; that is, each pair of them is relatively prime. This fact was needed to complete the proof of the Pythagorean triples theorem (Theorem 2.1 on page 17). [Hint. Assume that there is a common prime factor and use the fact (Lemma 4.1) that if a prime divides a product, then it divides one of the factors.]

4.4. Give a proof by induction of each of the following formulas. [We mention that (a) is the formula that we proved in Section 1.1 using a geometric argument and that (c) is the first n terms of the geometric series.]

- (a) $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$
- (b) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
- (c) $1 + a + a^2 + a^3 + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a} \quad (a \neq 1)$
- (d) $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1)n} = \frac{n-1}{n}$

4.5. This exercise asks you to continue the investigation of the \mathbb{E} -Zone. Remember as you work that for the purposes of this exercise, odd numbers do not exist!

- (a) Describe all \mathbb{E} -primes.
- (b) Show that every even number can be factored as a product of \mathbb{E} -primes. [Hint. Mimic our proof of this fact for ordinary numbers.]
- (c) We saw that 180 has three different factorizations as a product of \mathbb{E} -primes. Find the smallest number that has two different factorizations as a product of \mathbb{E} -primes. Is 180 the smallest number with three factorizations? Find the smallest number with four factorizations.
- (d) The number 12 has only one factorization as a product of \mathbb{E} -primes: $12 = 2 \cdot 6$. (As usual, we consider $2 \cdot 6$ and $6 \cdot 2$ to be the same factorization.) Describe all even numbers that have only one factorization as a product of \mathbb{E} -primes.

4.6. Welcome to \mathbb{M} -World, where the only numbers that exist are positive integers that leave a remainder of 1 when divided by 4. In other words, the only \mathbb{M} -numbers that exist are

$$\{1, 5, 9, 13, 17, 21, \dots\}.$$

(Another description is that these are the numbers of the form $4t + 1$ for $t = 0, 1, 2, \dots$) In the \mathbb{M} -World, we cannot add numbers, but we can multiply them, since if a and b both leave a remainder of 1 when divided by 4 then so does their product. (Do you see why this is true?)

We say that m \mathbb{M} -divides n if $n = mk$ for some \mathbb{M} -number k . And we say that n is an \mathbb{M} -prime if its only \mathbb{M} -divisors are 1 and itself. (Of course, we don't consider 1 itself to be an \mathbb{M} -prime.)

- (a) Find the first six \mathbb{M} -primes.
- (b) Find an \mathbb{M} -number n that has two *different* factorizations as a product of \mathbb{M} -primes.

4.7. [Computer Exercise] In this exercise you are asked to write programs to factor a (positive) integer n into a product of primes. (If $n = 0$, be sure to return an error message instead of going into an infinite loop!) A convenient way to represent the factorization of n is as a $2 \times r$ matrix. Thus, if

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

then store the factorization of n as the matrix

$$\begin{pmatrix} p_1 & p_2 & \cdots & p_r \\ k_1 & k_2 & \cdots & k_r \end{pmatrix}.$$

(If your programming language doesn't allow dynamic storage allocation, you'll have to decide ahead of time how many factors to allow.)

- (a) Write a program to factor n by trying each possible factor $d = 2, 3, 4, 5, 6, \dots$ (This is an extremely inefficient method but will serve as a warm-up exercise.)
- (b) Modify your program by storing the values of the first 100 (or more) primes and first removing these primes from n before looking for larger prime factors. You can speed up your program when trying larger d 's as potential factors if you don't bother checking d 's that are even, or divisible by 3, or by 5. You can also increase efficiency by using the fact that a number m is prime if it is not divisible by any number between 2 and \sqrt{m} . Use your program to find the complete factorization of all numbers between 1,000,000 and 1,000,030.
- (c) Write a subroutine that prints the factorization of n in a nice format. Optimally, the exponents should appear as exponents; but if this is not possible, then print the factorization of (say) $n = 75460 = 2^2 \cdot 5 \cdot 7^3 \cdot 11$ as

$$2^2 * 5 * 7^3 * 11 .$$

(To make the output easier to read, don't print exponents that equal 1.)

Chapter 5

Number Theory — Lecture #5

5.1 Congruences

Divisibility is a powerful tool in the theory of numbers. We have seen this amply demonstrated in our work on Pythagorean triples, greatest common divisors, and factorization into primes. In this chapter we will discuss the theory of congruences. Congruences provide a convenient way to describe divisibility properties. In fact, they are so convenient and natural that they make the theory of divisibility very similar to the theory of equations.

We say that a is *congruent to b modulo m* , and we write

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

if m divides $a - b$. For example,

$$7 \equiv 2 \pmod{5} \quad \text{and} \quad 47 \equiv 35 \pmod{6},$$

since

$$5 \mid (7 - 2) \quad \text{and} \quad 6 \mid (47 - 35).$$

In particular, if a divided by m leaves a remainder of r , then a is congruent to r modulo m . Notice that the remainder satisfies $0 \leq r < m$, so every integer is congruent, modulo m , to a number between 0 and $m - 1$.

The number m is called the *modulus* of the congruence. Congruences with the same modulus behave in many ways like ordinary equations. Thus, if

$$\begin{aligned} a_1 &\equiv b_1 \pmod{m} \quad \text{and} \quad a_2 \equiv b_2 \pmod{m}, \quad \text{then} \\ a_1 \pm a_2 &\equiv b_1 \pm b_2 \pmod{m} \quad \text{and} \quad a_1 a_2 \equiv b_1 b_2 \pmod{m}. \end{aligned}$$

Warning. It is not always possible to divide congruences. In other words, if $ac \equiv bc \pmod{m}$, it need not be true that $a \equiv b \pmod{m}$. For example, $15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$, but $15 \not\equiv 20 \pmod{10}$. Even more distressing, it is possible to have

$$uv \equiv 0 \pmod{m} \text{ with } u \not\equiv 0 \pmod{m} \text{ and } v \not\equiv 0 \pmod{m}.$$

Thus $6 \cdot 4 \equiv 0 \pmod{12}$, but $6 \not\equiv 0 \pmod{12}$ and $4 \not\equiv 0 \pmod{12}$. However, if $\gcd(c, m) = 1$, then it is okay to cancel c from the congruence $ac \equiv bc \pmod{m}$. You will be asked to verify this as an exercise.

Congruences with unknowns can be solved in the same way that equations are solved. For example, to solve the congruence

$$x + 12 \equiv 5 \pmod{8},$$

we subtract 12 from each side to get

$$x \equiv 5 - 12 \equiv -7 \pmod{8}.$$

This solution is fine, or we can use the equivalent solution $x \equiv 1 \pmod{8}$. Notice that -7 and 1 are the same modulo 8 , since their difference is divisible by 8 .

Here's another example. To solve

$$4x \equiv 3 \pmod{19},$$

we will multiply both sides by 5 . This gives

$$20x \equiv 15 \pmod{19}.$$

But $20 \equiv 1 \pmod{19}$, so $20x \equiv x \pmod{19}$. Thus the solution is

$$x \equiv 15 \pmod{19}.$$

We can check our answer by substituting 15 into the original congruence. Is

$$4 \cdot 15 \equiv 3 \pmod{19}?$$

Yes, because $4 \cdot 15 - 3 = 57 = 3 \cdot 19$ is divisible by 19 .

We solved this last congruence by a trick, but if all else fails, there's always the "climb every mountain" technique.¹ To solve a congruence modulo m , we can just try each value $0, 1, \dots, m-1$ for each variable. For example, to solve the congruence

$$x^2 + 2x - 1 \equiv 0 \pmod{7},$$

we just try $x = 0, x = 1, \dots, x = 6$. This leads to the two solutions $x \equiv 2 \pmod{7}$ and $x \equiv 3 \pmod{7}$. Of course, there are other solutions, such as $x \equiv 9 \pmod{7}$. But 9 and 2 are not really different solutions, since they are the same modulo 7 . So when we speak of "finding all the solutions to a congruence," we normally mean that we will find all incongruent solutions, that is, all solutions that are not congruent to one another.

¹Also known as the "ford every stream" technique for those who prefer wet feet to vertigo.

We also observe that there are many congruences, such as $x^2 \equiv 3 \pmod{10}$, that have no solutions. This shouldn't be too surprising. After all, there are ordinary equations such as $x^2 = -1$ that have no (real) solutions.

Our final task in this chapter is to solve congruences that look like

$$ax \equiv c \pmod{m}.$$

Some congruences of this type have no solutions. For example, if

$$6x \equiv 15 \pmod{514}$$

were to have a solution, then 514 would have to divide $6x - 15$. But $6x - 15$ is always odd, so it cannot be divisible by the even number 514. Hence the congruence $6x \equiv 15 \pmod{514}$ has no solutions.

Before giving the general theory, let's try an example. We will solve the congruence

$$18x \equiv 8 \pmod{22}.$$

This means we need to find a value of x with 22 dividing $18x - 8$, so we have to find a value of x with $18x - 8 = 22y$ for some y . In other words, we need to solve the linear equation

$$18x - 22y = 8.$$

We know from Section 3.2 that we can solve the equation

$$18u - 22v = \gcd(18, 22) = 2,$$

and indeed we easily find the solution $u = 5$ and $v = 4$. But we really want the right-hand side to equal 8, so we multiply by 4 to get

$$18 \cdot (5 \cdot 4) - 22 \cdot (4 \cdot 4) = 8.$$

Thus, $18 \cdot 20 \equiv 8 \pmod{22}$, so $x \equiv 20 \pmod{22}$ is a solution to the original congruence. We will soon see that this congruence has two different solutions modulo 22; the other one turns out to be $x \equiv 9 \pmod{22}$.

Suppose now that we are asked to solve an arbitrary congruence of the form

$$ax \equiv c \pmod{m}.$$

We need to find an integer x such that m divides $ax - c$. The number m will divide the number $ax - c$ if we can find an integer y such that $ax - c = my$. Rearranging this last equation slightly, we see that $ax \equiv c \pmod{m}$ has a solution if, and only if, the linear equation $ax - my = c$ has a solution. This should look familiar; it is precisely the sort of problem we solved in Section 3.2.

To make our formulas a bit neater, we will let $g = \gcd(a, m)$. Our first observation is that every number of the form $ax - my$ is a multiple of g ; so if g does not divide c , then $ax - my = c$ has no solutions and so $ax \equiv c \pmod{m}$ also has no solutions.

Next suppose that g does divide c . We know from the Linear Equation Theorem in Section 3.2 that there is always a solution to the equation

$$au + mv = g.$$

Suppose we find a solution $u = u_0, v = v_0$, either by trial and error or by using the Euclidean algorithm method described in Section 3.2. Since we are assuming that g divides c , we can multiply this equation by the integer c/g to obtain the equation

$$a \frac{cu_0}{g} + m \frac{cv_0}{g} = c.$$

This means that

$$x_0 \equiv \frac{cu_0}{g} \pmod{m} \text{ is a solution to the congruence } ax \equiv c \pmod{m}.$$

Are there other solutions? Suppose that x_1 is some other solution to the congruence $ax \equiv c \pmod{m}$. Then $ax_1 \equiv ax_0 \pmod{m}$, so m divides $ax_1 - ax_0$. This implies that

$$\frac{m}{g} \text{ divides } \frac{a(x_1 - x_0)}{g},$$

and we know that m/g and a/g have no common factors, so m/g must divide $x_1 - x_0$. In other words, there is some number k such that

$$x_1 = x_0 + k \cdot \frac{m}{g}.$$

But any two solutions that differ by a multiple of m are considered to be the same, so there will be exactly g different solutions that are obtained by taking $k = 0, 1, \dots, g-1$.

This completes our analysis of the congruence $ax \equiv c \pmod{m}$. We summarize our findings in the following statement.

Theorem 5.1 (Linear Congruence Theorem). *Let a, c , and m be integers with $m \geq 1$, and let $g = \gcd(a, m)$.*

- (a) *If $g \nmid c$, then the congruence $ax \equiv c \pmod{m}$ has no solutions.*
- (b) *If $g \mid c$, then the congruence $ax \equiv c \pmod{m}$ has exactly g incongruent solutions. To find the solutions, first find a solution (u_0, v_0) to the linear equation*

$$au + mv = g.$$

(A method for solving this equation is described in Section 3.2.) Then $x_0 = cu_0/g$ is a solution to $ax \equiv c \pmod{m}$, and a complete set of incongruent solutions is given by

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m} \text{ for } k = 0, 1, 2, \dots, g-1.$$

For example, the congruence

$$943x \equiv 381 \pmod{2576}$$

has no solutions, since $\gcd(943, 2576) = 23$ does not divide 381. On the other hand, the congruence

$$893x \equiv 266 \pmod{2432}$$

has 19 solutions, since $\gcd(893, 2432) = 19$ does divide 266. Notice that we are able to determine the number of solutions without having computed any of them. To actually find the solutions, we first solve

$$893u - 2432v = 19.$$

Using the methods from Section 3.2, we find the solution $(u, v) = (79, 29)$. Multiplying by $266/19 = 14$ gives the solution

$$(x, y) = (1106, 406) \quad \text{to the equation} \quad 893x - 2432y = 266.$$

Finally, the complete set of solutions to

$$893x \equiv 266 \pmod{2432}$$

is obtained by starting with $x \equiv 1106 \pmod{2432}$ and adding multiples of the quantity $2432/19 = 128$. (Don't forget that if the numbers go above 2432 we are allowed to subtract 2432.) The 19 incongruent solutions are

$$1106, 1234, 1362, 1490, 1618, 1746, 1874, 2002, 2130, 2258, \\ 2386, 82, 210, 338, 466, 594, 722, 850, 978.$$

Important Note. The most important case of the Linear Congruence Theorem is when $\gcd(a, m) = 1$. In this case, it says that the congruence

$$ax \equiv c \pmod{m} \tag{*}$$

has exactly one solution. We might even write the solution as a fraction

$$x \equiv \frac{c}{a} \pmod{m},$$

but if we do, then we must remember that the symbol " $\frac{c}{a} \pmod{m}$ " is really only a convenient shorthand for the solution to the congruence (*).

5.2 Congruences, Powers, and Fermat's Little Theorem

Take a number a and consider its powers a, a^2, a^3, \dots modulo m . Is there any pattern to these powers? We will start by looking at a prime modulus $m = p$, since the

pattern is easier to spot. This is a common situation in the theory of numbers, especially when working with congruences. So whenever you're faced with discovering a congruence pattern, it's usually a good idea to begin with a prime modulus.

For each of the primes $p = 3$, $p = 5$, and $p = 7$, we have listed integers $a = 0, 1, 2, \dots$ and some of their powers modulo p . Before reading further, you should stop, examine these tables, and try to formulate some conjectural patterns. Then test your conjectures by creating a similar table for $p = 11$ and seeing if your patterns are still true.

| a | a^2 | a^3 | a^4 |
|-----|-------|-------|-------|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 1 |

a^k modulo 3

| a | a^2 | a^3 | a^4 | a^5 | a^6 |
|-----|-------|-------|-------|-------|-------|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 3 | 1 | 2 | 4 |
| 3 | 4 | 2 | 1 | 3 | 4 |
| 4 | 1 | 4 | 1 | 4 | 1 |

a^k modulo 5

| a | a^2 | a^3 | a^4 | a^5 | a^6 | a^7 | a^8 |
|-----|-------|-------|-------|-------|-------|-------|-------|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 1 | 2 | 4 | 1 | 2 | 4 |
| 3 | 2 | 6 | 4 | 5 | 1 | 3 | 2 |
| 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 |
| 5 | 4 | 6 | 2 | 3 | 1 | 5 | 4 |
| 6 | 1 | 6 | 1 | 6 | 1 | 6 | 1 |

a^k modulo 7

Many interesting patterns are visible in these tables. The one that we will be concerned with in this chapter can be seen in the columns

$$a^2 \pmod{3}, \quad a^4 \pmod{5}, \quad \text{and} \quad a^6 \pmod{7}.$$

Every entry in these columns, aside from the top one, is equal to 1. Does this pattern continue to hold for larger primes? You can check the table you made for $p = 11$, and you will find that

$$1^{10} \equiv 1 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11}, \quad 3^{10} \equiv 1 \pmod{11} \dots$$

$$9^{10} \equiv 1 \pmod{11}, \quad \text{and} \quad 10^{10} \equiv 1 \pmod{11}.$$

This leads us to make the following conjecture:

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{for every integer } 1 \leq a < p.$$

Of course, we don't really need to restrict a to be between 1 and $p - 1$. If a_1 and a_2 differ by a multiple of p , then their powers will be the same modulo p . So the real condition on a is that it not be a multiple of p . This result was first stated by Pierre de Fermat in a letter to Frénicle de Bessy dated 1640, but Fermat gave no indication of his proof. The first known proof appears to be due to Gottfried Leibniz.²

²Gottfried Leibniz (1646–1716) is best known as one of the discoverers of the calculus. He and Isaac Newton worked out the main theorems of the calculus independently and at about the same time. The German and English mathematical communities spent the next two centuries arguing over who deserved priority. The current consensus is that both Leibniz and Newton should be given joint credit as the (independent) discoverers of the calculus.

Theorem 5.2 (Fermat's Little Theorem). *Let p be a prime number, and let a be any number with $a \not\equiv 0 \pmod{p}$. Then*

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

Before giving the proof of Fermat's Little Theorem, we want to indicate its power and show how it can be used to simplify computations. As a particular example, consider the congruence

$$6^{22} \equiv 1 \pmod{23}.$$

This says that the number $6^{22} - 1$ is a multiple of 23. If we wanted to check this fact without using Fermat's Little Theorem, we would have to multiply out 6^{22} , subtract 1, and divide by 23. Here's what we get:

$$6^{22} - 1 = 23 \cdot 5722682775750745.$$

Similarly, in order to verify directly that $73^{100} \equiv 1 \pmod{101}$, we would have to compute $73^{100} - 1$. Unfortunately, $73^{100} - 1$ has 187 digits! And notice that this example only uses $p = 101$, which is a comparatively small prime. Fermat's Little Theorem thus describes a very surprising fact about extremely large numbers.

We can use Fermat's Little Theorem to simplify computations. For example, in order to compute $2^{35} \pmod{7}$, we can use the fact that $2^6 \equiv 1 \pmod{7}$. So we write $35 = 6 \cdot 5 + 5$ and use the law of exponents to compute

$$2^{35} = 2^{6 \cdot 5 + 5} = (2^6)^5 \cdot 2^5 \equiv 1^5 \cdot 2^5 \equiv 32 \equiv 4 \pmod{7}.$$

Similarly, suppose that we want to solve the congruence $x^{103} \equiv 4 \pmod{11}$. Certainly, $x \not\equiv 0 \pmod{11}$, so Fermat's Little Theorem tells us that

$$x^{10} \equiv 1 \pmod{11}.$$

Raising both sides to the 10th power gives $x^{100} \equiv 1 \pmod{11}$, and then multiplying by x^3 gives $x^{103} \equiv x^3 \pmod{11}$. So, to solve the original congruence, we just need to solve $x^3 \equiv 4 \pmod{11}$. This can be solved by trying successively $x = 1, x = 2, \dots$. Thus,

| | | | | | | | | | | | |
|-----------------|---|---|---|---|---|---|---|---|---|---|----|
| $x \pmod{11}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $x^3 \pmod{11}$ | 0 | 1 | 8 | 5 | 9 | 4 | 7 | 2 | 6 | 3 | 10 |

So the congruence $x^{103} \equiv 4 \pmod{11}$ has the solution $x \equiv 5 \pmod{11}$.

We are now ready to prove Fermat's Little Theorem. In order to illustrate the method of proof, we will first prove that $3^6 \equiv 1 \pmod{7}$. Of course, there is no need to give a fancy proof of this fact, since $3^6 - 1 = 728 = 7 \cdot 104$. Nevertheless, when attempting to understand a proof or when attempting to construct a proof, it is often worthwhile using specific numbers. Of course, the idea is to devise a proof that doesn't really use the fact that we are considering specific numbers and then hope that the proof can be made to work in general.

To prove that $3^6 \equiv 1 \pmod{7}$, we start with the numbers

$$1, 2, 3, 4, 5, 6,$$

multiply each of them by 3, and reduce modulo 7. The results are listed in the following table:

| | | | | | | |
|---------------|---|---|---|---|---|---|
| $x \pmod{7}$ | 1 | 2 | 3 | 4 | 5 | 6 |
| $3x \pmod{7}$ | 3 | 6 | 2 | 5 | 1 | 4 |

Notice that each of the numbers 1, 2, 3, 4, 5, 6 reappears exactly once in the second row. So if we multiply together all the numbers in the second row, we get the same result as multiplying together all the numbers in the first row. Of course, we must work modulo 7. Thus,

$$\underbrace{(3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot 4)(3 \cdot 5)(3 \cdot 6)}_{\text{numbers in second row}} \equiv \underbrace{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}_{\text{numbers in first row}} \pmod{7}.$$

To save space, we use the standard symbol $n!$ for the number n factorial, which is the product of $1, 2, \dots, n$. In other words,

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

Factoring out the six factors of 3 on the left-hand side of our congruence gives

$$3^6 \cdot 6! \equiv 6! \pmod{7}.$$

Notice that $6!$ is relatively prime to 7, so we can cancel the $6!$ from both sides. This gives $3^6 \equiv 1 \pmod{7}$, which is exactly Fermat's Little Theorem.

We are now ready to prove Fermat's Little Theorem in general. The key observation in our proof for $3^6 \pmod{7}$ was that multiplication by 3 rearranged the numbers $1, 2, 3, 4, 5, 6 \pmod{7}$. So first we are going to verify the following claim:

Lemma 5.3. *Let p be a prime number and let a be a number with $a \not\equiv 0 \pmod{p}$. Then the numbers*

$$a, 2a, 3a, \dots, (p-1)a \pmod{p}$$

are the same as the numbers

$$1, 2, 3, \dots, (p-1) \pmod{p},$$

although they may be in a different order.

Proof. The list $a, 2a, 3a, \dots, (p-1)a$ contains $p-1$ numbers, and clearly none of them are divisible by p . Suppose that we take two numbers ja and ka in this list, and suppose that they happen to be congruent,

$$ja \equiv ka \pmod{p}.$$

Then $p \mid (j - k)a$, so $p \mid (j - k)$, since we are assuming that p does not divide a . Notice that we are using the Prime Divisibility Property (Lemma 4.1), which says that if a prime divides a product then it divides one of the factors. On the other hand, we know that $1 \leq j, k \leq p - 1$, so $|j - k| < p - 1$. There is only one number with absolute value less than $p - 1$ that is divisible by p and that number is zero. Hence, $j = k$. This shows that different multiples in the list $a, 2a, 3a, \dots, (p - 1)a$ are distinct modulo p .

So we now know that the list $a, 2a, 3a, \dots, (p - 1)a$ contains $p - 1$ distinct nonzero values modulo p . But there are only $p - 1$ distinct nonzero values modulo p , that is, the numbers $1, 2, 3, \dots, (p - 1)$. Hence, the list $a, 2a, 3a, \dots, (p - 1)a$ and the list $1, 2, 3, \dots, (p - 1)$ must contain the same numbers modulo p , although the numbers may appear in a different order. This finishes the proof of the lemma.

Using the lemma, it is easy to finish the proof of Fermat's Little Theorem. The lemma says that the lists of numbers

$$a, 2a, 3a, \dots, (p - 1)a \pmod{p} \quad \text{and} \quad 1, 2, 3, \dots, (p - 1) \pmod{p}$$

are the same, so the product of the numbers in the first list is equal to the product of the numbers in the second list:

$$a \cdot (2a) \cdot (3a) \cdots ((p - 1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p}.$$

Next we factor our $p - 1$ copies of a from the left-hand side to obtain

$$a^{p-1} \cdot (p - 1)! \equiv (p - 1)! \pmod{p}.$$

Finally, we observe that $(p - 1)!$ is relatively prime to p , so we may cancel it from both sides to obtain

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

which completes the proof of Fermat's Little Theorem. \square

Fermat's Little Theorem can be used to show that a number is not a prime without actually factoring it. For example, it turns out that³

$$2^{1234566} \equiv 899557 \pmod{1234567}.$$

This means that 1234567 cannot be a prime, since if it were, Fermat's Little Theorem would tell us that $2^{1234566}$ must be congruent to 1 modulo 1234567. Of course, the number 1234567 is enough that it's not hard to factor it explicitly as $1234567 = 127 \cdot 9721$. But consider the number

$$m = 10^{100} + 37.$$

When we compute $2^{m-1} \pmod{m}$, we get

³If you're wondering how we computed $2^{1234566} \pmod{1234567}$, we mention that there's a very fast algorithm for computing powers of this sort. It goes by various names, including the "square-and-multiply method."

$$\begin{aligned}
2^{m-1} \equiv & 36263603275458610624877601996335839108 \\
& 36873253019151380128320824091124859463 \\
& 579459059730070231844397 \pmod{m}.
\end{aligned}$$

Again we deduce from Fermat's Little Theorem that $10^{100} + 37$ is not prime, but it is not at all clear how to find a factor. A quick check on a desktop computer reveals no prime factors less than 200,000. It is somewhat surprising that we can easily write down numbers that we know are composite, yet for which we are unable to find any factors.

Exercises

5.1. Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

- (a) Verify that $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ and that $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$.
- (b) Verify that $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

5.2. Suppose that

$$ac \equiv bc \pmod{m}$$

and also assume that $\gcd(c, m) = 1$. Prove that $a \equiv b \pmod{m}$.

5.3. Find all incongruent solutions to each of the following congruences.

- (a) $7x \equiv 3 \pmod{15}$
- (b) $6x \equiv 5 \pmod{15}$
- (c) $x^2 \equiv 1 \pmod{8}$
- (d) $x^2 \equiv 2 \pmod{7}$
- (e) $x^2 \equiv 3 \pmod{7}$

5.4. Prove that the following divisibility tests work.

- (a) The number a is divisible by 4 if and only if its last two digits are divisible by 4.
- (b) The number a is divisible by 8 if and only if its last three digits are divisible by 8.
- (c) The number a is divisible by 3 if and only if the sum of its digits is divisible by 3.
- (d) The number a is divisible by 9 if and only if the sum of its digits is divisible by 9.
- (e) The number a is divisible by 11 if and only if the alternating sum of the digits of a is divisible by 11. (If the digits of a are $a_1 a_2 a_3 \dots a_{d-1} a_d$, the alternating sum means to take $a_1 - a_2 + a_3 - \dots$ with alternating plus and minus signs.)

[Hint. For (a), reduce modulo 100, and similarly for (b). For (c), (d), and (e), write a as a sum of multiples of powers of 10 and reduce modulo 3, 9, and 11.]

5.5. Find all incongruent solutions to each of the following linear congruences.

- (a) $8x \equiv 6 \pmod{14}$
- (b) $66x \equiv 100 \pmod{121}$
- (c) $21x \equiv 14 \pmod{91}$

5.6. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.

- (a) $72x \equiv 47 \pmod{200}$
- (b) $4183x \equiv 5781 \pmod{15087}$
- (c) $1537x \equiv 2863 \pmod{6731}$

5.7 (Computer Exercise). Write a program that solves the congruence

$$ax \equiv c \pmod{m}.$$

[If $\gcd(a, m)$ does not divide c , return an error message and the value of $\gcd(a, m)$.] Test your program by finding all of the solutions to the congruences in Exercise 5.6.

5.8 (Computer Exercise). Write a program that takes as input a positive integer m and a polynomial $f(X)$ having integer coefficients and produces as output all of the solutions to the congruence

$$f(X) \equiv 0 \pmod{m}.$$

(Don't try to be fancy. Just substitute $X = 0, 1, 2, \dots, m-1$ and see which values are solutions.) Test your program by taking the polynomial

$$f(X) = X^{11} + 21X^7 - 8X^3 + 8$$

and solving the congruence $f(X) \equiv 0 \pmod{m}$ for each of the following values of m ,

$$m \in \{130, 137, 144, 151, 158, 165, 172\}.$$

5.9. Use Fermat's Little Theorem to perform the following tasks.

- (a) Find a number $0 \leq a < 73$ with $a \equiv 9^{794} \pmod{73}$.
- (b) Solve $x^{86} \equiv 6 \pmod{29}$.
- (c) Solve $x^{39} \equiv 3 \pmod{13}$.

5.10. The quantity $(p-1)! \pmod{p}$ appeared in our proof of Fermat's Little Theorem, although we didn't need to know its value.

- (a) Compute $(p-1)! \pmod{p}$ for some small values of p , find a pattern, and make a conjecture.
- (b) Prove that your conjecture is correct. [Try to discover why $(p-1)! \pmod{p}$ has the value it does for small values of p , and then generalize your observation to prove the formula for all values of p .]

5.11. Exercise 5.10 asked you to determine the value of $(p-1)! \pmod{p}$ when p is a prime number.

- (a) Compute the value of $(m-1)! \pmod{m}$ for some small values of m that are not prime. Do you find the same pattern as you found for primes?
- (b) If you know the value of $(n-1)! \pmod{n}$, how can you use the value to definitely distinguish whether n is prime or composite?

5.12. If p is a prime number and if $a \not\equiv 0 \pmod{p}$, then Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$.

- (a) The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number?
- (b) The congruence $129^{64026} \equiv 15179 \pmod{64027}$ is true. Can you conclude that 64027 is a composite number?
- (c) The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number?

Chapter 6

Number Theory — Lecture #6

6.1 Prime Numbers

Prime numbers are the basic building blocks of number theory. That's what the Fundamental Theorem of Arithmetic (Theorem 4.3) tells us. Every number is built up in a unique fashion by multiplying together prime numbers. There are analogous situations in other areas of science, and without exception the discovery and description of the building blocks has had a profound effect on its discipline. For example, the field of chemistry was revolutionized by the discovery that every chemical is formed from a few basic elements and by Mendeleev cataloging these elements into families whose properties recur periodically. We will do something similar below when we split the set of prime numbers into various subsets, for example, into the set congruent to 1 modulo 4 and the set congruent to 3 modulo 4. Similarly, a tremendous advance in physics occurred when scientists discovered that the atoms comprising every element are made up of three basic particles, protons, neutrons, and electrons,¹ and that the number of each determines the chemical and physical attributes of the atom. For example, an atom made up of 92 protons and only 143 neutrons has properties that clearly distinguish it from its cousin with three additional neutrons.

The fact that prime numbers are basic building blocks is sufficient reason to study their properties. Of course, this doesn't imply that those properties will be interesting. Studying how to conjugate irregular verbs is important when learning a language, but that doesn't make it very appealing. Luckily, the more one studies prime numbers, the more interesting they become, and the more beautiful and surprising become the relationships that one discovers. In this brief unit we will only have time to mention a few of the many remarkable properties of prime numbers.

To begin with, let's list the first few primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \dots$$

¹This description of an atom is a simplification, but it is a fairly accurate portrayal of the original atomic theories advanced in the early part of the twentieth century.

What can we glean from this list? First, it looks like 2 is the only even prime. This is true, of course. If n is even and larger than 2 then it factors as $n = 2 \cdot (n/2)$. This makes 2 somewhat unusual among the set of primes, so people have been known to say that

“2 is the oddest prime!”²

A more important observation from our list of primes is signified by the ellipsis (three dots) appended at the end. This means that the list is not complete. For example, 67 and 71 are the next two primes. However, the real issue is whether the list ends or whether it continues indefinitely. In other words, are there infinitely many prime numbers? The answer is yes. We now give a beautiful proof that appeared in Euclid’s *Elements* more than 2000 years ago.

Theorem 6.1 (Infinitely Many Primes Theorem). *There are infinitely many prime numbers.*

Euclid’s Proof. Suppose that you have already compiled a (finite) list of primes. I am going to show you how to find a new prime that isn’t in your list. Since you can then add the new prime to the list and repeat the process, this will show that there must be infinitely many primes.

So suppose we start with some list of primes p_1, p_2, \dots, p_r . We multiply them together and add 1, which gives the number

$$A = p_1 p_2 \cdots p_r + 1.$$

If A itself is prime, we’re done, since A is too large to be in the original list. But even if A is not prime, it will certainly be divisible by some prime, since every number can be written as a product of primes. Let q be some prime dividing A , for example, the smallest one. I claim that q is not in the original list, so it will be the desired new prime.

Why isn’t q in the original list? We know that q divides A , so

$$q \text{ divides } p_1 p_2 \cdots p_r + 1.$$

If q were to equal one of the p_i ’s, then it would have to divide 1, which is not possible. This means that q is a new prime that may be added to our list. Repeating this process, we can create a list of primes that is as long as we want. This shows that there must be infinitely many prime numbers. \square

Euclid’s proof is very clever and beautiful. We will illustrate the ideas in Euclid’s proof by using them to create a list of primes. We start with a list consisting of the single prime $\{2\}$. Following Euclid, we compute $A = 2 + 1 = 3$. This A is already prime, so we append it to our list. Now we have two primes, $\{2, 3\}$. Again using

²Naturally, I would never even consider repeating such a weak joke! Notice that this is one of those jokes that is language specific. For example, it doesn’t work in French, since an odd number is *impair*, while an odd person or event is *étrange* or *bizarre*.

Euclid's argument, we compute $A = 2 \cdot 3 + 1 = 7$, and again A is prime and can be added to the list. This gives three primes, $\{2, 3, 7\}$. Repeating the argument gives $A = 2 \cdot 3 \cdot 7 + 1 = 43$, another prime! So now our list has four primes, $\{2, 3, 7, 43\}$. Into the breach once more, we compute $A = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$. This time, A is not prime, it factors as $A = 13 \cdot 139$. We add 13 to our list, which now reads $\{2, 3, 7, 43, 13\}$. One more time, we compute $A = 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 + 1 = 23479$. This A also factors, $A = 53 \cdot 443$. This gives the list $\{2, 3, 7, 43, 13, 53\}$, and we will stop here. But in principle we could continue this process to produce a list of primes of any specified length.

We now know that the list of primes continues without end, and we also observed that 2 is the only even prime. Every odd number is congruent to either 1 or 3 modulo 4, so we might ask which primes are congruent to 1 modulo 4 and which are congruent to 3 modulo 4. This separates the set of (odd) primes into two families, just as the periodic table separates the elements into families having similar properties. In the following list, we have boxed the primes congruent to 1 modulo 4:

$$3, \boxed{5}, 7, 11, \boxed{13}, \boxed{17}, 19, 23, \boxed{29}, 31, \boxed{37}, \boxed{41}, 43, 47, \boxed{53}, 59, \\ \boxed{61}, 67, 71, \boxed{73}, 79, 83, \boxed{89}, \boxed{97}, \boxed{101}, \dots$$

There doesn't seem to be any obvious pattern, although there do seem to be plenty of primes of each kind. Here's a longer list.

| | |
|-----------------------|---|
| $p \equiv 1 \pmod{4}$ | 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197, ... |
| $p \equiv 3 \pmod{4}$ | 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, ... |

Is it possible that one of the lines in this list eventually stops, or are there infinitely many primes in each family? It turns out that each line continues indefinitely. We will use a variation of Euclid's proof to show that there are infinitely many primes congruent to 3 modulo 4. Later in Section 9.2.1 we will discuss the 1 modulo 4 primes.

Theorem 6.2 (Primes 3 (Mod 4) Theorem). *There are infinitely many primes that are congruent to 3 modulo 4.*

Proof. We suppose that we have already compiled a (finite) list of primes, all of which are congruent to 3 modulo 4. Our goal is to make the list longer by finding a new 3 modulo 4 prime. Repeating this process gives a list of any desired length, thereby proving that there are infinitely many primes congruent to 3 modulo 4.

Suppose that our initial list of primes congruent to 3 modulo 4 is

$$3, p_1, p_2, \dots, p_r.$$

Consider the number

$$A = 4p_1p_2 \cdots p_r + 3.$$

(Notice that we don't include the prime 3 in the product.) We know that A can be factored into a product of primes, say

$$A = q_1 q_2 \cdots q_s.$$

I claim that among the primes q_1, q_2, \dots, q_s at least one of them must be congruent to 3 modulo 4. This is the key step in the proof. Why is it true? Well, if not, then q_1, q_2, \dots, q_s would all be congruent to 1 modulo 4, in which case their product A would be congruent to 1 modulo 4. But you can see from its definition that A is clearly congruent to 3 modulo 4. Hence, at least one of q_1, q_2, \dots, q_s must be congruent to 3 modulo 4, say $q_i \equiv 3 \pmod{4}$.

My second claim is that q_i is not in the original list. Why not? Well, we know that q_i divides A , while it is clear from the definition of A that none of $3, p_1, p_2, \dots, p_r$ divides A . Thus, q_i is not in our original list, so we may add it to the list and repeat the process. In this way we can create as long a list as we want, which shows that there must be infinitely many primes congruent to 3 modulo 4. \square

We can use the ideas in the proof of the Primes 3 (Mod 4) Theorem to create a list of primes congruent to 3 modulo 4. We need to start with a list containing at least one such prime, and remember that 3 is not allowed in our list. So we start with the list consisting of the single prime $\{7\}$. We compute $A = 4 \cdot 7 + 3 = 31$. This A is itself prime, so it is a new 3 (mod 4) prime to add to our list. The list now reads $\{7, 31\}$, so we compute $A = 4 \cdot 7 \cdot 31 + 3 = 871$. This A is not prime; it factors as $A = 13 \cdot 67$. The proof of the theorem tells us that at least one of the prime factors will be congruent to 3 modulo 4. In this case, the prime 67 is 3 (mod 4), so we add it to our list. Next we take $\{7, 31, 67\}$, compute $A = 4 \cdot 7 \cdot 31 \cdot 67 + 3 = 58159$, and factor it as $A = 19 \cdot 3061$. This time it is the first factor 19 that is 3 (mod 4), so our list becomes $\{7, 31, 67, 19\}$. We will repeat the process one more time. So

$$A = 4 \cdot 7 \cdot 31 \cdot 67 \cdot 19 + 3 = 1104967 = 179 \cdot 6173,$$

which gives the prime 179 to add to the list, $\{7, 31, 67, 19, 179\}$.

Why won't the same idea work for 1 (mod 4) primes? This is not an idle question; it's almost as important to understand the limitations of an argument as it is to understand why the argument is valid. So suppose we try to create a list of 1 (mod 4) primes. If we start with the list $\{p_1, p_2, \dots, p_r\}$, we can compute the number $A = 4p_1 p_2 \cdots p_r + 1$, factor it, and try to find a prime factor that is a new 1 (mod 4) prime. What happens if we start with the list $\{5\}$? We compute $A = 4 \cdot 5 + 1 = 21 = 3 \cdot 7$, and neither of the factors 3 or 7 is a 1 (mod 4) number. So we're stuck. The problem is that it is possible to multiply two 3 (mod 4) numbers, such as 3 and 7, and end up with a 1 (mod 4) number like $A = 21$. In general, we cannot use the fact that $A \equiv 1 \pmod{4}$ to deduce that some prime factor of A is 1 (mod 4), and that's why this proof won't work for primes congruent to 1 modulo 4.

There is no particular reason to consider only congruences modulo 4. For example, every number is congruent to either 0, 1, 2, 3, or 4 modulo 5; and except for 5

itself, every prime number is congruent to one of 1, 2, 3, or 4 modulo 5. (Why?) So we can break up the set of prime numbers into four families, depending on their congruence class modulo 5. Here's a list of the first few numbers in each family:

| | |
|-----------------------|---|
| $p \equiv 1 \pmod{5}$ | 11, 31, 41, 61, 71, 101, 131, 151, 181, 191, 211, 241 |
| $p \equiv 2 \pmod{5}$ | 2, 7, 17, 37, 47, 67, 97, 107, 127, 137, 157, 167, 197 |
| $p \equiv 3 \pmod{5}$ | 3, 13, 23, 43, 53, 73, 83, 103, 113, 163, 173, 193, 223 |
| $p \equiv 4 \pmod{5}$ | 19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239 |

Again there seem to be lots of primes in each family, so we might guess that each contains infinitely many prime numbers.

In general, if we fix a modulus m and a number a , when might we expect there to be infinitely many primes congruent to a modulo m ? There is one situation in which this cannot happen, that is if a and m have a common factor. For example, suppose that p is a prime and that $p \equiv 35 \pmod{77}$. This means that $p = 35 + 77y = 7(5 + 11y)$, so the only possibility is $p = 7$, and even $p = 7$ doesn't work. Generally, if p is a prime satisfying $p \equiv a \pmod{m}$, then $\gcd(a, m)$ divides p . So either $\gcd(a, m) = 1$ or else $\gcd(a, m) = p$, which means there is at most one possibility for p . Thus, it is really only interesting to ask about primes congruent to a modulo m if we assume that $\gcd(a, m) = 1$. A famous theorem of Dirichlet from 1837 says that with this assumption there are always infinitely many primes congruent to a modulo m .

Theorem 6.3 (Dirichlet's Theorem on Primes in Arithmetic Progressions³). *Let a and m be integers with $\gcd(a, m) = 1$. Then there are infinitely many primes that are congruent to a modulo m . That is, there are infinitely many prime numbers p satisfying*

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

Earlier in this chapter we proved Dirichlet's Theorem for $(a, m) = (3, 4)$, and Exercise 6.2 asks you to do $(a, m) = (5, 6)$. Unfortunately, the proof of Dirichlet's Theorem for all (a, m) is quite complicated, so we will not be able to give it here. The proof uses advanced methods from calculus and, in fact, calculus with complex numbers!

6.2 Counting Primes

How many prime numbers are there? We have already given the answer that there are infinitely many. Of course, there are also infinitely many composite numbers. Which

³An arithmetic progression is a list of numbers with a common difference. For example, 2, 7, 12, 17, 22, ... is an arithmetic progression with common difference 5. The numbers congruent to a modulo m form an arithmetic progression with common difference m , which explains the name of Dirichlet's Theorem.

are there more of, primes or composites? Despite the fact that there are infinitely many of each, we can compare them by using a counting function.

First, let's start with an easier question that will illustrate the underlying idea. Our intuition says that approximately half of all numbers are even. We can put this intuition onto firmer ground by looking at the even number counting function:

$$\text{Even}(x) = \#\{\text{even numbers } n \text{ with } 1 \leq n \leq x\}.$$

This function counts how many even numbers there are less than or equal to x . For example,

$$\begin{aligned} \text{Even}(3) &= 1, & \text{Even}(4) &= 2, & \text{Even}(5) &= 2, & \dots \\ \text{Even}(100) &= 50, & \text{Even}(101) &= 50, & \dots \end{aligned}$$

To study what fraction of all numbers are even, we should look at the ratio $\text{Even}(x)/x$. Thus,

$$\begin{aligned} \frac{\text{Even}(3)}{3} &= \frac{1}{3}, & \frac{\text{Even}(4)}{4} &= \frac{1}{2}, & \frac{\text{Even}(5)}{5} &= \frac{2}{5}, & \dots \\ \frac{\text{Even}(100)}{100} &= \frac{1}{2}, & \frac{\text{Even}(101)}{101} &= \frac{50}{101}, & \dots \end{aligned}$$

It is certainly not true that the ratio $\text{Even}(x)/x$ is always equal to $\frac{1}{2}$, but it is true that when x is large $\text{Even}(x)/x$ will be close to $\frac{1}{2}$. If you have taken a little bit of calculus, you will recognize that we are trying to say that

$$\lim_{x \rightarrow \infty} \frac{\text{Even}(x)}{x} = \frac{1}{2}.$$

This statement⁴ just means that as x gets larger and larger the distance between $\text{Even}(x)/x$ and $\frac{1}{2}$ gets closer and closer to 0.

Now let's do the same thing for prime numbers. The counting function for prime numbers is called $\pi(x)$, where “ π ” is an abbreviation for “prime.” (This use of the Greek letter π has nothing to do with the number 3.14159...) Thus

$$\pi(x) = \#\{\text{primes } p \text{ with } p \leq x\}$$

For example, $\pi(10) = 4$, since the primes less than 10 are 2, 3, 5, and 7. Similarly, the primes less than 60 are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59,$$

so $\pi(60) = 17$. Here's a short table giving the values of $\pi(x)$ and the ratio $\pi(x)/x$.

| x | 10 | 25 | 50 | 100 | 200 | 500 | 1000 | 5000 |
|------------|-------|-------|-------|-------|-------|-------|-------|-------|
| $\pi(x)$ | 4 | 9 | 15 | 25 | 46 | 95 | 168 | 669 |
| $\pi(x)/x$ | 0.400 | 0.360 | 0.300 | 0.250 | 0.230 | 0.190 | 0.168 | 0.134 |

⁴This mathematical statement is read “the limit, as x goes to infinity, of $\text{Even}(x)/x$ is equal to $1/2$.”

It certainly looks like the ratio $\pi(x)/x$ is getting smaller and smaller as x gets larger. Assuming that this pattern continues, we would be justified in saying that “most numbers are not prime.” This raises the further question of just how rapidly $\pi(x)/x$ decreases. The answer is provided by the following celebrated result, which is one of the pinnacles of nineteenth-century number theory.

Theorem 6.4 (The Prime Number Theorem). *When x is large, the number of primes less than x is approximately equal to $x/\ln(x)$. In other words,*

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

The quantity $\ln(x)$, which is called the natural logarithm of x , is the logarithm of x to the base $e = 2.7182818 \dots$ ⁵ Table 6.1 compares the values of $\pi(x)$ and $x/\ln(x)$. By examining similar, but shorter, tables around 1800, Carl Friedrich

| x | 10 | 100 | 1000 | 10^4 | 10^6 | 10^9 |
|---------------------|-------|-------|--------|---------|----------|-------------|
| $\pi(x)$ | 4 | 25 | 168 | 1229 | 78498 | 50847534 |
| $x/\ln(x)$ | 4.34 | 21.71 | 144.76 | 1085.74 | 72382.41 | 48254942.43 |
| $\pi(x)/(x/\ln(x))$ | 0.921 | 1.151 | 1.161 | 1.132 | 1.084 | 1.054 |

Table 6.1: Some values for $\pi(x)$ and $x/\ln(x)$

Gauss and Adrien-Marie Legendre independently were led to conjecture that the Prime Number Theorem should be true. Almost a century passed before a proof was found. In 1896 Jacques Hadamard and Ch. de la Vallée Poussin each managed to prove the Prime Number Theorem. Just as with Dirichlet’s Theorem, the proof uses methods from complex analysis (i.e., calculus with complex numbers). More recently, in 1948, Paul Erdős and Atle Selberg found an “elementary” proof of the Prime Number Theorem. Their proof is elementary in the sense that it does not require methods from complex analysis, but it is by no means easy, so we are not able to present it here.

It is somewhat surprising that to prove theorems about whole numbers, such as Dirichlet’s Theorem and the Prime Number Theorem, mathematicians have to use tools from calculus. An entire branch of mathematics called Analytic Number Theory is devoted to proving theorems in number theory using calculus methods.

There are many famous unsolved problems involving prime numbers. We conclude this chapter by describing three such problems with a little bit of their history.

⁵If you are not familiar with natural logarithms, you can just think of $\ln(x)$ as being approximately equal to $2.30259 \log(x)$, where $\log(x)$ is the usual logarithm to the base 10. The natural logarithm is so important in mathematics and science that most scientific calculators have a special button to compute it. The natural logarithm appears “naturally” in problems involving compound growth, such as population growth, interest payments, and decay of radioactive materials. It is a wonderful fact that this widely applicable function also appears in the purely mathematical problem of counting prime numbers.

Conjecture 6.5 (Goldbach's Conjecture). *Every even number $n \geq 4$ is a sum of two primes.*

Goldbach proposed this conjecture to Euler in a letter dated June 7, 1742. It is not hard to check that Goldbach's Conjecture is true for the first few even numbers. Thus,

$$\begin{aligned} 4 &= 2 + 2, & 6 &= 3 + 3, & 8 &= 3 + 5, & 10 &= 3 + 7, & 12 &= 5 + 7, \\ 14 &= 3 + 11, & 16 &= 3 + 13, & 18 &= 5 + 13, & 20 &= 7 + 13 \dots \end{aligned}$$

This verifies Goldbach's Conjecture for all even numbers up to 20. Using computers, Goldbach's conjecture has been checked for all even numbers up to $2 \cdot 10^{10}$. Even better, mathematicians have been able to prove results that are similar to Goldbach's Conjecture. These suggest that Goldbach's Conjecture is also true. One such theorem was proved by I.M. Vinogradov in 1937. He showed that every (sufficiently large) odd number n is a sum of three primes. A second theorem, proved by Chen Jing-run in 1966, says that every (sufficiently large) even number is a sum of two numbers $p + a$, where p is a prime number and a is either prime or a product of two primes.

Conjecture 6.6 (The Twin Primes Conjecture). *There are infinitely many prime numbers p such that $p + 2$ is also prime.*

The list of prime numbers is quite irregular, and there are often very large gaps between consecutive primes. For example, there are 111 composite numbers following the prime 370,261. On the other hand, there seem to be quite a few instances in which a prime p is followed almost immediately by another prime $p + 2$. (Of course, $p + 1$ cannot be prime, since it is even.) These pairs are called *twin primes*, and the Twin Primes Conjecture says that the list of twin primes should never end. The first few twin primes are

$$\begin{aligned} (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), \\ (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), \\ (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313). \end{aligned}$$

Just as with Goldbach's Conjecture, people have used computers to compile long lists of twin primes, including, for example, the tremendous pair consisting of

$$242206083 \cdot 2^{38880} - 1 \quad \text{and} \quad 242206083 \cdot 2^{38880} + 1.$$

As further evidence for the validity of the conjecture, Chen Jing-run proved in 1966 that there are infinitely many primes p such that $p + 2$ is either a prime or a product of two primes.

Conjecture 6.7 (The $N^2 + 1$ Conjecture). *There are infinitely many primes of the form $N^2 + 1$.*

If N is odd, then $N^2 + 1$ is even, so it cannot be prime (unless $N = 1$). However, if N is even, then $N^2 + 1$ seems frequently to be prime. The $N^2 + 1$ Conjecture says that this should happen infinitely often. The first few primes of this form are

$$\begin{aligned}
2^2 + 1 &= 5, & 4^2 + 1 &= 17, & 6^2 + 1 &= 37, & 10^2 + 1 &= 101, \\
14^2 + 1 &= 197, & 16^2 + 1 &= 257, & 20^2 + 1 &= 401, & 24^2 + 1 &= 577, \\
26^2 + 1 &= 677, & 36^2 + 1 &= 1297, & 40^2 + 1 &= 1601.
\end{aligned}$$

The best result currently known was proved by Henryk Iwaniec in 1978. He showed that there are infinitely many values of N for which $N^2 + 1$ is either prime or a product of two primes.

Although no one knows if there are infinitely many twin primes or infinitely many primes of the form $N^2 + 1$, mathematicians have guessed what their counting functions should look like. Let

$$\begin{aligned}
\text{Twin}(x) &= \#\{\text{primes } p \leq x \text{ such that } p + 2 \text{ is also prime}\}, \\
\text{Sq}(x) &= \#\{\text{primes } p \leq x \text{ such that } p \text{ has the form } N^2 + 1\}.
\end{aligned}$$

Then it is conjectured that

$$\lim_{x \rightarrow \infty} \frac{\text{Twin}(x)}{x/(\ln x)^2} = C \quad \text{and} \quad \lim_{x \rightarrow \infty} \frac{\text{Sq}(x)}{\sqrt{x}/\ln x} = C'.$$

The numbers C and C' are a bit complicated to describe precisely. For example, C is approximately equal to 0.66016.

Exercises

6.1. Start with the list consisting of the single prime $\{5\}$ and use the ideas in Euclid's proof that there are infinitely many primes to create a list of primes until the numbers get too large for you to easily factor. (You should be able to factor any number less than 1000.)

6.2. (a) Show that there are infinitely many primes that are congruent to 5 modulo 6. [Hint. Use $A = 6p_1p_2 \cdots p_r + 5$.]

(b) Try to use the same idea (with $A = 5p_1p_2 \cdots p_r + 4$) to show that there are infinitely many primes congruent to 4 modulo 5. What goes wrong? In particular, what happens if you start with $\{19\}$ and try to make a longer list?

6.3. Let p be an odd prime number. Write the quantity

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1}$$

as a fraction A_p/B_p in lowest terms.

(a) Find the value of $A_p \pmod{p}$ and prove that your answer is correct.

(b) Make a conjecture for the value of $A_p \pmod{p^2}$.

(c) Prove your conjecture in (b). (This is quite difficult.)

6.4. Let m be a positive integer, let $a_1, a_2, \dots, a_{\phi(m)}$ be the integers between 1 and m that are relatively prime to m , and write the quantity

$$\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_{\phi(m)}}$$

as a fraction A_m/B_m in lowest terms.

- (a) Find the value of $A_m \pmod{m}$ and prove that your answer is correct.
 (b) Generate some data for the value of $A_m \pmod{m^2}$, try to find patterns, and then try to prove that the patterns you observe are true in general. In particular, when is $A_m \equiv 0 \pmod{m^2}$?

6.5. Recall that the number n factorial, which is written $n!$, is equal to the product

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

- (a) Find the highest power of 2 dividing each of the numbers $1!, 2!, 3!, \dots, 10!$.
 (b) Formulate a rule that gives the highest power of 2 dividing $n!$. Use your rule to compute the highest power of 2 dividing $100!$ and $1000!$.
 (c) Prove that your rule in (b) is correct.
 (d) Repeat (a), (b), and (c), but this time for the largest power of 3 dividing $n!$.
 (e) Try to formulate a general rule for the highest power of a prime p that divides $n!$. Use your rule to find the highest power of 7 dividing $1000!$ and the highest power of 11 dividing $5000!$.
 (f) Using your rule from (e) or some other method, prove that if p is prime and if p^m divides $n!$ then $m < n/(p-1)$. (This inequality is very important in many areas of advanced number theory.)
- 6.6.** (a) Find a prime p satisfying $p \equiv 1338 \pmod{1115}$. Are there infinitely many such primes?
 (b) Find a prime p satisfying $p \equiv 1438 \pmod{1115}$. Are there infinitely many such primes?
- 6.7.** (a) Explain why the statement “one-fifth of all numbers are congruent to 2 modulo 5” makes sense by using the counting function

$$F(x) = \#\{\text{positive numbers } n \leq x \text{ satisfying } n \equiv 2 \pmod{5}\}.$$

- (b) Explain why the statement “most numbers are not squares” makes sense by using the counting function

$$\square(x) = \#\{\text{square numbers less than } x\}.$$

Find a simple function of x that is approximately equal to $\square(x)$ when x is large.

- 6.8.** (a) Check that every even number between 70 and 100 is a sum of two primes.
 (b) How many different ways can 70 be written as a sum of two primes $70 = p + q$ with $p \leq q$? Same question for 90? Same question for 98?

6.9. The number $n!$ (n factorial) is the product of all numbers from 1 to n . For example, $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$ and $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040$. If $n \geq 2$, show that all the numbers

$$n! + 2, \quad n! + 3, \quad n! + 4, \quad \dots, \quad n! + (n-1), \quad n! + n$$

are composite numbers.

- 6.10.** (a) Do you think there are infinitely many primes of the form $N^2 + 2$?
 (b) Do you think there are infinitely many primes of the form $N^2 - 2$?
 (c) Do you think there are infinitely many primes of the form $N^2 + 3N + 2$?
 (d) Do you think there are infinitely many primes of the form $N^2 + 2N + 2$?

6.11. The Prime Number Theorem says that the number of primes smaller than x is approximately $x/\ln(x)$. This exercise asks you to explain why certain statements are plausible. So do not try to write down formal mathematical proofs. Instead, explain as convincingly as you can in words why the Prime Number Theorem makes each of the following statements reasonable.

- (a) If you choose a random integer between 1 and x , then the probability that you chose a prime number is approximately $1/\ln(x)$.
- (b) If you choose two random integers between 1 and x , then the probability that both of them are prime numbers is approximately $1/(\ln x)^2$.
- (c) The number of twin primes between 1 and x should be approximately $x/(\ln x)^2$. [Notice that this explains the conjectured limit formula for the twin prime counting function $\text{Twin}(x)$.]

6.12. (This exercise is for people who have taken some calculus.) The Prime Number Theorem says that the counting function for primes, $\pi(x)$, is approximately equal to $x/\ln(x)$ when x is large. It turns out that $\pi(x)$ is even closer to the value of the definite integral $\int_2^x dt/\ln(t)$.

- (a) Show that

$$\lim_{x \rightarrow \infty} \left(\int_2^x \frac{dt}{\ln(t)} \right) / \left(\frac{x}{\ln(x)} \right) = 1.$$

This means that $\int_2^x dt/\ln(t)$ and $x/\ln(x)$ are approximately the same when x is large. [Hint. Use L'Hôpital's rule and the Second Fundamental Theorem of Calculus.]

- (b) It can be shown that

$$\int \frac{dt}{\ln(t)} = \ln(\ln(t)) + \ln(t) + \frac{(\ln(t))^2}{2 \cdot 2!} + \frac{(\ln(t))^3}{3 \cdot 3!} + \frac{(\ln(t))^4}{4 \cdot 4!} + \dots$$

Use this series to compute numerically the value of $\int_2^x dt/\ln(t)$ for $x = 10, 100, 1000, 10^4, 10^6$, and 10^9 . Compare the values you get with the values of $\pi(x)$ and $x/\ln(x)$ given in the table on page 63. Which is closer to $\pi(x)$, the integral $\int_2^x dt/\ln(t)$ or the function $x/\ln(x)$? (This problem can be done with a simple calculator, but you'll probably prefer to use a computer or programmable calculator.)

- (c) Differentiate the series in (b) and show that the derivative is actually equal to $1/\ln(t)$. [Hint. Use the series for e^x .]

Chapter 7

Number Theory — Lecture #7

7.1 The Fibonacci Sequence

In 1202 Leonardo of Pisa (also known as Leonardo Fibonacci) published his *Liber Abbaci*, a highly influential book of practical mathematics. In this book Leonardo introduced the elegant Hindu/Arabic numerical system (the digits 1, 2, ..., 9 and a symbol/placeholder for 0) to Europeans who were still laboring under the handicap of Roman numerals. Leonardo's book also contains the following curious Rabbit Problem.

In the first month, start with a pair of baby rabbits. One month later they have grown up. The following month the pair of grown rabbits produce a pair of babies, so now we have one pair of grown rabbits and one pair of baby rabbits. Each month thereafter, each pair of grown rabbits produces a new pair of babies, and every pair of baby rabbits grows up. How many pairs of rabbits will there be at the end of one year?

The first few months of rabbit procreation are illustrated in Figure 7.1, where each small circle in Figure 7.1 represents a pair of baby rabbits and each large circle represents a pair of adult rabbits. If we let

F_n = Number of pairs of rabbits after n months,

and if we remember that each month the baby pairs grow up and that each month the grown pairs produce new baby pairs, we can compute the number of pairs of rabbits (baby and adult) in each subsequent month. Thus $F_1 = 1$ (one baby pair) and $F_2 = 1$ (one adult pair) and $F_3 = 2$ (one adult pair plus a new baby pair) and $F_4 = 3$ (two adult pairs plus a new baby pair). Continuing with this computation, we find that This answers Fibonacci's question. At the end of the year, after the 12th month is completed, there are 233 pairs of rabbits. The *Fibonacci sequence* of numbers

1, 1, 2, 3, 5, 8, 13, 21, ...

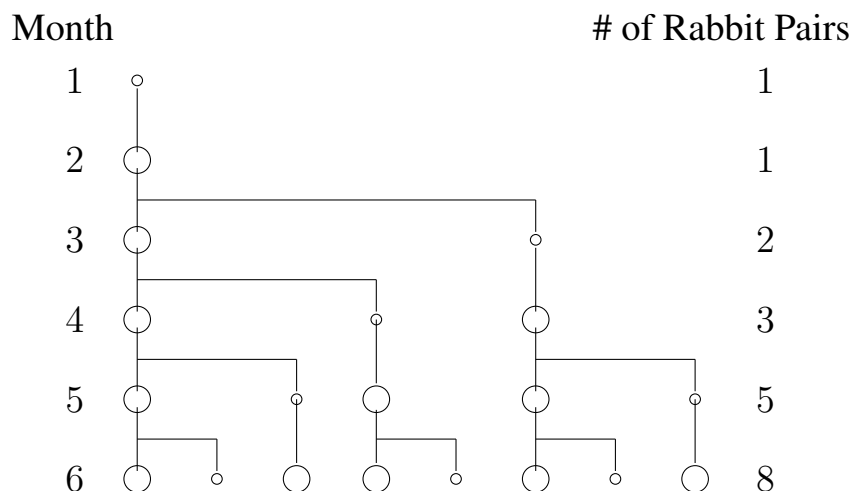


Figure 7.1: The first few months of rabbit procreation

arising from Fibonacci's Rabbit Problem has intrigued people from the thirteenth century up to the present day.¹

Suppose that we want to extend our list of *Fibonacci numbers* F_n beyond the 12th month. Looking at our list, we see that each Fibonacci number is simply the sum of the previous two Fibonacci numbers. In symbols, this becomes the formula

$$F_n = F_{n-1} + F_{n-2}.$$

Notice that this isn't really a *formula* for F_n , because it doesn't directly give the value of F_n . Instead it gives a rule telling us how to compute the n^{th} Fibonacci number from the previous numbers. The fancy mathematical word for this sort of rule is a *recursion* or a *recursive formula*.

We used the recursive formula for F_n to create Table 7.2 giving the first 30 Fibonacci numbers. The Fibonacci numbers appear to grow very rapidly. Indeed, the 31st Fibonacci number is already larger than 1 million,

$$F_{31} = 1,346,269;$$

and in 45 months (less than 4 years),

$$F_{45} = 1,134,903,170,$$

and we have more than 1 billion pairs of rabbits! Now look at Table 7.3 and notice how large the numbers become before we reach even the 200th Fibonacci number.

Number theory is all about patterns, but how can we possibly find a pattern in numbers that grow so rapidly? One thing we can do is try to discover just how fast

¹There is even a journal called the *Fibonacci Quarterly* that was started in 1962 and is devoted to Fibonacci's sequence and its generalizations.

| | | |
|----------------------------|-----------------|--------------|
| $F_1 = 0$ Adult Pairs | + 1 Baby Pair | = 1 Pair |
| $F_2 = 1$ Adult Pair | + 0 Baby Pairs | = 1 Pair |
| $F_3 = 1$ Adult Pair | + 1 Baby Pair | = 2 Pairs |
| $F_4 = 2$ Adult Pairs | + 1 Baby Pair | = 3 Pairs |
| $F_5 = 3$ Adult Pairs | + 2 Baby Pairs | = 5 Pairs |
| $F_6 = 5$ Adult Pairs | + 3 Baby Pairs | = 8 Pairs |
| $F_7 = 8$ Adult Pairs | + 5 Baby Pairs | = 13 Pairs |
| $F_8 = 13$ Adult Pairs | + 8 Baby Pairs | = 21 Pairs |
| $F_9 = 21$ Adult Pairs | + 13 Baby Pairs | = 34 Pairs |
| $F_{10} = 34$ Adult Pairs | + 21 Baby Pairs | = 55 Pairs |
| $F_{11} = 55$ Adult Pairs | + 34 Baby Pairs | = 89 Pairs |
| $F_{12} = 89$ Adult Pairs | + 55 Baby Pairs | = 144 Pairs |
| $F_{13} = 144$ Adult Pairs | + 89 Baby Pairs | = 233 Pairs. |

Table 7.1: The first year of rabbit procreation

the Fibonacci numbers are growing. For example, how much larger than its predecessor is each successive Fibonacci number? This is measured by the ratio F_n/F_{n-1} . Table 7.4 gives the value of F_n/F_{n-1} for all $n \leq 18$.

It looks like the ratio F_n/F_{n-1} is getting closer and closer to some number around 1.61803. It's hard to guess exactly what number this is, so let's see how we might figure it out.

The last table suggests that F_n is approximately equal to αF_{n-1} for some fixed number α whose value we don't know. So we write

$$F_n \approx \alpha F_{n-1},$$

where the squiggly equals sign means “approximately equal to.” The same reasoning tells us that

$$F_{n-1} \approx \alpha F_{n-2},$$

and if we substitute this into $F_n \approx \alpha F_{n-1}$, we get

$$F_n \approx \alpha F_{n-1} \approx \alpha^2 F_{n-2}.$$

So we suspect that $F_n \approx \alpha^2 F_{n-2}$ and $F_{n-1} \approx \alpha F_{n-2}$. We also know the Fibonacci recursive equation $F_n = F_{n-1} + F_{n-2}$, so we find that

$$\alpha^2 F_{n-2} \approx \alpha F_{n-2} + F_{n-2}.$$

Dividing by F_{n-2} and moving everything to one side yields the equation

$$\alpha^2 - \alpha - 1 \approx 0.$$

| n | F_n | n | F_n | n | F_n |
|-----|-------|-----|-------|-----|---------|
| 1 | 1 | 11 | 89 | 21 | 10,946 |
| 2 | 1 | 12 | 144 | 22 | 17,711 |
| 3 | 2 | 13 | 233 | 23 | 28,657 |
| 4 | 3 | 14 | 377 | 24 | 46,368 |
| 5 | 5 | 15 | 610 | 25 | 75,025 |
| 6 | 8 | 16 | 987 | 26 | 121,393 |
| 7 | 13 | 17 | 1,597 | 27 | 196,418 |
| 8 | 21 | 18 | 2,584 | 28 | 317,811 |
| 9 | 34 | 19 | 4,181 | 29 | 514,229 |
| 10 | 55 | 20 | 6,765 | 30 | 832,040 |

Table 7.2: The Fibonacci Numbers F_n

We know how to solve an equation like this: use the quadratic formula.

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad \text{or} \quad \frac{1 - \sqrt{5}}{2}$$

We were looking for the value of α , but we seem to have hit the jackpot and found two values! Both of these values satisfy the equation $\alpha^2 = \alpha + 1$, so for any number n , they both satisfy the equation

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2}.$$

This looks a lot like the Fibonacci recursive equation $F_n = F_{n-1} + F_{n-2}$. In other words, if we let $G_n = \alpha^n$ for either of the values of α listed above, then

$$G_n = G_{n-1} + G_{n-2}.$$

In fact, we can do even better by using both of the values, so we let α be the first value and β be the second value,

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

We now consider the sequence

$$H_n = A\alpha^n + B\beta^n, \quad n = 1, 2, 3, \dots$$

It has the property

$$\begin{aligned}
F_{60} &= 1,548,008,755,920 \\
F_{74} &= 1,304,969,544,928,657 \\
F_{88} &= 1,100,087,778,366,101,931 \\
F_{103} &= 1,500,520,536,206,896,083,277 \\
F_{117} &= 1,264,937,032,042,997,393,488,322 \\
F_{131} &= 1,066,340,417,491,710,595,814,572,169 \\
F_{146} &= 1,454,489,111,232,772,683,678,306,641,953 \\
F_{160} &= 1,226,132,595,394,188,293,000,174,702,095,995 \\
F_{174} &= 1,033,628,323,428,189,498,226,463,595,560,281,832 \\
F_{189} &= 1,409,869,790,947,669,143,312,035,591,975,596,518,914.
\end{aligned}$$

Table 7.3: A list of some large Fibonacci numbers

| | |
|------------------------|---------------------------|
| $F_3/F_2 = 2.00000$ | $F_{11}/F_{10} = 1.61818$ |
| $F_4/F_3 = 1.50000$ | $F_{12}/F_{11} = 1.61797$ |
| $F_5/F_4 = 1.66666$ | $F_{13}/F_{12} = 1.61805$ |
| $F_6/F_5 = 1.60000$ | $F_{14}/F_{13} = 1.61802$ |
| $F_7/F_6 = 1.62500$ | $F_{15}/F_{14} = 1.61803$ |
| $F_8/F_7 = 1.61538$ | $F_{16}/F_{15} = 1.61803$ |
| $F_9/F_8 = 1.61904$ | $F_{17}/F_{16} = 1.61803$ |
| $F_{10}/F_9 = 1.61764$ | $F_{18}/F_{17} = 1.61803$ |

Table 7.4: Values of the ratio of successive Fibonacci numbers

$$\begin{aligned}
H_{n-1} + H_{n-2} &= (A\alpha^{n-1} + B\beta^{n-1}) + (A\alpha^{n-2} + B\beta^{n-2}) \\
&= A(\alpha^{n-1} + \alpha^{n-2}) + B(\beta^{n-1} + \beta^{n-2}) \\
&= A\alpha^n + B\beta^n \\
&= H_n,
\end{aligned}$$

so H_n satisfies the same recursive formula as the Fibonacci sequence, and we are free to choose the numbers A and B to have any values that we want.

The idea now is to choose A and B so that the H_n sequence and the Fibonacci sequence start with the same two values. In other words, we want to choose A and B such that

$$H_1 = F_1 = 1 \quad \text{and} \quad H_2 = F_2 = 1.$$

This means we need to solve

$$A\alpha + B\beta = 1 \quad \text{and} \quad A\alpha^2 + B\beta^2 = 1.$$

(Remember that α and β are specific numbers.) These two equations are easy to solve. We use $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$ to rewrite the second equation as

$$A(\alpha + 1) + B(\beta + 1) = 1.$$

Subtracting the first equation from this gives

$$A + B = 0, \quad \text{so} \quad B = -A.$$

Substituting $B = -A$ into the first equation gives

$$A\alpha - A\beta = 1,$$

which lets us solve for

$$A = 1/(\alpha - \beta) = 1/\sqrt{5}.$$

Also $B = -A = -1/\sqrt{5}$, which gives us the formula

$$H_n = (\alpha^n - \beta^n)/\sqrt{5}.$$

The culmination of our calculations is the following beautiful formula for the n^{th} term of the Fibonacci sequence. It is named after Binet, who published it in 1843, although the formula was known to Euler and to Daniel Bernoulli at least 100 years earlier.

Theorem 7.1 (Binet's Formula). *The Fibonacci sequence F_n is the sequence described by the recursion*

$$F_1 = F_2 = 1 \quad \text{and} \quad F_n = F_{n-1} + F_{n-2} \quad \text{for } n = 3, 4, 5, \dots$$

Then the n^{th} term of the Fibonacci sequence is given by the formula

$$F_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right\}.$$

Proof. For each number $n = 1, 2, 3, \dots$, let H_n be the number

$$H_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right\}.$$

We will prove by induction on n that $H_n = F_n$ for every number n .

First we check that

$$H_1 = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1 + \sqrt{5}}{2} \right) - \left(\frac{1 - \sqrt{5}}{2} \right) \right\} = \frac{1}{\sqrt{5}} \cdot \sqrt{5} = 1$$

and

$$\begin{aligned} H_2 &= \frac{1}{\sqrt{5}} \left\{ \left(\frac{1 + \sqrt{5}}{2} \right)^2 - \left(\frac{1 - \sqrt{5}}{2} \right)^2 \right\} \\ &= \frac{1}{\sqrt{5}} \left\{ \frac{6 + 2\sqrt{5}}{4} - \frac{6 - 2\sqrt{5}}{4} \right\} = \frac{1}{\sqrt{5}} \cdot \frac{4\sqrt{5}}{4} = 1. \end{aligned}$$

This shows that $H_1 = F_1$ and $H_2 = F_2$.

Now suppose that $n \geq 3$ and that $H_i = F_i$ for every value of i between 1 and $n-1$. In particular, $H_{n-1} = F_{n-1}$ and $H_{n-2} = F_{n-2}$. We need to prove that $H_n = F_n$. But we have already checked that

$$H_n = H_{n-1} + H_{n-2},$$

and we know from the definition of the Fibonacci sequence that

$$F_n = F_{n-1} + F_{n-2},$$

so we see that $H_n = F_n$. This completes our induction proof that $H_n = F_n$ for every value of n . \square

7.2 The Fibonacci Sequence Modulo m

What happens to the numbers in the Fibonacci sequence if we reduce them modulo m ? There are only finitely many different numbers modulo m , so the values do not get larger and larger. As always, we start by computing some examples.

Here's what the Fibonacci sequence modulo m looks like for the first few values of m .

$$\begin{aligned} F_n \pmod{2} & \quad \mathbf{1,1,0,1,1,0,1,1,0,1,1,0} \dots \\ F_n \pmod{3} & \quad \mathbf{1,1,2,0,2,2,1,0,1,1,2,0,2,2,1} \dots \\ F_n \pmod{4} & \quad \mathbf{1,1,2,3,1,0,1,1,2,3,1,0,1,1,2} \dots \\ F_n \pmod{5} & \quad \mathbf{1,1,2,3,0,3,3,1,4,0,4,3,2,0,2,2,4,1,0,1,1,2} \dots \\ F_n \pmod{6} & \quad \mathbf{1,1,2,3,5,2,1,3,4,1,5,0,5,5,4,3,1,4,5,3,2,5,1,0,1,1,2,3} \dots \end{aligned}$$

Notice in each case that the Fibonacci sequence eventually starts to repeat. In other words, when we compute the Fibonacci sequence modulo m , we eventually find two consecutive 1's appearing, and as soon this happens, the sequence repeats. (We leave as an exercise for you to prove that this always happens.) Thus there is an integer $N \geq 1$ such that

$$F_{n+N} \equiv F_n \pmod{m} \quad \text{for all } n = 1, 2, \dots$$

The smallest such integer N is called the *period of the Fibonacci sequence modulo m* . We denote it by $N(m)$. The preceding examples give us the following short table:

| m | 2 | 3 | 4 | 5 | 6 |
|--------|---|---|---|----|----|
| $N(m)$ | 3 | 8 | 6 | 20 | 24 |

The period of the Fibonacci sequence modulo m exhibits many interesting patterns, but our brief table is much too short to use in making conjectures. For now we concentrate on the case that the modulus is a prime p . Table 7.5 lists the period $N(p)$

for all primes $p \leq 229$. Looking at the first two columns of the table, we immediately notice the five values

$$N(11) = 10, \quad N(31) = 30, \quad N(41) = 40, \quad N(61) = 60, \quad N(71) = 70,$$

so we might be tempted to conjecture that if $p \equiv 1 \pmod{10}$, then $N(p) = p - 1$. Unfortunately, this conjecture is not correct, since later entries in the table include

$$N(101) = 50, \quad N(151) = 50, \quad N(181) = 90, \quad \text{and} \quad N(211) = 42.$$

However, we observe that in all cases the period $N(p)$ divides $p - 1$. This suggests that we look at the list of the primes p satisfying $N(p) \mid p - 1$,

$$11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, \\ 151, 179, 181, 191, 199, 211, 229, \dots$$

The pattern is obvious. These are the primes that are congruent to 1 or 9 modulo 10, which is the same as the set of primes that are congruent to 1 or 4 modulo 5. So we are led to conjecture that

$$p \equiv 1 \text{ or } 4 \pmod{5} \stackrel{?}{\implies} N(p) \mid p - 1. \quad (7.1)$$

We sketch a proof of this conjecture in Section 9.2.2, although we will not have time to discuss it in class.

This concludes our discussion about the period of the Fibonacci sequence modulo m , but there are many other questions to ask and many more patterns to be discovered. For example:

Are there infinitely many primes satisfying $N(p) = p - 1$?

This is not currently known! In Exercises 7.12–7.15 you will be asked to investigate further the values of $N(m)$ for both prime and composite values of m .

7.3 The Fibonacci Sequence: Supplement

We include some additional material that will not be covered in class. And no, it won't be on the exam, either!



7.3.1 An Historical Interlude

The number

$$\frac{1 + \sqrt{5}}{2} = 1.61803\dots$$

| p | $N(p)$ | p | $N(p)$ | p | $N(p)$ | p | $N(p)$ | p | $N(p)$ |
|-----|--------|-----|--------|-----|--------|-----|--------|-----|--------|
| 2 | 3 | 31 | 30 | 73 | 148 | 127 | 256 | 179 | 178 |
| 3 | 8 | 37 | 76 | 79 | 78 | 131 | 130 | 181 | 90 |
| 5 | 20 | 41 | 40 | 83 | 168 | 137 | 276 | 191 | 190 |
| 7 | 16 | 43 | 88 | 89 | 44 | 139 | 46 | 193 | 388 |
| 11 | 10 | 47 | 32 | 97 | 196 | 149 | 148 | 197 | 396 |
| 13 | 28 | 53 | 108 | 101 | 50 | 151 | 50 | 199 | 22 |
| 17 | 36 | 59 | 58 | 103 | 208 | 157 | 316 | 211 | 42 |
| 19 | 18 | 61 | 60 | 107 | 72 | 163 | 328 | 223 | 448 |
| 23 | 48 | 67 | 136 | 109 | 108 | 167 | 336 | 227 | 456 |
| 29 | 14 | 71 | 70 | 113 | 76 | 173 | 348 | 229 | 114 |

Table 7.5: The Period of the Fibonacci Sequence Modulo the Prime p

is often called the *Golden Ratio*, although it has many other names, including for example the *Divine Proportion*. The first recorded definition appears in Euclid's *Elements*, where it was called the *extreme and mean ratio*.² Various authors have attributed aesthetic merit to artistic compositions built on the divine proportion. For example, it has been suggested that the Parthenon was designed so that its exterior dimensions are in the golden ratio. Here is a small rectangle  whose sides are in the golden ratio, and here is a larger divinely proportioned rectangle . Do you find the proportions of these rectangles to be especially pleasing to the eye?

7.3.2 General Linear Recurrences

The Fibonacci sequence is an example of a *Linear Recurrence Sequence*. The word *linear* in this context means that the n^{th} term of the sequence is a linear combination of some of the previous terms. Here are examples of some other linear recurrence sequences:

$$\begin{array}{llll}
 A_n = 3A_{n-1} + 10A_{n-2} & A_1 = 1 & A_2 = 3 & \\
 B_n = 2B_{n-1} - 4B_{n-2} & B_1 = 0 & B_2 = -2 & \\
 C_n = 4C_{n-1} - C_{n-2} - 6C_{n-3} & C_1 = 0 & C_2 = 0 & C_3 = 1
 \end{array}$$

The method that we used to derive Binet's Formula for the n^{th} Fibonacci number can be used, *mutatis mutandis*,³ to find a formula for the n^{th} term of any linear recurrence

²Euclid's definition says that "a straight line is said to have been cut in *extreme and mean ratio* when, as the whole line is to the greater segment, so is the greater to the lesser. This means that the line segment of length L is split into two pieces, the larger having length a and the smaller length b , these pieces satisfy $\frac{L}{b} = \frac{b}{a}$. Since $L = a + b$, we can rewrite this as $\frac{L}{b} = \frac{b}{L-b}$. Clearing the denominators and bringing everything to one side of the equation gives $L^2 - bL - b^2 = 0$, and then the quadratic formula tells us that $\frac{L}{b} = \frac{1+\sqrt{5}}{2}$ equals to golden ratio.

³A useful Latin phrase meaning "the necessary changes having been made." The implication, of course, is that the necessary changes are relatively minor.

sequence. Of course, not all recurrence sequences are linear. Here are some examples of recurrence sequences that are not linear:

$$\begin{aligned} D_n &= D_{n-1} + D_{n-2}^2 & D_1 &= 1 & D_2 &= 1 \\ E_n &= E_{n-1}E_{n-2} + E_{n-3} & E_1 &= 1 & E_2 &= 2 & E_3 &= 1 \end{aligned}$$

In general, there is no simple expression for the n^{th} term of a nonlinear recurrence sequence. This does not mean that nonlinear sequences are uninteresting, quite the contrary, but it does mean that they are much harder to analyze than linear recurrence sequences.

Exercises

- 7.1.** (a) Look at a table of Fibonacci numbers and compare the values of F_m and F_{mn} for various choices of m and n . Try to find a pattern. [*Hint.* Look for a divisibility pattern.]
 (b) Prove that the pattern you found in (a) is true.
 (c) If $\gcd(m, n) = 1$, try to find a stronger pattern involving the values of F_m , F_n , and F_{mn} .
 (d) Is the pattern that you found in (c) still true if $\gcd(m, n) \neq 1$?
 (e) Prove that the pattern you found in (c) is true.

- 7.2.** (a) Find as many square Fibonacci numbers as you can. Do you think that there are finitely many or infinitely many square Fibonacci numbers?
 (b) Find as many triangular Fibonacci numbers as you can. Do you think there are finitely many or infinitely many triangular Fibonacci numbers?

- 7.3.** (a) Make a list of Fibonacci numbers F_n that are prime.
 (b) Using your data, fill in the box to make an interesting conjecture:

If F_n is prime, then n is .

[*Hint.* Actually, your conjecture should be that the statement is true with one exception.]

- (c) Does your conjecture in (b) work in the other direction? In other words, is the following statement true, where the box is the same as in (b)?

If n is , then F_n is prime.

- (d) Prove that your conjecture in (b) is correct.

- 7.4.** The Fibonacci numbers satisfy many amazing identities.

- (a) Compute the quantity $F_{n+1}^2 - F_{n-1}^2$ for the first few integers $n = 2, 3, 4, \dots$ and try to guess its value. [*Hint.* It is equal to a Fibonacci number.] Prove that your guess is correct.
 (b) Same question (and same hint!) for the quantity $F_{n+1}^3 + F_n^3 - F_{n-1}^3$.
 (c) Same question (and almost the same hint!) for the quantity $F_{n+2}^2 - F_{n-2}^2$.
 (d) Same question (but not the same hint!) for the quantity $F_{n-1}F_{n+1} - F_n^2$.
 (e) Same question for $4F_nF_{n-1} + F_{n-2}^2$. [*Hint.* Compare the value with the square of a Fibonacci number.]
 (f) Same question for the quantity $F_{n+4}^4 - 4F_{n+3}^4 - 19F_{n+2}^4 - 4F_{n+1}^4 + F_n^4$.

7.5. The *Lucas sequence* is the sequence of numbers L_n given by the rules $L_1 = 1$, $L_2 = 3$, and $L_n = L_{n-1} + L_{n-2}$.

- Write down the first 10 terms of the Lucas sequence.
- Find a simple formula for L_n , similar to Binet's Formula for the Fibonacci number F_n .
- Compute the value of $L_n^2 - 5F_n^2$ for each $1 \leq n \leq 10$. Make a conjecture about this value. Prove that your conjecture is correct.
- Show that L_{3n} and F_{3n} are even for all values of n . Combining this fact with the formula you discovered in (c), find an interesting equation satisfied by the pair of numbers $(\frac{1}{2}L_{3n}, \frac{1}{2}F_{3n})$. Relate your answer to Exercise 1.7.

7.6. Write down the first few terms for each of the following linear recursion sequences, and then find a formula for the n^{th} term similar to Binet's formula for the n^{th} Fibonacci number. Be sure to check that your formula is correct for the first few values.

- $A_n = 3A_{n-1} + 10A_{n-2}$ $A_1 = 1$ $A_2 = 3$
- $B_n = 2B_{n-1} - 4B_{n-2}$ $B_1 = 0$ $B_2 = -2$
- $C_n = 4C_{n-1} - C_{n-2} - 6C_{n-3}$ $C_1 = 0$ $C_2 = 0$ $C_3 = 1$

[Hint. For (b), you'll need to use complex numbers. For (c), the cubic polynomial has some small integer roots.]

7.7. Let P_n be the linear recursion sequence defined by

$$P_n = P_{n-1} + 4P_{n-2} - 4P_{n-3}, \quad P_1 = 1, \quad P_2 = 9, \quad P_3 = 1.$$

- Write down the first 10 terms of P_n .
- Does the sequence behave in a strange manner?
- Find a formula for P_n that is similar to Binet's formula. Does your formula for P_n explain the strange behavior that you noted in (b)?

7.8. (This question requires some elementary calculus.)

- Compute the value of the limit

$$\lim_{n \rightarrow \infty} \frac{\log(F_n)}{n}.$$

Here F_n is the n^{th} Fibonacci number.

- Compute $\lim_{n \rightarrow \infty} (\log(A_n))/n$, where A_n is the sequence in Exercise 7.6(a).
- Compute $\lim_{n \rightarrow \infty} (\log(|B_n|))/n$, where B_n is the sequence in Exercise 7.6(b).
- Compute $\lim_{n \rightarrow \infty} (\log(C_n))/n$, where C_n is the sequence in Exercise 7.6(c).

7.9. Write down the first few terms for each of the following nonlinear recursion sequences. Can you find a simple formula for the n^{th} term? Can you find any patterns in the list of terms?

- $D_n = D_{n-1} + D_{n-2}^2$ $D_1 = 1$ $D_2 = 1$
- $E_n = E_{n-1}E_{n-2} + E_{n-3}$ $E_1 = 1$ $E_2 = 2$ $E_3 = 1$

7.10. Prove that the Fibonacci sequence modulo m eventually repeats with two consecutive 1's. [Hint. The Fibonacci recursion can also be used backwards. Thus if you know the values of F_n and F_{n+1} , then you can recover the value of F_{n-1} using $F_{n-1} = F_{n+1} - F_n$.]

7.11. Let $N = N(m)$ be the period of Fibonacci sequence modulo m .

- What is the value of F_N modulo m ? What is the value of F_{N-1} modulo m ?

- (b) Write out the Fibonacci sequence modulo m in the reverse direction,

$$F_{N-1}, F_{N-2}, F_{N-3}, \dots, F_3, F_2, F_1 \pmod{m}.$$

Do this for several values of m , and try to find a pattern. [Hint. The pattern will be more evident if you take some of the values modulo m to lie between $-m$ and -1 , instead of between 1 and m .]

- (c) Prove that the pattern you found in (b) is correct.

7.12. The material in Table 7.6 suggests that if $m \geq 3$ then the period $N(m)$ of the Fibonacci sequence modulo m is always an even number. Prove that this is true, or find a counterexample.

7.13. Let $N(m)$ be the period of the Fibonacci sequence modulo m .

- (a) Use Table 7.6 to compare the values of $N(m_1)$, $N(m_2)$, and $N(m_1 m_2)$ for various values of m_1 and m_2 , especially for $\gcd(m_1, m_2) = 1$.
 (b) Make a conjecture relating $N(m_1)$, $N(m_2)$, and $N(m_1 m_2)$ when m_1 and m_2 satisfy $\gcd(m_1, m_2) = 1$.
 (c) Use your conjecture from (b) to guess the values of $N(5184)$ and $N(6887)$. [Hint. $6887 = 71 \cdot 97$.]
 (d) Prove that your conjecture in (b) is correct.

| m | $N(m)$ | m | $N(m)$ | m | $N(m)$ | m | $N(m)$ | m | $N(m)$ |
|-----|--------|-----|--------|-----|--------|-----|--------|-----|--------|
| 1 | — | 21 | 16 | 41 | 40 | 61 | 60 | 81 | 216 |
| 2 | 3 | 22 | 30 | 42 | 48 | 62 | 30 | 82 | 120 |
| 3 | 8 | 23 | 48 | 43 | 88 | 63 | 48 | 83 | 168 |
| 4 | 6 | 24 | 24 | 44 | 30 | 64 | 96 | 84 | 48 |
| 5 | 20 | 25 | 100 | 45 | 120 | 65 | 140 | 85 | 180 |
| 6 | 24 | 26 | 84 | 46 | 48 | 66 | 120 | 86 | 264 |
| 7 | 16 | 27 | 72 | 47 | 32 | 67 | 136 | 87 | 56 |
| 8 | 12 | 28 | 48 | 48 | 24 | 68 | 36 | 88 | 60 |
| 9 | 24 | 29 | 14 | 49 | 112 | 69 | 48 | 89 | 44 |
| 10 | 60 | 30 | 120 | 50 | 300 | 70 | 240 | 90 | 120 |
| 11 | 10 | 31 | 30 | 51 | 72 | 71 | 70 | 91 | 112 |
| 12 | 24 | 32 | 48 | 52 | 84 | 72 | 24 | 92 | 48 |
| 13 | 28 | 33 | 40 | 53 | 108 | 73 | 148 | 93 | 120 |
| 14 | 48 | 34 | 36 | 54 | 72 | 74 | 228 | 94 | 96 |
| 15 | 40 | 35 | 80 | 55 | 20 | 75 | 200 | 95 | 180 |
| 16 | 24 | 36 | 24 | 56 | 48 | 76 | 18 | 96 | 48 |
| 17 | 36 | 37 | 76 | 57 | 72 | 77 | 80 | 97 | 196 |
| 18 | 24 | 38 | 18 | 58 | 42 | 78 | 168 | 98 | 336 |
| 19 | 18 | 39 | 56 | 59 | 58 | 79 | 78 | 99 | 120 |
| 20 | 60 | 40 | 60 | 60 | 120 | 80 | 120 | 100 | 300 |

Table 7.6: The Period $N(m)$ of the Fibonacci Sequence Modulo m

7.14. Let $N(m)$ be the period of the Fibonacci sequence modulo m .

- (a) Use Table 7.6 to compare the values of $N(p)$ and $N(p^2)$ for various primes p .

- (b) Make a conjecture relating the values of $N(p)$ and $N(p^2)$ when p is a prime.
- (c) More generally, make a conjecture relating the value of $N(p)$ to the values of all the higher powers $N(p^2), N(p^3), N(p^4), \dots$.
- (d) Use your conjectures from (b) and (c) to guess the values of $N(2209)$, $N(1024)$, and $N(729)$. [Hint. $2209 = 47^2$. You can factor 1024 and 729 yourself!]
- (e) Try to prove your conjectures in (b) and/or (c).

7.15. Let $N(m)$ be the period of the Fibonacci sequence modulo m . In the text we analyzed $N(p)$ when p is a prime satisfying $p \equiv 1$ or 4 modulo 5 . This exercise asks you to consider the other primes.

- (a) Use Table 7.5 on page 77 to make a list of the periods $N(p)$ of the Fibonacci sequence modulo p when p is a prime number satisfying $p \equiv 2$ or 3 modulo 5 .
- (b) If $p \equiv 1$ or 4 modulo 5 , we proved that $N(p)$ divides $p - 1$. Formulate a similar conjecture for the primes that satisfy $p \equiv 2$ or 3 modulo 5 .
- (c) Try to prove your conjecture in (b). (This is probably hard using only the tools that you currently know.)
- (d) The one prime that we have not considered is $p = 5$. For various values of c , look at the sequence

$$n \cdot c^{n-1} \pmod{5}, \quad n = 1, 2, 3, \dots,$$

and compare it with the Fibonacci sequence modulo 5 . Make a conjecture, and then prove that your conjecture is correct.

7.16. A *Markoff triple* is a triple of positive integers (x, y, z) that satisfies the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

There is one obvious Markoff triple, namely $(1, 1, 1)$, as well as many non-obvious triples, for example $(2, 5, 29)$ and $(13, 34, 1325)$.

- (a) Find all Markoff triples that satisfy $x = y$.
- (b) Let (x_0, y_0, z_0) be a Markoff triple. Show that the following are also Markoff triples:

$$F(x_0, y_0, z_0) = (x_0, z_0, 3x_0z_0 - y_0),$$

$$G(x_0, y_0, z_0) = (y_0, z_0, 3y_0z_0 - x_0),$$

$$H(x_0, y_0, z_0) = (x_0, y_0, 3x_0y_0 - z_0).$$

This gives several ways to create new Markoff triples from old ones, similar to the way that we created new Fibonacci number from old ones.

- (c) Starting with the Markoff triple $(1, 1, 1)$, repeatedly apply the functions F and G described in (b) to create at least eight more Markoff triples.⁴ Arrange them in a picture with two Markoff triples connected by a line segment if one is obtained from the other by using F or G .
- (d) Prove that $(1, F_{2k-1}, F_{2k+1})$ is a Markoff triple for all $k \geq 1$.

⁴Markoff proved that every Markoff triple can be obtained by starting from $(1, 1, 1)$ and repeatedly applying F , G , and H .

Chapter 8

Number Theory — Lecture #8

8.1 Squares Modulo p

In Section 5.1 (Theorem 5.1) we learned how to solve linear congruences,

$$ax \equiv c \pmod{m}.$$

It's now time to take the plunge and move on to quadratic equations. We will look at the following types of questions:

- Is 3 congruent to the square of some number modulo 7?
- Does the congruence $x^2 \equiv -1 \pmod{13}$ have a solution?
- For which primes p does the congruence $x^2 \equiv 2 \pmod{p}$ have a solution?

We can answer the first two questions right now. To see if 3 is congruent to the square of some number modulo 7, we just square each of the numbers from 0 to 6, reduce modulo 7, and see if any of them is equal to 3. Thus,

$$\begin{aligned}0^2 &\equiv 0 \pmod{7} \\1^2 &\equiv 1 \pmod{7} \\2^2 &\equiv 4 \pmod{7} \\3^2 &\equiv 2 \pmod{7} \\4^2 &\equiv 2 \pmod{7} \\5^2 &\equiv 4 \pmod{7} \\6^2 &\equiv 1 \pmod{7}.\end{aligned}$$

So we see that 3 is not congruent to a square modulo 7. In a similar fashion, if we square each number from 0 to 12 and reduce modulo 13, we find that the congruence $x^2 \equiv -1 \pmod{13}$ has two solutions, $x \equiv 5 \pmod{13}$ and $x \equiv 8 \pmod{13}$.¹

¹For many years during the nineteenth century, mathematicians were uneasy with the idea of the number $\sqrt{-1}$. Its current appellation “imaginary number” still reflects that disquiet. But if you work mod-

As always, we need to look at some data before we can even begin to look for patterns and make conjectures. Here are some tables giving all the squares modulo p for $p = 5, 7, 11$, and 13 .

| b | b^2 |
|-----|-------|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 4 |
| 4 | 1 |

Modulo 5

| b | b^2 |
|-----|-------|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 2 |
| 4 | 2 |
| 5 | 4 |
| 6 | 1 |

Modulo 7

| b | b^2 |
|-----|-------|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 5 |
| 5 | 3 |
| 6 | 3 |
| 7 | 5 |
| 8 | 9 |
| 9 | 4 |
| 10 | 1 |

Modulo 11

| b | b^2 |
|-----|-------|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 3 |
| 5 | 12 |
| 6 | 10 |
| 7 | 10 |
| 8 | 12 |
| 9 | 3 |
| 10 | 9 |
| 11 | 4 |
| 12 | 1 |

Modulo 13

Many interesting patterns are already apparent from these lists. For example, each number (other than 0) that appears as a square seems to appear exactly twice. Thus, 5 is both 4^2 and 7^2 modulo 11, and 3 is both 4^2 and 9^2 modulo 13. In fact, if we fold each list over in the middle, the same numbers appear as squares on the top and on the bottom.

How can we describe this pattern with a formula? We are saying that the square of the number b and the square of the number $p - b$ are the same modulo p . But now that we've described our pattern by a formula, it's easy to prove. Thus,

$$(p - b)^2 = p^2 - 2pb + b^2 \equiv b^2 \pmod{p}.$$

So if we want to list all the (nonzero) numbers that are squares modulo p , we only need to compute half of them:

$$1^2 \pmod{p}, \quad 2^2 \pmod{p}, \quad 3^2 \pmod{p}, \dots, \quad \left(\frac{p-1}{2}\right)^2 \pmod{p}.$$

Our goal is to find patterns that can be used to distinguish squares from nonsquares modulo p . Ultimately, we will be led to one of the most beautiful theorems in all

ulo 13, for example, then there's nothing mysterious about $\sqrt{-1}$. In fact, 5 and 8 are both square roots of -1 modulo 13.

number theory, the Law of Quadratic Reciprocity, but first we must perform the mundane task of assigning some names to the numbers we want to study.

A nonzero number that is congruent to a square modulo p is called a *quadratic residue modulo p* . A number that is not congruent to a square modulo p is called a *(quadratic) nonresidue modulo p* . We abbreviate these long expressions by saying that a quadratic residue is a QR and a quadratic nonresidue is an NR. A number that is congruent to 0 modulo p is neither a residue nor a nonresidue.

To illustrate this terminology using the data from our tables:

3 and 12 are QRs modulo 13.

2 and 5 are NRs modulo 13.

Note that 2 and 5 are NRs because they do not appear in the list of squares modulo 13. The full set of QRs modulo 13 is $\{1, 3, 4, 9, 10, 12\}$, and the full set of NRs modulo 13 is $\{2, 5, 6, 7, 8, 11\}$. Similarly, the set of QRs modulo 7 is $\{1, 2, 4\}$ and the set of NRs modulo 7 is $\{3, 5, 6\}$.

Notice that there are six quadratic residues and six nonresidues modulo 13, and there are three quadratic residues and three nonresidues modulo 7. Using our earlier observation that $(p - b)^2 \equiv b^2 \pmod{p}$, we can easily verify that there are an equal number of quadratic residues and nonresidues modulo any (odd) prime.

Theorem 8.1. *Let p be an odd prime. Then there are exactly $(p - 1)/2$ quadratic residues modulo p and exactly $(p - 1)/2$ nonresidues modulo p .*

Proof. The quadratic residues are the nonzero numbers that are squares modulo p , so they are the numbers

$$1^2, 2^2, \dots, (p - 1)^2 \pmod{p}.$$

But, as we noted above, we only need to go halfway,

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p},$$

since the same numbers are repeated in reverse order if we square the remaining numbers

$$\left(\frac{p+1}{2}\right)^2, \dots, (p-2)^2, (p-1)^2 \pmod{p}.$$

So in order to show that there are exactly $(p - 1)/2$ quadratic residues, we need to check that the numbers $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ are all different modulo p .

Suppose that b_1 and b_2 are numbers between 1 and $(p - 1)/2$, and suppose that $b_1^2 \equiv b_2^2 \pmod{p}$. We want to show that $b_1 = b_2$. The fact that $b_1^2 \equiv b_2^2 \pmod{p}$ means that

$$p \text{ divides } b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2).$$

However, $b_1 + b_2$ is between 2 and $p - 1$, so it can't be divisible by p . Thus p must divide $b_1 - b_2$. But $|b_1 - b_2| < (p - 1)/2$, so the only way for $b_1 - b_2$ to be divisible by p is to have $b_1 = b_2$. This shows that the numbers $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ are all different modulo p , so there are exactly $(p - 1)/2$ quadratic residues modulo p . Now we need only observe that there are $p - 1$ numbers between 1 and $p - 1$, so if half of them are quadratic residues, the other half must be nonresidues. \square

Suppose that we take two quadratic residues and multiply them together. Do we get a QR or an NR, or do we sometimes get one and sometimes the other? For example, 3 and 10 are QRs modulo 13, and their product $3 \cdot 10 = 30 \equiv 4$ is again a QR modulo 13. Actually, this should have been clear without any computation, since if we multiply two squares, we should get a square. We can formally verify this in the following way. Suppose that a_1 and a_2 are both QRs modulo p . This means that there are numbers b_1 and b_2 such that $a_1 \equiv b_1^2 \pmod{p}$ and $a_2 \equiv b_2^2 \pmod{p}$. Multiplying these two congruences together, we find that $a_1 a_2 \equiv (b_1 b_2)^2 \pmod{p}$, which shows that $a_1 a_2$ is a QR.

The situation is less clear if we multiply a QR by an NR, or if we multiply two NRs together. Here are some examples using the data in our tables:

| QR \times NR $\equiv ?? \pmod{p}$ | | | NR \times NR $\equiv ?? \pmod{p}$ | | |
|-------------------------------------|----|--|-------------------------------------|----|--|
| $2 \times 5 \equiv 3 \pmod{7}$ | NR | | $3 \times 5 \equiv 1 \pmod{7}$ | QR | |
| $5 \times 6 \equiv 8 \pmod{11}$ | NR | | $6 \times 7 \equiv 9 \pmod{11}$ | QR | |
| $4 \times 5 \equiv 7 \pmod{13}$ | NR | | $5 \times 11 \equiv 3 \pmod{13}$ | QR | |
| $10 \times 7 \equiv 5 \pmod{13}$ | NR | | $7 \times 11 \equiv 12 \pmod{13}$ | QR | |

Thus, multiplying a quadratic residue and a nonresidue seems to yield a nonresidue, while the product of two nonresidues always seems to be a residue. Symbolically, we might write

$$\text{QR} \times \text{QR} = \text{QR}, \quad \text{QR} \times \text{NR} = \text{NR}, \quad \text{NR} \times \text{NR} = \text{QR}.$$

We've already seen that the first relation is true, and we now verify the other two relations.

Theorem 8.2 (Quadratic Residue Multiplication Rule). (Version 1) *Let p be an odd prime. Then:*

- (i) *The product of two quadratic residues modulo p is a quadratic residue.*
- (ii) *The product of a quadratic residue and a nonresidue is a nonresidue.*
- (iii) *The product of two nonresidues is a quadratic residue.*

These three rules can be summarized symbolically by the formulas

$$\text{QR} \times \text{QR} = \text{QR}, \quad \text{QR} \times \text{NR} = \text{NR}, \quad \text{NR} \times \text{NR} = \text{QR}.$$

Proof. We have already seen that $\text{QR} \times \text{QR} = \text{QR}$. Suppose next that a_1 is a QR, say $a_1 \equiv b_1^2 \pmod{p}$, and that a_2 is an NR. We are going to assume that $a_1 a_2$ is

a QR and derive a contradiction. The assumption that $a_1 a_2$ is a QR means that it is congruent to b_3^2 for some b_3 , so we have

$$b_3^2 \equiv a_1 a_2 \equiv b_1^2 a_2 \pmod{p}.$$

Note that $\gcd(b_1, p) = 1$, since $p \nmid a_1$ and $a_1 = b_1^2$, so the Linear Congruence Theorem (Theorem 8.1) says that we can find an inverse for b_1 modulo p . In other words, we can find some c_1 such that $c_1 b_1 \equiv 1 \pmod{p}$. Multiplying both sides of the above congruence by c_1^2 gives

$$c_1^2 b_3^2 \equiv c_1^2 a_1 a_2 \equiv (c_1 b_1)^2 a_2 \equiv a_2 \pmod{p}.$$

Thus $a_2 \equiv (c_1 b_3)^2 \pmod{p}$ is a QR, contradicting the fact that a_2 is a NR. This completes the proof that

$$\text{QR} \times \text{NR} = \text{NR}.$$

We are left to deal with the product of two NRs. Let a be an NR and consider the set of values

$$a, 2a, 3a, \dots, (p-2)a, (p-1)a \pmod{p}.$$

By an argument we've used before (see Lemma 5.3 on page 52), these are just the numbers $1, 2, \dots, (p-1)$ rearranged in some different order. In particular, they include the $\frac{1}{2}(p-1)$ QRs and the $\frac{1}{2}(p-1)$ NRs. However, as we already proved, each time that we multiply a by a QR, we get an NR, so the $\frac{1}{2}(p-1)$ products

$$a \times \text{QR}$$

already give us all $\frac{1}{2}(p-1)$ NRs in the list. Hence when we multiply a by an NR, the only possibility is that it is equal to one of the QRs in the list, because the $a \times \text{QR}$ products have already used up all of the NRs in the list.² \square

This completes the proof of the quadratic residue multiplication rules. Now take a minute to stare at

$$\text{QR} \times \text{QR} = \text{QR}, \quad \text{QR} \times \text{NR} = \text{NR}, \quad \text{NR} \times \text{NR} = \text{QR}.$$

Do these rules remind you of anything? If not, here's a hint. Suppose that we try to replace the symbols QR and NR with numbers. What numbers would work? That's right, the symbol QR behaves like $+1$ and the symbol NR behaves like -1 . Notice that the somewhat mysterious third rule, the one that says that the product of two nonresidues is a quadratic residue, reflects the equally mysterious rule³

$$(-1) \times (-1) = +1.$$

²“When you have eliminated all of the quadratic residues, the remaining numbers, no matter how improbable, must be the nonresidues!” (with apologies to Sherlock Holmes and Sir Arthur Conan Doyle).

³You may no longer consider the formula $(-1) \times (-1) = +1$ mysterious, since it's so familiar to you. But you should have found it mysterious the first time you saw it. And if you stop to think about it, there is no obvious reason why the product of two negative numbers should equal a positive number. Can you come up with a convincing argument that $(-1) \times (-1)$ must equal $+1$?

Having observed that QRs behave like $+1$ and NRs behave like -1 , Adrien-Marie Legendre introduced the following useful notation.

The *Legendre symbol* of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a nonresidue modulo } p. \end{cases}$$

For example, data from our earlier tables says that

$$\left(\frac{3}{13}\right) = 1, \quad \left(\frac{11}{13}\right) = -1, \quad \left(\frac{2}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = -1.$$

Using the Legendre symbol, our quadratic residue multiplication rules can be given by a single formula.

Theorem 8.3 (Quadratic Residue Multiplication Rule). (Version 2) *Let p be an odd prime. Then*

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

The Legendre symbol is useful for making calculations. For example, suppose that we want to know if 75 is a square modulo 97. We can compute

$$\left(\frac{75}{97}\right) = \left(\frac{3 \cdot 5 \cdot 5}{97}\right) = \left(\frac{3}{97}\right) \left(\frac{5}{97}\right) \left(\frac{5}{97}\right) = \left(\frac{3}{97}\right).$$

Notice that it doesn't matter whether $\left(\frac{5}{97}\right)$ is $+1$ or -1 , since it appears twice, and $(+1)^2 = (-1)^2 = 1$. Now we observe that $10^2 \equiv 3 \pmod{97}$, so 3 is a QR. Hence,

$$\left(\frac{75}{97}\right) = \left(\frac{3}{97}\right) = 1.$$

Of course, we were lucky in being able to recognize 3 as a QR modulo 97. Is there some way to evaluate a Legendre symbol like $\left(\frac{3}{97}\right)$ without relying on luck or trial and error? The answer is yes, which leads us to our next topic.

Exercises

8.1. Make a list of all the quadratic residues and all the nonresidues modulo 19.

8.2. For each odd prime p , we consider the two numbers

$A = \text{sum of all } 1 \leq a < p \text{ such that } a \text{ is a quadratic residue modulo } p,$

$B = \text{sum of all } 1 \leq a < p \text{ such that } a \text{ is a nonresidue modulo } p.$

For example, if $p = 11$, then the quadratic residues are

$$\begin{aligned} 1^2 &\equiv 1 \pmod{11}, & 2^2 &\equiv 4 \pmod{11}, & 3^2 &\equiv 9 \pmod{11}, \\ 4^2 &\equiv 5 \pmod{11}, & 5^2 &\equiv 3 \pmod{11}, \end{aligned}$$

so

$$A = 1 + 4 + 9 + 5 + 3 = 22 \quad \text{and} \quad B = 2 + 6 + 7 + 8 + 10 = 33.$$

- (a) Make a list of A and B for all odd primes $p < 20$.
- (b) What is the value of $A + B$? Prove that your guess is correct.
- (c) Compute $A \bmod p$ and $B \bmod p$. Find a pattern and prove that it is correct. [*Hint*. See Exercise 4.4 for a formula for $1^2 + 2^2 + \cdots + n^2$ that might be useful.]
- (d) Compile some more data and give a criterion on p which ensures that $A = B$.
- (e) [Computer Exercise] Write a computer program to compute A and B , and use it to make a table for all odd $p < 100$. If $A \neq B$, which one tends to be larger, A or B ? Try to prove that your guess is correct, but be forewarned that this is a *very* difficult problem.

Chapter 9

Number Theory — Lecture #9

9.1 Is -1 a Square Modulo p ? Is 2?

In the previous lecture we took a prime p and looked at the a 's that are quadratic residues and the a 's that are nonresidues. For example, we made a table of squares modulo 13 and used the table to see that 3 and 12 are QRs modulo 13, while 2 and 5 are NRs modulo 13.

In keeping with all of the best traditions of mathematics, we now turn this problem on its head. Rather than taking a particular prime p and listing the a 's that are QRs and NRs, we instead fix an a and ask for which primes p is a a QR. To make it clear exactly what we're asking, we start with the particular value $a = -1$. The question that we want to answer is as follows:

For which primes p is -1 a QR?

We can rephrase this question in other ways, such as “For which primes p does the congruence $x^2 \equiv -1 \pmod{p}$ have a solution?” and “For which primes p is $\left(\frac{-1}{p}\right) = 1$?”

As always, we need some data before we can make any hypotheses. We can answer our question for small primes in the usual mindless way by making a table of $1^2, 2^2, 3^2, \dots \pmod{p}$ and checking if any of the numbers are congruent to -1 modulo p . So, for example, -1 is not a square modulo 3, since $1^2 \not\equiv -1 \pmod{3}$ and $2^2 \not\equiv -1 \pmod{3}$, while -1 is a square modulo 5, since $2^2 \equiv -1 \pmod{5}$. Here's a more extensive list.

| p | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|----|------|----|----|------|-------|----|----|--------|----|
| Solution(s) to $x^2 \equiv -1 \pmod{p}$ | NR | 2, 3 | NR | NR | 5, 8 | 4, 13 | NR | NR | 12, 17 | NR |

Reading from this table, we compile the following data:

-1 is a quadratic residue for $p = 5, 13, 17, 29$.

-1 is a nonresidue for $p = 3, 7, 11, 19, 23, 31$.

It's not hard to discern the pattern. If p is congruent to 1 modulo 4, then -1 seems to be a quadratic residue modulo p , and if p is congruent to 3 modulo 4, then -1 seems to be a nonresidue. We can express this guess using Legendre symbols,

$$\left(\frac{-1}{p}\right) \stackrel{?}{=} \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Let's check our conjecture on the next few cases. The next two primes, 37 and 41, are both congruent to 1 modulo 4, and sure enough,

$$\begin{aligned} x^2 &\equiv -1 \pmod{37} \text{ has the solutions } x \equiv 6 \text{ and } 31 \pmod{37}, \text{ and} \\ x^2 &\equiv -1 \pmod{41} \text{ has the solutions } x \equiv 9 \text{ and } 32 \pmod{41}. \end{aligned}$$

Similarly, the next two primes 43 and 47 are congruent to 3 modulo 4, and we check that -1 is a nonresidue for 43 and 47. Our guess looks good!

Having successfully answered, at least conjecturally, the question of when -1 is a square modulo p , we move on to the question of when 2, the “oddest” of all primes, is a square modulo p . Just as we did with $a = -1$, we are looking for some simple characterization for the primes p such that 2 is a quadratic residue modulo p . Can you find the pattern in the following data, where the line labeled $x^2 \equiv 2$ gives the solutions to $x^2 \equiv 2 \pmod{p}$ if 2 is a quadratic residue modulo p and is marked NR if 2 is a nonresidue?

| | | | | | | | | | | |
|----------------|----|----|------|----|----|-------|----|-------|----|-------|
| p | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
| $x^2 \equiv 2$ | NR | NR | 3, 4 | NR | NR | 6, 11 | NR | 5, 18 | NR | 8, 23 |

| | | | | | | | | | | |
|----------------|----|--------|----|-------|----|----|----|----|--------|--------|
| p | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 | 71 | 73 |
| $x^2 \equiv 2$ | NR | 17, 24 | NR | 7, 40 | NR | NR | NR | NR | 12, 59 | 32, 41 |

| | | | | | | | | | | |
|----------------|-------|----|--------|--------|-----|--------|-----|-----|--------|---------|
| p | 79 | 83 | 89 | 97 | 101 | 103 | 107 | 109 | 113 | 127 |
| $x^2 \equiv 2$ | 9, 70 | NR | 25, 64 | 14, 83 | NR | 38, 65 | NR | NR | 51, 62 | 16, 111 |

Here's the list of primes separated according to whether 2 is a residue or a nonresidue.

$$\begin{aligned} 2 \text{ is a quadratic residue for } p &= 7, 17, 23, 31, 41, 47, 71, 73, \\ &\quad 79, 89, 97, 103, 113, 127 \\ 2 \text{ is a nonresidue for } p &= 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, \\ &\quad 61, 67, 83, 101, 107, 109 \end{aligned}$$

For $a = -1$, it turned out that the congruence class of p modulo 4 was crucial. Is there a similar pattern if we reduce these two lists of primes modulo 4? Here's what happens if we do.

$$\begin{aligned}
7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127 \\
&\equiv 3, 1, 3, 3, 1, 3, 3, 1, 3, 1, 1, 3, 1, 3 \pmod{4}, \\
3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109 \\
&\equiv 3, 1, 3, 1, 3, 1, 1, 3, 1, 3, 1, 3, 3, 1, 3, 1 \pmod{4}.
\end{aligned}$$

This doesn't look too promising. Maybe we should try reducing modulo 3.

$$\begin{aligned}
7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127 \\
&\equiv 1, 2, 2, 1, 2, 2, 2, 1, 1, 2, 1, 1, 2, 1 \pmod{3} \\
3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109 \\
&\equiv 0, 2, 2, 1, 1, 2, 1, 1, 2, 2, 1, 1, 2, 2, 2, 1 \pmod{3}.
\end{aligned}$$

This doesn't look any better. Let's make one more attempt before we give up. What happens if we reduce modulo 8?

$$\begin{aligned}
7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127 \\
&\equiv 7, 1, 7, 7, 1, 7, 7, 1, 7, 1, 1, 7, 1, 7 \pmod{8} \\
3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109 \\
&\equiv 3, 5, 3, 5, 3, 5, 5, 3, 5, 3, 5, 3, 5, 3, 5 \pmod{8}.
\end{aligned}$$

Eureka! It surely can't be a coincidence that the first line is all 1's and 7's and the second line is all 3's and 5's. This suggests the general rule that 2 is a quadratic residue modulo p if p is congruent to 1 or 7 modulo 8 and that 2 is a nonresidue if p is congruent to 3 or 5 modulo 8. In terms of Legendre symbols, we would write

$$\left(\frac{2}{p}\right) \stackrel{?}{=} \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases} \quad (9.1)$$

To recapitulate in broad terms, the data suggests that:

$$\begin{aligned}
-1 \text{ is a square mod } p &\iff p \text{ satisfies some condition mod } 4. \\
2 \text{ is a square mod } p &\iff p \text{ satisfies some condition mod } 8.
\end{aligned}$$

These are parts of the Law of Quadratic Reciprocity. The word "Reciprocity" refers to the fact that it converts a mod p property into a mod m property for some other m , in these cases $m = 4$ or $m = 8$. We turn now to the general problem. Our quest is to determine, for a given number a , exactly which primes p have a as a quadratic residue. We have (conjecturally) solved this problem for $a = -1$ and $a = 2$. Now we tackle the question of computing the Legendre symbol $\left(\frac{a}{p}\right)$ for other values of a . For example, suppose we want to compute $\left(\frac{70}{p}\right)$. We can use the Quadratic Residue Multiplication Rules (Theorem 8.3) to compute

$$\left(\frac{70}{p}\right) = \left(\frac{2 \cdot 5 \cdot 7}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{5}{p}\right) \left(\frac{7}{p}\right).$$

We already know how to find $\left(\frac{2}{p}\right)$, so we're left with the problem of determining $\left(\frac{5}{p}\right)$ and $\left(\frac{7}{p}\right)$.

In general, if we want to compute $\left(\frac{a}{p}\right)$ for any number a , we can start by factoring a into a product of primes, say

$$a = q_1 q_2 \cdots q_r.$$

(It's okay if some of the q_i 's are the same.) Then the Quadratic Residue Multiplication Rules give

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \cdots \left(\frac{q_r}{p}\right).$$

The moral of this story: If we know how to compute $\left(\frac{q}{p}\right)$ for primes q , then we know how to compute $\left(\frac{a}{p}\right)$ for every a .¹ Since nothing we have done so far tells us anything about $\left(\frac{q}{p}\right)$ (for fixed q and varying p), the time has come² to compile some data and use it to make some conjectures. Table 9.1 gives the value of the Legendre symbol $\left(\frac{q}{p}\right)$ for all odd primes $p, q \leq 37$.

| $p \backslash q$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|------------------|----|----|----|----|----|----|----|----|----|----|----|
| 3 | | -1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 |
| 5 | -1 | | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 |
| 7 | -1 | -1 | | 1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 |
| 11 | 1 | 1 | -1 | | -1 | -1 | -1 | 1 | -1 | 1 | 1 |
| 13 | 1 | -1 | -1 | -1 | | 1 | -1 | 1 | 1 | -1 | -1 |
| 17 | -1 | -1 | -1 | -1 | 1 | | 1 | -1 | -1 | -1 | -1 |
| 19 | -1 | 1 | 1 | 1 | -1 | 1 | | 1 | -1 | -1 | -1 |
| 23 | 1 | -1 | -1 | -1 | 1 | -1 | -1 | | 1 | 1 | -1 |
| 29 | -1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | | -1 | -1 |
| 31 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | -1 | | -1 |
| 37 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 | -1 | -1 | |

Table 9.1: The Value of the Legendre Symbol $\left(\frac{q}{p}\right)$

Before reading further, you should take some time to study Table 9.1 and try to find some patterns. Don't worry if you don't immediately discover the answer; the

¹Yet another instance of the principle that primes are the basic building blocks of number theory, so if you can solve a problem for primes, you're usually well on your way to solving it for all numbers.

²"The time has come," the Walrus said, "to talk of many things, of shoes, and primes, and residues, and cabbages and kings."

most important pattern concealed in this table is somewhat subtle. But you will find that it is well worth the effort to uncover the design on your own, since you then share the thrill of discovery with Legendre and Gauss.

Now that you've formulated your own conjectures, we'll examine the table together. We are going to compare the rows with the columns or, what amounts to the same thing, we are going to compare the entries when we reflect across the diagonal of the table. For example, the row with $p = 5$ reads

| | | | | | | | | | | | |
|----------------------------|----|---|----|----|----|----|----|----|----|----|----|
| q | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
| $\left(\frac{q}{5}\right)$ | -1 | | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 |

Similarly, the column with $q = 5$ (turned sideways to save space) is

| | | | | | | | | | | | |
|----------------------------|----|---|----|----|----|----|----|----|----|----|----|
| p | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
| $\left(\frac{5}{p}\right)$ | -1 | | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 |

They match! So we might guess that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

for all primes p . Do you see how useful a rule like this would be? We are looking for a method to calculate the Legendre symbol $\left(\frac{5}{p}\right)$, a difficult problem, but the Legendre symbol $\left(\frac{p}{5}\right)$ is easy to compute, because it only depends on p modulo 5. In other words, we know that

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 4 \pmod{5}, \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod{5}. \end{cases}$$

So if our guess that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ is correct, then we would know, for example, that 5 is a nonresidue modulo 3593, since

$$\left(\frac{5}{3593}\right) = \left(\frac{3593}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Similarly,

$$\left(\frac{5}{3889}\right) = \left(\frac{3889}{5}\right) = \left(\frac{4}{5}\right) = 1,$$

so 5 should be a quadratic residue modulo 3889, and sure enough we find that $5 \equiv 2901^2 \pmod{3889}$.

Emboldened by this success, we might guess that

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

for all primes p and q . Unfortunately, this isn't even true for the first row and column of the table. For example,

$$\left(\frac{3}{7}\right) = -1 \quad \text{and} \quad \left(\frac{7}{3}\right) = 1.$$

So sometimes $\left(\frac{q}{p}\right)$ is equal to $\left(\frac{p}{q}\right)$, and sometimes it is equal to $-\left(\frac{p}{q}\right)$. Table 9.2 table will help us find a rule explaining when they are the same and when they are opposites.

| $p \backslash q$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|------------------|---|---|---|----|----|----|----|----|----|----|----|
| 3 | | ♥ | ★ | ★ | ♥ | ♥ | ★ | ★ | ♥ | ★ | ♥ |
| 5 | ♥ | | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ |
| 7 | ★ | ♥ | | ★ | ♥ | ♥ | ★ | ★ | ♥ | ★ | ♥ |
| 11 | ★ | ♥ | ★ | | ♥ | ♥ | ★ | ★ | ♥ | ★ | ♥ |
| 13 | ♥ | ♥ | ♥ | ♥ | | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ |
| 17 | ♥ | ♥ | ♥ | ♥ | ♥ | | ♥ | ♥ | ♥ | ♥ | ♥ |
| 19 | ★ | ♥ | ★ | ★ | ♥ | ♥ | | ★ | ♥ | ★ | ♥ |
| 23 | ★ | ♥ | ★ | ★ | ♥ | ♥ | ★ | | ♥ | ★ | ♥ |
| 29 | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | | ♥ | ♥ |
| 31 | ★ | ♥ | ★ | ★ | ♥ | ♥ | ★ | ★ | ♥ | | ♥ |
| 37 | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | ♥ | |

Table 9.2: Table with ♥ if $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ and ★ if $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

Looking at this table, we can pick out the primes that have ♥-filled rows and columns:

$$p = 5, 13, 17, 29, 37.$$

The primes whose rows and columns are not exactly the same (i.e., the rows and columns containing ★'s) are

$$p = 3, 7, 11, 19, 23, 31.$$

With our previous experience, there is no mystery about these lists; the former consists of the primes that are congruent to 1 modulo 4, and the latter contains the primes that are congruent to 3 modulo 4.

So our first conjecture might be that if $p \equiv 1 \pmod{4}$ or if $q \equiv 1 \pmod{4}$ then the rows and columns are the same. We can write this in terms of Legendre symbols.

Conjecture: If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

What happens if both p and q are congruent to 3 modulo 4? Looking at the table, we find in every instance that $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ are opposites. So we are led to make a further guess.

Conjecture: If $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$, then $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

These two conjectural relations form the heart of the Law of Quadratic Reciprocity.

Theorem 9.1 (Law of Quadratic Reciprocity). *Let p and q be distinct odd primes.*

$$\begin{aligned} \left(\frac{-1}{p}\right) &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases} \\ \left(\frac{2}{p}\right) &= \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases} \\ \left(\frac{q}{p}\right) &= \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}. \end{cases} \end{aligned}$$

There is a reasonably elementary proof of the Law of Quadratic Reciprocity for $\left(\frac{-1}{p}\right)$, which we give in Supplement Section 9.3. The proof for $\left(\frac{2}{p}\right)$ is somewhat more intricate, and although there are many different proofs of the relationship between $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$, none is easy. We refer you to any standard number theory textbook for the proof.

9.1.1 An Historical Interlude

Euler and Lagrange were the first to formulate the Law of Quadratic Reciprocity, but it remained for Gauss to give the first proof in his famous monograph *Disquisitiones arithmeticae* in 1801. Gauss discovered the law for himself when he was 19, and during his lifetime he found seven different proofs! Mathematicians during the nineteenth century subsequently formulated and proved Cubic and Quartic Reciprocity Laws, and these in turn were subsumed into the Class Field Theory developed by David Hilbert, Emil Artin, and others from the 1890s through the 1920s and 1930s. During the 1960s and 1970s a number of mathematicians formulated a series of conjectures that vastly generalize Class Field Theory and that today go by the name of the Langlands Program. The fundamental theorem proved by Andrew Wiles in 1995 is a small piece of the Langlands Program, yet it sufficed to solve Fermat's 350-year-old "Last Theorem."

9.1.2 Using Quadratic Reciprocity to Compute $\left(\frac{a}{p}\right)$

The Law of Quadratic Reciprocity is not only a beautiful and subtle theoretical statement about numbers, it is also a practical tool for determining whether a number is

a quadratic residue. Essentially, it lets us flip the Legendre symbol $\left(\frac{q}{p}\right)$ and replace it by $\pm\left(\frac{p}{q}\right)$. Then we can reduce p modulo q and repeat the process. This leads to Legendre symbols with smaller and smaller entries, so eventually we arrive at Legendre symbols that we can compute. Here's an example with detailed justification for each step.

$$\begin{aligned}
 \left(\frac{14}{137}\right) &= \left(\frac{2}{137}\right)\left(\frac{7}{137}\right) && \text{Quadratic Residue Multiplication Rule,} \\
 &= \left(\frac{7}{137}\right) && \text{Quadratic Reciprocity says } \left(\frac{2}{137}\right) = 1, \\
 &&& \text{since } 137 \equiv 1 \pmod{8}, \\
 &= \left(\frac{137}{7}\right) && \text{Quadratic Reciprocity and } 137 \equiv 1 \pmod{4}, \\
 &= \left(\frac{4}{7}\right) && \text{reducing 137 modulo 7,} \\
 &= 1 && \text{since } 4 = 2^2 \text{ is certainly a square.}
 \end{aligned}$$

Thus, 14 is a quadratic residue modulo 137. In fact, the solutions to the congruence $x^2 \equiv 14 \pmod{137}$ are $x \equiv 39 \pmod{137}$ and $x \equiv 98 \pmod{137}$.

Here's a second example that illustrates how the sign can change back and forth a number of times.

$$\begin{aligned}
 \left(\frac{55}{179}\right) &= \left(\frac{5}{179}\right)\left(\frac{11}{179}\right) \\
 &= \left(\frac{179}{5}\right) \times (-1) \times \left(\frac{179}{11}\right) && \begin{array}{l} \text{since } 5 \equiv 1 \pmod{4} \text{ and} \\ 11 \equiv 179 \equiv 3 \pmod{4}, \end{array} \\
 &= \left(\frac{4}{5}\right) \times (-1) \times \left(\frac{3}{11}\right) && \begin{array}{l} \text{since } 179 \equiv 4 \pmod{5} \text{ and} \\ 179 \equiv 3 \pmod{11}, \end{array} \\
 &= 1 \times (-1) \times \left(\frac{3}{11}\right) && \text{since } 4 = 2^2 \text{ is a square,} \\
 &= 1 \times (-1) \times (-1) \times \left(\frac{11}{3}\right) && \text{since } 3 \equiv 11 \equiv 3 \pmod{4}, \\
 &= 1 \times (-1) \times (-1) \times \left(\frac{2}{3}\right) && \text{since } 11 \equiv 2 \pmod{3}, \\
 &= 1 \times (-1) \times (-1) \times (-1) && \text{since } 2 \text{ is a nonresidue mod } 3, \\
 &= -1.
 \end{aligned}$$

So 55 is a nonresidue modulo 179.

There is often more than one way to use Quadratic Reciprocity to evaluate a given Legendre symbol $\left(\frac{a}{p}\right)$, for example, by using the equality $\left(\frac{p}{q}\right) = \left(\frac{p-q}{q}\right)$. Thus we can compute $\left(\frac{299}{397}\right)$ as

$$\begin{aligned}\left(\frac{299}{397}\right) &= \left(\frac{13}{397}\right)\left(\frac{23}{397}\right) = \left(\frac{397}{13}\right)\left(\frac{397}{23}\right) = \left(\frac{7}{13}\right)\left(\frac{6}{23}\right) \\ &= \left(\frac{13}{7}\right)\left(\frac{2}{23}\right)\left(\frac{3}{23}\right) = \left(\frac{-1}{7}\right) \times 1 \times -\left(\frac{23}{3}\right) = -1 \times -\left(\frac{2}{3}\right) = -1,\end{aligned}$$

or we can compute it as

$$\left(\frac{299}{397}\right) = \left(\frac{-98}{397}\right) = \left(\frac{-1}{397}\right)\left(\frac{2}{397}\right)\left(\frac{7}{397}\right)^2 = 1 \times (-1) \times (\pm 1)^2 = -1.$$

Of course, regardless of the path taken, the final destination is always the same.

The Law of Quadratic Reciprocity furnishes an efficient way to compute the Legendre symbol $\left(\frac{a}{p}\right)$,³ even for large values of a and p . In fact, the number of steps to compute $\left(\frac{a}{p}\right)$ is more or less equal to the number of digits in p , so it is possible to evaluate Legendre symbols for numbers with hundreds of digits. We won't spend the time to do an example that is that large, but are content with the following modest example.

$$\begin{aligned}\left(\frac{37603}{48611}\right) &= \left(\frac{31}{48611}\right)\left(\frac{1213}{48611}\right) = -\left(\frac{48611}{31}\right)\left(\frac{48611}{1213}\right) \\ &= -\left(\frac{3}{31}\right)\left(\frac{91}{1213}\right) = \left(\frac{31}{3}\right)\left(\frac{7}{1213}\right)\left(\frac{13}{1213}\right) \\ &= \left(\frac{1}{3}\right)\left(\frac{1213}{7}\right)\left(\frac{1213}{13}\right) = \left(\frac{2}{7}\right)\left(\frac{4}{13}\right) = 1\end{aligned}$$

Hence, 37603 is a quadratic residue modulo 48611.

9.2 Quadratic Reciprocity to the Rescue

We now use quadratic reciprocity to help answer two questions that arose earlier:

- Are there infinitely many primes satisfying $p \equiv 1 \pmod{4}$?
- If $p \equiv 1$ or $4 \pmod{5}$, does the period of the Fibonacci sequence always divide $p - 1$?

9.2.1 Primes that are Congruent to 1 Modulo 4

As you may recall, we showed in Theorem 6.2 that there are infinitely many primes that are congruent to 3 modulo 4, but we left unanswered the analogous question for primes congruent to 1 modulo 4. Happily, we can use the first part of Quadratic Reciprocity to answer this question.

³Although we should point out that the method we've described for computing $\left(\frac{a}{p}\right)$ may require factoring large numbers. However, it turns out that $\left(\frac{a}{p}\right)$ can be computed without any factoring using a generalized version of the Law of Quadratic Reciprocity!

Theorem 9.2 (Primes 1 (Mod 4) Theorem). *There are infinitely many primes that are congruent to 1 modulo 4.*

Proof. Suppose we are given a list of primes p_1, p_2, \dots, p_r , all of which are congruent to 1 modulo 4. We are going to find a new prime, not in our list, that is congruent to 1 modulo 4. Repeating this process gives a list of any desired length.

Consider the number

$$A = (2p_1p_2 \cdots p_r)^2 + 1.$$

We know that A can be factored into a product of primes, say

$$A = q_1q_2 \cdots q_s.$$

It is clear that q_1, q_2, \dots, q_s are not in our original list, since none of the p_i 's divide A . So all we need to do is show that at least one of the q_i 's is congruent to 1 modulo 4. In fact, we'll see that all of them are.

First we note that A is odd, so all the q_i 's are odd. Next, each q_i divides A , so

$$(2p_1p_2 \cdots p_r)^2 + 1 = A \equiv 0 \pmod{q_i}.$$

This means that $x = 2p_1p_2 \cdots p_r$ is a solution to the congruence

$$x^2 \equiv -1 \pmod{q_i},$$

so -1 is a quadratic residue modulo q_i . Now Quadratic Reciprocity tells us that $q_i \equiv 1 \pmod{4}$. \square

We can use the procedure described in this proof to produce a list of primes that are congruent to 1 modulo 4. Thus, if we start with $p_1 = 5$, then we form $A = (2p_1)^2 + 1 = 101$, so our second prime is $p_2 = 101$. Then

$$A = (2p_1p_2)^2 + 1 = 1020101,$$

which is again prime, so our third prime is $p_3 = 1020101$. We'll go one more step,

$$\begin{aligned} A &= (2p_1p_2p_3)^2 + 1 \\ &= 1061522231810040101 \\ &= 53 \cdot 1613 \cdot 12417062216309. \end{aligned}$$

Notice that all the primes 53, 1613, and 12417062216309 are congruent to 1 modulo 4, just as predicted by the theory.

9.2.2 Period of the Fibonacci Sequence Modulo Primes that are Congruent to 1 or 4 Modulo 5

In Section 7.2 we studied the period $N(p)$ of the Fibonacci sequence modulo p . Thus $N(p)$ tells us how many terms it takes before the values of the Fibonacci sequence modulo p start to repeat. The data we accumulated suggested that if p is

congruent to 1 or 4 modulo 5, then $N(p)$ divides $p - 1$. One approach to proving this conjecture is to use Binet's formula modulo p , but Binet's formula involves $\sqrt{5}$. However, if p is congruent to 1 or 4 modulo 5, then Quadratic Reciprocity can be used to show that 5 is a square modulo p , leading to the following theorem and proof.

Theorem 9.3 (Fibonacci Sequence Modulo p Theorem). *Let p be a prime that is congruent to either 1 or 4 modulo 5. Then the period $N(p)$ of the Fibonacci sequence modulo p satisfies*

$$N(p) \mid p - 1.$$

Proof. We are assuming that $p \equiv 1$ or $4 \pmod{5}$, so the Law of Quadratic Reciprocity (Theorem 9.1) tells us that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) \text{ or } \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1.$$

Thus 5 is a quadratic residue modulo p , so we can find a number c with the property that $c^2 \equiv 5 \pmod{p}$. We will assume that c is odd, since if it isn't odd, we can always use $c + p$ instead. We note that $c \not\equiv 0 \pmod{p}$, so c has a mod p inverse, which we denote by c^{-1} . In other words, c^{-1} is a number satisfying $cc^{-1} \equiv 1 \pmod{p}$.

We now define a sequence of numbers modulo p by the formula

$$J_n \equiv c^{-1} \left(\left(\frac{1+c}{2} \right)^n - \left(\frac{1-c}{2} \right)^n \right) \pmod{p}.$$

(Notice that this is exactly Binet's formula if we treat c as $\sqrt{5}$.) Using the fact that $c^2 \equiv 5 \pmod{p}$, it is easy to check that

$$J_1 \equiv J_2 \equiv 1 \pmod{p} \quad \text{and} \quad J_n \equiv J_{n-1} + J_{n-2} \quad \text{for all } n \geq 3.$$

Thus the sequence J_n has the same starting values and satisfies the same recursion as the Fibonacci sequence modulo p . It follows that

$$F_n \equiv J_n \pmod{p} \quad \text{for all } n \geq 1.$$

To simplify notation, we let

$$U = \frac{1+c}{2} \quad \text{and} \quad V = \frac{1-c}{2},$$

and then

$$F_n \equiv c^{-1}(U^n - V^n) \pmod{p}.$$

In particular, we can use Fermat's Little Theorem (Theorem 5.2) to deduce that

$$\begin{aligned} F_{i+(p-1)j} &\equiv c^{-1}(U^{i+(p-1)j} - V^{i+(p-1)j}) \pmod{p} \\ &\equiv c^{-1}(U^i \cdot (U^{p-1})^j + V^i \cdot (V^{p-1})^j) \pmod{p} \\ &\equiv c^{-1}(U^i - V^i) \pmod{p} \\ &\equiv F_i \pmod{p}. \end{aligned}$$

Thus the Fibonacci sequence modulo p repeats every $p - 1$ steps.

However, the definition of $N(p)$ says that the sequence repeats every $N(p)$ steps, and that $N(p)$ is the smallest such value. We divide $p - 1$ by $N(p)$ to get a quotient and remainder

$$p - 1 = N(p)q + r \quad \text{with } 0 \leq r < N(p).$$

Using the fact that the sequence repeats every $p - 1$ steps and that it also repeats every $N(p)$ steps allows us to compute

$$F_i \equiv F_{i+(p-1)j} \equiv F_{i+N(p)qj+rj} \equiv F_{i+rj} \pmod{p}.$$

Thus the Fibonacci sequence also repeats every r steps. But $r < N(p)$, and $N(p)$ is the smallest possible positive period, so we must have $r = 0$. Hence

$$p - 1 = N(p)q,$$

which completes the proof that $N(p)$ divides $p - 1$. □

9.3 Proof that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ [Supplement]

We conjectured that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

The tool that we use to verify this conjecture might be called the “Square Root of Fermat’s Little Theorem.” How, you may well ask, does one take the square root of a theorem? Recall that Fermat’s Little Theorem (Theorem 5.2 in Section 5.2) says

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

We won’t really be taking the square root of this theorem, of course. Instead, we take the square root of the quantity a^{p-1} and ask for its value. So we want to answer the following question:

Let $A = a^{(p-1)/2}$. What is the value of A modulo p ?

One thing is obvious. If we square A , then Fermat’s Little Theorem tells us that

$$A^2 = a^{p-1} \equiv 1 \pmod{p}.$$

Hence, p divides $A^2 - 1 = (A - 1)(A + 1)$, so either p divides $A - 1$ or p divides $A + 1$. (Notice how we are using Lemma 4.1, which is the property of prime numbers that we proved on page 37.) Thus A must be congruent to either $+1$ or -1 .

Here are a few random values of p , a , and A . For comparison purposes, we have also included the value of the Legendre symbol $\left(\frac{a}{p}\right)$. Do you see a pattern?

| | | | | | | | | | | |
|----------------------------|----|----|----|----|-----|-----|-----|-----|-----|------|
| p | 11 | 31 | 47 | 97 | 173 | 409 | 499 | 601 | 941 | 1223 |
| a | 3 | 7 | 10 | 15 | 33 | 78 | 33 | 57 | 222 | 129 |
| $A \pmod{p}$ | 1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 |
| $\left(\frac{a}{p}\right)$ | 1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 |

It certainly appears that $A \equiv 1 \pmod{p}$ when a is a quadratic residue and that $A \equiv -1 \pmod{p}$ when a is a nonresidue. In other words, it looks like $A \pmod{p}$ has the same value as the Legendre symbol $\left(\frac{a}{p}\right)$. We use a counting argument to verify this assertion, which goes by the name of Euler's Criterion.

Theorem 9.4 (Euler's Criterion). *Let p be an odd prime. Then*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Proof. Suppose first that a is a quadratic residue, say $a \equiv b^2 \pmod{p}$. Then Fermat's Little Theorem (Theorem 5.2) tells us that

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

Hence $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$, which is Euler's Criterion when a is a quadratic residue.

We next consider the congruence

$$X^{(p-1)/2} - 1 \equiv 0 \pmod{p}. \quad (9.2)$$

We have just proven that every quadratic residue is a solution to this congruence, and we know from Theorem 8.1 that there are exactly $\frac{1}{2}(p-1)$ distinct quadratic residues. A polynomial of degree d can have at most d roots modulo p ,⁴ so the polynomial congruence (9.2) can have at most $\frac{1}{2}(p-1)$ distinct solutions. Hence

$$\{\text{solutions to } X^{(p-1)/2} - 1 \equiv 0 \pmod{p}\} = \{\text{quadratic residues modulo } p\}.$$

Now let a be a nonresidue. Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$, so

$$0 \equiv a^{p-1} - 1 \equiv (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \pmod{p}.$$

The first factor is not zero modulo p , because we already showed that the solutions to $X^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ are the quadratic residues. Hence the second factor must vanish modulo p , so

$$a^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}.$$

This shows that Euler's Criterion is also true for nonresidues. \square

⁴Lack of time has prevented us from proving this fact about roots of polynomials modulo p . You might try giving a proof yourself.

Using Euler's Criterion, it is very easy to determine if -1 is a quadratic residue modulo p . For example, if we want to know whether -1 is a square modulo the prime $p = 6911$, we just need to compute

$$(-1)^{(6911-1)/2} = (-1)^{3455} = -1.$$

Euler's Criterion then tells us that

$$\left(\frac{-1}{6911}\right) \equiv -1 \pmod{6911}.$$

But $\left(\frac{a}{p}\right)$ is always either $+1$ or -1 , so in this case we must have $\left(\frac{-1}{6911}\right) = -1$. Hence, -1 is a nonresidue modulo 6911 .

Similarly, for the prime $p = 7817$ we find that

$$(-1)^{(7817-1)/2} = (-1)^{3908} = 1.$$

Hence, $\left(\frac{-1}{7817}\right) = 1$, so -1 is a quadratic residue modulo 7817 . Observe that, although we now know that the congruence

$$x^2 \equiv -1 \pmod{7817}$$

has a solution, we still don't have any efficient way to find a solution. The solutions turn out to be $x \equiv 2564 \pmod{7817}$ and $x \equiv 5253 \pmod{7817}$.

As these two examples make clear, Euler's Criterion can be used to determine exactly which primes have -1 as a quadratic residue.

Theorem 9.5 (Quadratic Reciprocity). (Part I) *Let p be an odd prime. Then*

$$\begin{aligned} -1 \text{ is a quadratic residue modulo } p & \text{ if } p \equiv 1 \pmod{4}, \text{ and} \\ -1 \text{ is a nonresidue modulo } p & \text{ if } p \equiv 3 \pmod{4}. \end{aligned}$$

In other words, using the Legendre symbol,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. Euler's Criterion says that

$$(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \pmod{p}.$$

Suppose first that $p \equiv 1 \pmod{4}$, say $p = 4k + 1$. Then

$$(-1)^{(p-1)/2} = (-1)^{2k} = 1, \quad \text{so} \quad 1 \equiv \left(\frac{-1}{p}\right) \pmod{p}.$$

But $\left(\frac{-1}{p}\right)$ is either $+1$ or -1 , so it must equal 1 . This proves that if $p \equiv 1 \pmod{4}$ then $\left(\frac{-1}{p}\right) = 1$.

Next we suppose that $p \equiv 3 \pmod{4}$, say $p = 4k + 3$. Then

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1, \quad \text{so} \quad -1 \equiv \left(\frac{-1}{p}\right) \pmod{p}.$$

This shows that $\left(\frac{-1}{p}\right)$ must equal -1 , which completes the proof of Quadratic Reciprocity (Part I). \square

Exercises

9.1. Determine whether each of the following congruences has a solution. (All of the moduli are primes.)

- (a) $x^2 \equiv -1 \pmod{5987}$ (c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$
 (b) $x^2 \equiv 6780 \pmod{6781}$ (d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$

[Hint. For (c), use the quadratic formula to find out what number you need to take the square root of modulo 337, and similarly for (d).]

9.2. Use the procedure described in the Primes 1 (Mod 4) Theorem to generate a list of primes congruent to 1 modulo 4, starting with the seed $p_1 = 17$.

9.3. In Exercise 8.2 we defined A and B to be the sums of the residues, respectively non-residues, modulo p . Part (d) of that exercise asked you to find a condition on p which implies that $A = B$. Using the material in this section, prove that your criterion is correct. [Hint. The important fact you'll need is the condition for -1 to be a quadratic residue.]

9.4. Use the Law of Quadratic Reciprocity to compute the following Legendre symbols.

- (a) $\left(\frac{85}{101}\right)$ (b) $\left(\frac{29}{541}\right)$ (c) $\left(\frac{101}{1987}\right)$ (d) $\left(\frac{31706}{43789}\right)$

9.5. Does the congruence

$$x^2 - 3x - 1 \equiv 0 \pmod{31957}$$

have any solutions? [Hint. Use the quadratic formula to find out what number you need to take the square root of modulo the prime 31957.]

9.6. Show that there are infinitely many primes congruent to 1 modulo 3. [Hint. See the proof of the "1 (Modulo 4) Theorem" in Section 9.2.1, use $A = (2p_1p_2 \cdots p_r)^2 + 3$, and try to pick out a good prime dividing A .]

9.7. Let p be a prime number ($p \neq 2$ and $p \neq 5$), and let A be some given number. Suppose that p divides the number $A^2 - 5$. Show that p must be congruent to either 1 or 4 modulo 5.

9.8 (Computer Exercise). Write a program that uses Quadratic Reciprocity to compute the Legendre symbol $\left(\frac{a}{p}\right)$.

9.9. Let p be a prime satisfying $p \equiv 3 \pmod{4}$, and suppose that a is a quadratic residue modulo p .

- (a) Show that $x = a^{(p+1)/4}$ is a solution to the congruence

$$x^2 \equiv a \pmod{p}.$$

This gives an explicit way to find square roots modulo p for primes congruent to 3 modulo 4.

- (b) Find a solution to the congruence $x^2 \equiv 7 \pmod{787}$. (Your answer should lie between 1 and 786.)

9.10. Let p be a prime satisfying $p \equiv 5 \pmod{8}$ and suppose that a is a quadratic residue modulo p .

- (a) Show that one of the values

$$x = a^{(p+3)/8} \quad \text{or} \quad x = 2a \cdot (4a)^{(p-5)/8}$$

is a solution to the congruence

$$x^2 \equiv a \pmod{p}.$$

This gives an explicit way to find square roots modulo p for primes congruent to 5 modulo 8.

- (b) Find a solution to the congruence $x^2 \equiv 5 \pmod{541}$. (Give an answer lying between 1 and 540.)
 (c) Find a solution to the congruence $x^2 \equiv 13 \pmod{653}$. (Give an answer lying between 1 and 652.)

9.11 (Computer Exercise). Let p be a prime that is congruent to 5 modulo 8. Write a program to solve the congruence

$$x^2 \equiv a \pmod{p}$$

using the method described in the previous exercise and successive squaring. The output should be a solution satisfying $0 \leq x < p$. Be sure to check that a is a quadratic residue, and return an error message if it is not. Use your program to solve the congruences

$$x^2 \equiv 17 \pmod{1021}, \quad x^2 \equiv 23 \pmod{1021}, \quad x^2 \equiv 31 \pmod{1021}.$$

Appendix A

Class Exercise: Lecture #1

Mix and Match Number Types

We've just seen lots of interesting sorts of numbers. Can you find overlaps? The following questions ask "are there any ...," but implicitly includes the instruction that if there are any, then you should try to describe them.

- *Are there any odd numbers that are also even numbers?*
- *Are there any square numbers that are also cube numbers?*
- *Are there any prime numbers that are also square numbers?*
- *Are there any prime numbers that are a sum of two square numbers?*
- *Are there any perfect numbers that are also odd numbers?*
- *Are there any square numbers that are also triangle numbers?*

Appendix B

Class Exercise: Lecture #2

Pythagorean-Like Triples

A *primitive Pythagorean triple* (PPT) is a triple of positive integers (a, b, c) having no common factors and satisfying

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

We consider two tweaks of the problem of finding all PPTs. For each, gather some data and then try to find a general answer.

- *Describe the no-common-factor triples (a, b, c) satisfying*

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

- *Describe the no-common-factor triples (a, b, c) satisfying*

$$a^2 + b^2 = 3c^2.$$

- *More generally, look at solution to $a^2 + b^2 = kc^2$ for other values of k .*

Appendix C

Class Exercise: Lecture #3

Least Common Multiples

The *greatest common divisor* of a and b is the largest number d that divides both of them. We've already talked about $\gcd(a, b)$.

Similarly, the *least common multiple* of a and b is the smallest number L that is divisible by both a and b . It is denoted $\text{LCM}(a, b)$. For example,

$$\text{LCM}(6, 10) = 30, \quad \text{since } 6 \mid 30 \text{ and } 10 \mid 30,$$

and 30 is the smallest number with this property.

- Compute the \gcd 's and LCM 's in the following table:

| m | n | $\gcd(m, n)$ | $\text{LCM}(m, n)$ |
|-----|-----|--------------|--------------------|
| 8 | 12 | | |
| 20 | 30 | | |
| 51 | 68 | | |
| 24 | 18 | | |

- Using the data in the table, conjecture a relationship between the values of m , n , $\gcd(m, n)$ and $\text{LCM}(m, n)$.
- Suppose that $\gcd(m, n) = 18$ and $\text{LCM}(m, n) = 720$. Find m and n . Is there more than one possibility? If so, find all of them.

Appendix D

Class Exercise: Lecture #4

Further Travels in the \mathbb{E} -Zone

NOTE: In the \mathbb{E} -Zone odd numbers do not exist!

- *Here are the first few \mathbb{E} -primes:*

2, 6, 10, 14, 18, 22, 26, 30.

Extend the list. Try to find a nice description of all \mathbb{E} -primes.

- *What is the smallest even number that has two different factorizations as a product of \mathbb{E} -primes? (Changing the order of the factors doesn't count!) What about the smallest even number that has three different factorizations as a product of \mathbb{E} -primes? Four factorizations? Etc.*

- *The number 12 has only one factorization as a product of \mathbb{E} -primes: $12 = 2 \cdot 6$. Find some other even numbers with this property. Can you describe all of them?*

Appendix E

Class Exercise: Lecture #5

Polynomial Roots Modulo m

You probably know that a polynomial of degree d can have at most d real roots. But how about if we work modulo m ? In other words, how many solutions can there be to the congruence

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_2 X^2 + a_1 X + a_0 \equiv 0 \pmod{m},$$

where congruent solutions are considered identical. For example,

$$X^2 + 1 \equiv 0 \pmod{13} \text{ has two solutions, namely } X \equiv 5 \text{ and } X \equiv 8.$$

- *How many solutions are there to the following congruences?*

$$X^2 + 1 \equiv 0 \pmod{2} \qquad X^2 + 1 \equiv 0 \pmod{3}$$

$$X^2 + 1 \equiv 0 \pmod{4} \qquad X^2 + 1 \equiv 0 \pmod{5}$$

Make a conjecture about the possible number of solutions to $X^2 + 1 \equiv 0 \pmod{m}$.

- *How many solutions are there to the following congruences?*

$$X^2 - 1 \equiv 0 \pmod{3} \qquad X^2 - 1 \equiv 0 \pmod{4}$$

$$X^2 - 1 \equiv 0 \pmod{8} \qquad X^2 - 1 \equiv 0 \pmod{15}$$

Do your answers make you rethink your earlier conjecture?

- *I used a computer to check the number of solutions to $X^2 + 1 \equiv 0 \pmod{m}$ for every $3 \leq m \leq 4000$, and there were always either 2, 4, or 6 solutions. This suggests that $X^2 + 1 \equiv 0 \pmod{m}$ always has an even number of solutions. Either prove that this is true, or find a counterexample.*

Appendix F

Class Exercise: Lecture #6

Sums of Reciprocals

For every integer $m \geq 2$, we look at the fraction

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{m-1}.$$

Here is some data:

$$\begin{array}{r} \frac{1}{1} + \frac{1}{2} = \frac{3}{2} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} = \frac{11}{6} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{137}{60} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{49}{20} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} = \frac{363}{140} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} = \frac{761}{280} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} = \frac{7129}{2520} \\ \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} = \frac{7381}{2520} \end{array}$$

Let N_m be the numerator of the fraction for m , so for our data we have

| m | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|-------|---|----|----|-----|----|-----|-----|------|------|
| N_m | 3 | 11 | 25 | 137 | 49 | 363 | 761 | 7129 | 7381 |

- Can you find some interesting property of the numerators? (As is often the case, looking at N_p for prime values of p may be easier.)
- Can you prove something interesting about the numerators N_p when p is prime?

Appendix G

Class Exercise: Lecture #7

The $3n + 1$ Problem

The $3n + 1$ *Algorithm* works as follows: Start with any number n . If n is even, divide it by 2. If n is odd, replace it with $3n + 1$. Repeat. For example, if we start with 5,

$$\underbrace{5 \xrightarrow{3n+1} 16 \xrightarrow{n/2} 8 \xrightarrow{n/2} 4 \xrightarrow{n/2} 2 \xrightarrow{n/2} 1 \xrightarrow{3n+1} 4 \xrightarrow{n/2} 2 \xrightarrow{n/2} 1 \xrightarrow{3n+1} \dots}_{\text{Length 9}} \quad \underbrace{\hspace{10em}}_{\text{repeats}}$$

Notice that as soon as we get to 1, the sequence repeats 4, 2, 1. Starting at 7 gives

$$\begin{array}{ccccccccccccccccccc} 7 & \xrightarrow{3n+1} & 22 & \xrightarrow{n/2} & 11 & \xrightarrow{3n+1} & 34 & \xrightarrow{n/2} & 17 & \xrightarrow{3n+1} & 52 & \xrightarrow{n/2} & 26 & \xrightarrow{n/2} & 13 & \xrightarrow{3n+1} & 40 & \xrightarrow{n/2} & 20 & \xrightarrow{n/2} & 10 & \xrightarrow{n/2} & 5 & \xrightarrow{3n+1} & 16 & \xrightarrow{n/2} & 8 & \xrightarrow{n/2} & 4 & \xrightarrow{n/2} & 2 & \xrightarrow{n/2} & 1 \end{array}$$

Length 17

The $3n + 1$ Conjecture (also known as the Collatz Conjecture). *No matter what n you start with, the $3n + 1$ Algorithm eventually gets down to 1.*

The *length* of the sequence starting from n , i.e., the number of entries required to get down to 1, is denoted $L(n)$. Thus

$$L(5) = 9 \quad \text{and} \quad L(7) = 17.$$

— Continued on Next Page —>

- Find the length of the $3n + 1$ algorithm for each of the following starting values:

(i) $n = 21$ (ii) $n = 13$ (iii) $n = 31$ (You might not want to finish (iii)!)

- Here is a table giving the length $L(n)$ for (almost) all $1 \leq n \leq 30$.

| | | | | | | | | | | | | | | | | | | | | |
|--------|---|---|---|---|---|---|----|---|----|----|----|----|----|----|----|----|----|----|----|----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| Length | 1 | 2 | 8 | 3 | 6 | 9 | 17 | 4 | 20 | 7 | 15 | 10 | — | 18 | 18 | 5 | 13 | 21 | 21 | 8 |

| | | | | | | | | | | | | | | | | | | | | |
|--------|----|----|----|----|----|----|-----|----|----|----|-----|----|----|----|----|----|----|----|----|----|
| n | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| Length | — | 16 | 16 | 11 | 24 | 11 | 112 | 19 | 19 | 19 | 107 | 6 | 27 | 14 | 14 | 22 | 22 | 22 | 35 | 9 |

| | | | | | | | | | | | | | | | | | | | | |
|--------|-----|----|----|----|----|----|-----|----|----|----|----|----|----|-----|-----|----|----|----|----|----|
| n | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| Length | 110 | 9 | 30 | 17 | 17 | 17 | 105 | 12 | 25 | 25 | 25 | 12 | 12 | 113 | 113 | 20 | 33 | 20 | 33 | 20 |

The Length of the $3n + 1$ Algorithm

Looking at the table, there seem to be a lot of values of n with $L(n) = L(n + 1)$. Can you find a pattern for at least some of those n ? Can you find an infinite list of n for which you can prove that $L(n) = L(n + 1)$?

Appendix H

Class Exercise: Lecture #8

Cubes Modulo p

We've looked at squares modulo p , so let's move on to cubes. A number a is called a *cubic residue modulo p* if it is congruent to a non-zero cube modulo p , that is, if there is a number $b \not\equiv 0 \pmod{p}$ such that

$$a \equiv b^3 \pmod{p}.$$

- Make a list of the cubic residues mod 5, mod 7, and if you feel like it, mod 13.
- If a and b are cubic residues modulo p , is the product ab always a cubic residue?
- If a or b (or both) are not cubic residues modulo p , what can you say about the product ab ? Use the following table of cubes modulo 19 to gather some data.

| Cubic Residues Mod 19 | Cubic Non-Residues Mod 19 |
|-----------------------|--|
| 1, 7, 8, 11, 12, 18 | 2, 3, 4, 5, 6, 9, 10, 13, 14, 15, 16, 17 |

- Here is a list of cubic residues for a few primes p that satisfy $p \equiv 2 \pmod{3}$.

| p | Cubic Residues Mod p |
|-----|---|
| 5 | 1, 2, 3, 4 |
| 11 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 |
| 17 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 |
| 23 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 |
| 29 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 |

What's the pattern? Can you prove it? (Hint: Fermat's little theorem may be useful!)

Appendix I

Class Exercise: Lecture #9

Cubic Reciprocity

Recall that the number a is called a *cubic residue modulo p* if it is congruent to a non-zero cube modulo p . Let p and q be primes. Can we relate the following two statements?

- q is (is not) a cubic residue modulo p .
- p is (is not) a cubic residue modulo q .

Here is a table to help in making conjectures.

| $p \backslash q$ | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 |
|------------------|---|---|----|----|----|----|----|----|----|----|----|
| 5 | — | ○ | ♡ | ♡ | ♡ | ○ | ♡ | ♡ | ○ | ○ | ♡ |
| 7 | ○ | — | ○ | ○ | ○ | ○ | ○ | ♡ | ★ | ★ | ♡ |
| 11 | ♡ | ○ | — | ○ | ♡ | ♡ | ♡ | ♡ | ○ | ♡ | ♡ |
| 13 | ♡ | ○ | ○ | — | ○ | ★ | ○ | ○ | ○ | ★ | ○ |
| 17 | ♡ | ○ | ♡ | ○ | — | ○ | ♡ | ♡ | ○ | ○ | ♡ |
| 19 | ○ | ○ | ♡ | ★ | ○ | — | ○ | ○ | ○ | ○ | ○ |
| 23 | ♡ | ○ | ♡ | ○ | ♡ | ○ | — | ♡ | ♡ | ♡ | ♡ |
| 29 | ♡ | ♡ | ♡ | ○ | ♡ | ○ | ♡ | — | ♡ | ♡ | ♡ |
| 31 | ○ | ★ | ○ | ○ | ○ | ○ | ♡ | ♡ | — | ○ | ○ |
| 37 | ○ | ★ | ♡ | ★ | ○ | ○ | ♡ | ♡ | ○ | — | ○ |
| 41 | ♡ | ♡ | ♡ | ○ | ♡ | ○ | ♡ | ♡ | ○ | ○ | — |

Table with ♡ if p and q are each cubic residues of the other, with ○ if one is and one isn't, and with ★ if neither is a cubic residue of the other.