NUMBER THEORY

GIRLS TALK MATH

Contents

1. Introduction

Number theory is the study of whole numbers and their properties. The famous 18th and 19th century German mathematican Carl Friedrich Gauss referred to number theory as the "queen of mathematics," in reference to both its beauty and its importance within mathematics. Today, number theory is considered to be part of "pure mathematics,", meaning that most people who study number theory don't necessarily have some real world application in mind for their research. They study number theory because it is interesting, it is fun, and because they want to learn more about how everything in math fits together. On the other hand, there are many applications of number theory to real world problems. For example, much of the mathematics underlying modern cryptography comes from number theory.

While number theory is a very old area of mathematics, it is still the subject of much active research by mathematicians today. Many famous unsolved problems that fascinate mathematicians come from number theory. These problems are often easy to state, but incredibly difficult to solve. We will see a few of these unsolved problems throughout these notes.

These notes are structured like a mathematics textbook, with some exercises sandwiched between chunks of new material. Reading mathematics like this is an active process, and it is best to read with a pencil and paper at your side, so you can follow through the examples on your own. Sometimes things won't make sense the first time you read them. That is totally okay, and it is normal. Things don't make sense to mathematicians the first time they read them either. If you have trouble understanding a passage, try to skim through it and move on to the next example. Often by working out the example you can see what the text was trying to say. If that doesn't work, proceed to an exercise. The exercises almost always follow after

a closely related example, and by comparing the two you can often figure out how to do the exercise. In doing this process you can learn a lot of mathematics. If you are still stuck, don't forget to ask your fellow group members or your group leader. Learning math is not a process that is easy to do alone, and the best mathematicians are so good because they know who to ask when they get stuck on something.

When reading these notes, you should try to do all the problems that are labeled "Exercise". These are the meat of the packet, and it is in doing these problems that you will learn the most from this packet. Occasionally you will come across a problem called a "Challenge Problem". You should read over the problem, and if you think you know how to attack it, go for it. Otherwise, feel free to move on. These are not necessary for understanding the packet, but if you are moving through the packet really quickly, they can help to expand your mathematical horizons.

2. Sage

Throughout these notes we will frequently mention the mathematical programming language Sage. This is freely available at the Sage website, and can be run online at https://sagecell.sagemath.org/. Sage is made for number theory, so it is very useful to have handy while working through these notes. Almost every calculation we do can be checked on Sage, and Sage can handle some calculations that we can't!

3. Prime Numbers and Prime Factorization

Before we start talking about number theory, let's be more precise about what we mean when we say "number". In number theory we will be mostly interested in the set of natural numbers

$$\{1, 2, 3, 4, \dots\}.$$

These are the positive whole numbers, and we denote this set by $\mathbb{N}$. We are also interested in the integers

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

which are all whole numbers, positive and negative. We denote this set by $\mathbb{Z}$. We see that every natural number is an integer, but not every integer is a natural number. In mathematical language, we say the set of natural numbers is a subset of the integers, and we write

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

In this first section, our focus will be on prime numbers. Remember: a *prime number* is a positive integer whose only factors are itself and 1. By convention, we say 1 is not prime (more on this later). A number is *composite* if it is not prime. Prime numbers are so important to us because, in some sense, they are the building blocks of all other numbers. To be more precise, every natural number greater than 1 has a unique factorization into a product of primes. In other words, if n is an integer, we can write

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

for some collection of prime numbers $p_1, \dots, p_r$, and some collection of exponents $a_1, \dots, a_r$. We call this the *unique factorization property* for primes, and the fact that every number satisfies the unique factorization property for primes is the *fundamental theorem of arithmetic*.

Example 3.1. The prime factorization for 60 is

$$60 = 2^2 \cdot 3^1 \cdot 5^1.$$

Exercise 3.2. Find prime factorizations for the following numbers:

1. 12
2. 38
3. 97
4. 100
5. 184
6. 216

It is this unique factorization property that leads us to say that 1 is not prime. Notice that any number can be written as a product containing arbitrarily many ones. Take $n = p_1^{a_1} \cdots p_r^{a_r}$ as above. Then

$$n = 1 \cdot p_1^{a_1} \cdots p_r^{a_r} = 1^2 \cdot p_1^{a_1} \cdots p_r^{a_r} = 1^m \cdot p_1^{a_1} \cdots p_r^{a_r}.$$

So while $a_1, \ldots, a_r$ are uniquely determined by n, the exponent for 1 can be anything. In other words, if 1 were prime, we would no longer have the unique factorization property for primes!

Prime numbers are still a topic of much modern mathematical research. For example, we have Goldbach's conjecture:

Conjecture 3.3 (Goldbach's Conjecture)**.** Every even integer greater than 2 can be expressed as the sum of two primes.

A conjecture is a statement that mathematicians believe to be true, but which they cannot yet prove. So Goldbach's conjecture is an unsolved problem at the moment. This has been verified on a computer for all even integers less than $4 \cdot 10^{18}$. This is pretty strong evidence that the conjecture is true, but it is not a proof. Could there be a super large even integer that is not the sum of two primes? Probably not, but no one knows for sure!

4. Divisibility

Prime factorizations can be useful for finding the greatest common divisor of two numbers. Let us begin by giving a precise mathematical definition for the notion of one number dividing another number.

Mathematical Definition 4.1. Let n and m be two integers. We say n *divides* m if there exists a third integer q such that

$$n \cdot q = m.$$

In mathematical notation, we often write $n|m$ to say n divides m.

Example 4.2. For example, 3 divides 60 because there is another integer, namely 20, such that $3 \cdot 20 = 60$. In this example $n = 3$, $m = 60$ and $q = 20$.

Example 4.3. Every even number is divisible by 2. Then by definition of "divides", any even number n can be written as $n = 2 \cdot k$ for some number k. For instance, $4 = 2 \cdot 2, 18 = 2 \cdot 9$, and $234 = 2 \cdot 117$.

On the other hand, any odd number is one more than an even number, so an odd number n can be written $n = 2 \cdot k + 1$. Let us prove that 2 does not divide an odd number. To do this, we will assume that our odd number $n = 2 \cdot k + 1$ is even, and

we will show that this assumption leads to a contradiction. This would imply that the assumption is itself false, so $2 \cdot k + 1$ is not even. This style of proof is common in mathematics, and it is called *proof by contradiction*.

Now assume $n = 2 \cdot k + 1$ is divisible by 2. Then there is some q such that

$$n = 2 \cdot q.$$

But we know $n = 2 \cdot k + 1$, so we get

$$2 \cdot k + 1 = 2 \cdot q.$$

Subtracting $2 \cdot k$ from both sides, we see

$$1 = 2 \cdot q - 2 \cdot k.$$

If we factor a 2 out of the right-hand side, we get

$$1 = 2 \cdot (q - k).$$

But, by definition, this says that 2 divides 1, which is outrageous! Therefore the assumption that $n = 2 \cdot q$ led to a contradiction, so the assumption must be false, and $n \neq 2 \cdot q$ for any q. Altogether we have shown that no odd number is divisible by 2.

Exercise 4.4. Suppose that a number n can be written

$$n = a \cdot k + 1,$$

where a and k are integers. Following Example 4.3, prove that n is not divisible by a.

Challenge Problem 4.5. Use the definition of "divides" to prove the following:

(a) Prove that if $a|b$ and $b|c$, then $a|c$.
(b) Prove that if $a|b$ and $c|d$, then $(a \cdot c)|(b \cdot d)$.

Now let's discuss how we can use prime factorizations to find the greatest common divisor of two numbers. Remember that the *greatest common divisor* of two integers a and b is the largest number d such that d divides a and d divides b (in symbols, $d|a$ and $d|b$). We will write

$$\gcd(a, b)$$

to denote the greatest common divisor (or gcd) of a and b. Remember that 1 divides every number. If $\gcd(a, b) = 1$, we say a and b are *relatively prime*.

There are a number of ways to compute the greatest common divisor of two numbers. The most straightforward is to list *all* factors of the given numbers, and find the greatest factor that they have in common.

Example 4.6. Suppose we want to find $\gcd(12, 60)$. We begin by listing all factors of each number:

- The factors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
- The factors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60.

The common factors are 1, 2, 3, 4, 6, and 12. The *greatest* common factor is 12, so $\gcd(24, 60) = 12$.

Another way to find the greatest common divisor of two numbers is to examine their prime factorizations.

Fact 4.7. The gcd of two numbers is the product of all of their common prime factors.

Example 4.8. Let's find $\gcd(24, 60)$ again, this time by looking at their prime factorizations. We have

$$24 = 2^3 \cdot 3^1,$$
$$60 = 2^2 \cdot 3^1 \cdot 5^1.$$

Let's expand this, and circle all their common factors:

$$24 = \textcircled{2} \cdot \textcircled{2} \cdot 2 \cdot \textcircled{3},$$
$$60 = \textcircled{2} \cdot \textcircled{2} \cdot \textcircled{3} \cdot 5.$$

Then 24 and 60 both have two factors of 2, and one factor of 3. Hence

$$\gcd(24, 60) = 2 \cdot 2 \cdot 3 = 12.$$

Exercise 4.9. Find the greatest common divisor for each of the following pairs:
(a) 5 and 15
(b) 27 and 81
(c) 121 and 99
(d) 6 and 19

The problem with both of these methods for finding the greatest common divisor is that they both require us to factor numbers. Factoring is a mathematical operation which becomes very difficult very quickly. As numbers get very large, it becomes impossible even for computers to find their factorizations quickly. Fortunately, there is a way to compute the gcd of two numbers without factoring. It is called the "Euclidean Algorithm," because it originated with the famous Greek geometer Euclid. We will return to this in a later section.

5. How many primes are there?

The Greek mathematician and geographer Eratosthenes famously came up with a method for finding all prime numbers less than a given number. His method is called the *Sieve of Eratosthenes*. The method goes as follows:

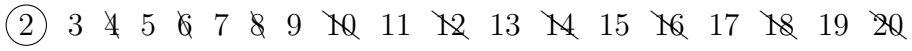
The Sieve of Eratosthenes

(1) List all numbers from 2 to a chosen number n.
(2) Circle 2; it is prime.
(3) Cross out all multiples of 2. Because 2 divides them, they are not prime.
(4) Circle 3; it is prime.
(5) Cross out all multiples of 3 that are not already crossed out. Because 3 divides them, they are not prime.
(6) Repeat this process: circle the left-most number which is not already circled or crossed out, and cross out all multiples of the number you just circled.
(7) Stop when every number between 2 and n is either circled or crossed out. The circled numbers are all the primes between 2 and n.

Example 5.1. Let's find all primes up to 20. First we list the numbers between 2 and 20:

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

Now 2 is prime, so we circle it and cross out all multiples of 2:



Repeat this process with 3. Circle 3 and cross out all multiples of 3 that are not already crossed out:

$$\textcircled{2}\ \textcircled{3}\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}$$

The left-most number that is not circled or crossed out is 5, so 5 must be prime. Now we circle it and cross out all multiples of 5 which are not yet crossed out:

$$\textcircled{2}\ \textcircled{3}\ \cancel{4}\ \textcircled{5}\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}$$

If we repeat this process a few more times, we end up with:

$$\textcircled{2}\ \textcircled{3}\ \cancel{4}\ \textcircled{5}\ \cancel{6}\ \textcircled{7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ \textcircled{11}\ \cancel{12}\ \textcircled{13}\ \cancel{14}\ \cancel{15}\ \cancel{16}\ \textcircled{17}\ \cancel{18}\ \textcircled{19}\ \cancel{20}$$

Therefore the primes between 2 and 20 are: 2, 3, 5, 7, 11, 13, 17, and 19.

Now, you should notice that we didn't actually need the Sieve of Eratosthenes to find these numbers. It is easy to determine whether a number less than 20 is prime; just check to see if it is divisible by anything smaller. However, once we start to look for bigger primes this method is impractical. Trying to write all primes less than one hundred or one thousand in this way can be very difficult. In these cases it is helpful to use the Sieve of Eratosthenes.

Exercise 5.2. Use the Sieve of Eratosthenes to find all prime numbers less than 225.

Challenge Problem 5.3. Suppose we are trying to determine if a number n is prime. Then we only need to check to see if the numbers less than or equal to $\sqrt{n}$ divide n. Can you explain why?

We can use the mathematical programming language Sage to check our answer. The command "prime_range(a,b)" tells you all prime numbers in a given range.

Example 5.4. Let's use Sage to find all prime numbers between 0 and 100. Type the following into Sage, and click "Evaluate":

$$\text{prime\_range}(0, 100)$$

The output should be a list of all prime numbers between 0 and 100.

Exercise 5.5. Use Sage to find all prime numbers less than 225. Use this list to check your answer from Exercise 5.2.

After looking at the Sieve of Eratosthenes, a natural question arises: how many primes are there? It seems obvious to us that there must be infinitely many primes, but mathematicians don't settle for "obvious"; we require proof. A famous proof that there are infinitely many primes was given by the ancient Greek mathematician Euclid. Let's walk through it together.

Exercise 5.6. Complete each of the following computations and determine if the resulting number is prime or not:

$$\begin{aligned} 2+1 &= \\ 2\cdot 3+1 &= \\ 2\cdot 3\cdot 5+1 &= \\ 2\cdot 3\cdot 5\cdot 7+1 &= \end{aligned}$$

Do you think the resulting pattern will continue forever? Why or why not? If it did, what would it tell you about the number of prime numbers?

Sage makes factoring numbers easy. To factor a number n simply type "factor(n)" and click evaluate.

Example 5.7. First let's factor something easy: Go to Sage and input the following:

$$\text{factor}(60)$$

When we click "Evaluate", we should get an output that looks like this:

$$2\text{^}2 \ * \ 3 \ * \ 5.$$

This tells us that $60 = 2^2 \cdot 3 \cdot 5$, which we already knew.

Now let's factor the next number in the pattern above: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$. Input the following into Sage:

$$\text{factor}(2^*3^*5^*7^*11 + 1)$$

and click enter. The output should be 2311. This tells us that $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$, and 2311 is prime, so there are no other factors.

Exercise 5.8. Continue the pattern from the previous exercise. Using Sage, factor the following numbers into products of primes:

(a) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$
(b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1$
(c) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 + 1$

What do you notice about the prime numbers that divide these numbers? How do they compare to the primes that we used to construct these numbers?

Exercise 5.9. If the pattern in the previous exercise continues forever, what would this tell you about the number of prime numbers? Explain.

Before these next exercises, you may want to review Mathematical Definition 4.1 to recall the precise definition for when a number divides another number. You may also find Exercise 4.4 to be helpful for these next exercises.

Exercise 5.10. Consider a general number of the form we've been studying:

$$2 \cdot 3 \cdot 5 \ldots p_n + 1$$

where $2, 3, 5, \ldots, p_n$ are consecutive primes.

(a) Does 2 divide $2 \cdot 3 \cdot 5 \cdots p_n + 1$? Why or why not? (Hint: look at Example 4.4.)
(b) Does 3 divide $2 \cdot 3 \cdot 5 \cdots p_n + 1$? Why or why not?
(c) Does any prime between 2 and p_n (including p_n) divide $2 \cdot 3 \cdot 5 \cdots p_n + 1$? Why or why not?

What do (a), (b), and (c) tell you about the prime divisors of $2 \cdot 3 \cdot 5 \cdots p_n + 1$?

Exercise 5.11. (a) Explain why the previous exercise guarantees that there must exist a prime larger than p_n.
(b) Explain why this process proves there must be infinitely many primes.

Challenge Problem 5.12. Can you come up with another way to prove that there are infinitely many prime numbers?

Let's end this section by pointing out that, although we know there are infinitely many primes, this does not mean we know everything there is to know about primes. In fact, there are a number of unsolved problems concerning prime numbers to this day. The most famous is the Twin Prime Conjecture. A pair of *twin primes* is a pair

of prime numbers p_1 and p_2 which are a space of 2 apart. In other words, if $p_2 > p_1$, then $p_2 - 2 = p_1$. For example, 3 and 5 are twin primes, 11 and 13 are twin primes, and 881 and 883 are twin primes.

Conjecture 5.13 (Twin Prime Conjecture)**.** There are infinitely many twin primes.

Exercise 5.14. Find another pair of twin primes.

6. The Division Theorem and the Euclidean Algorithm

To begin this section, we'll state a fact which you definitely know, but which you have probably never seen written in exactly this way.

Theorem 6.1 (The Division Theorem)**.** Suppose a and b are integers with $b \neq 0$. Then there exist unique integers q and r such that

$$a = b \cdot q + r,$$

and such that $0 \leq r < |b|$.

This fact restates something you already know: you can divide an integer by another nonzero integer. The q in the above statement is the quotient, or what you get as a result when you divide. The r is the remainder. You should think of the division theorem in the following way:

$$\text{if } a = b \cdot q + r \text{ with } 0 \leq r < |b|, \text{ then } a \text{ divided by } b \text{ is } q \text{ with remainder } r.$$

The converse is also true:

$$\text{if } a \text{ divided by } b \text{ is } q \text{ with remainder } r, \text{ then } a = b \cdot q + r, \text{ and } 0 \leq r < |b|.$$

Example 6.2. Take $a = 37$ and $b = 5$. Then if we divide a by b we get 7 with a remainder of 2. We can write this in the form above as

$$37 = 5 \cdot 7 + 2.$$

Here $q = 7$ and $b = 2$. Notice that $2 = r < |b| = 5$. Moreover, 7 and 2 are the unique values of q and r that make this work. If we take any other value for q, then the value of r that we need to balance the equation will be *larger* than 5. For example, suppose we tried to use $q = 6$, and suppose we still wanted to write $a = b \cdot q + r$. Then we have

$$37 = 5 \cdot 6 + r,$$

which would force $r = 7$. But now r is *greater* than 5, so it does not satisfy the conditions of Theorem 6.1

Recall that in section 4 we alluded to a more powerful method for finding greatest common divisors, called the Euclidean Algorithm. We will explain the Euclidean Algorithm now, but before we can begin we need to mention the following fact:

Fact 6.3. If $a = b \cdot q + r$, then $\gcd(a, b) = \gcd(b, r)$.

Challenge Problem 6.4. Prove Fact 6.3.

The Euclidean Algorithm Suppose we want to find the gcd of two integers a and b.

(1) Make sure that $b \leq a$. If necessary, we may need to rename a and b for this to work, but this is no big deal because $\gcd(a, b) = \gcd(b, a)$.

(2) Using Theorem 6.1, the Division Theorem, find b and r with $0 \leq r < |b|$ so that we can write

$$a = b \cdot q + r.$$

(3) (a) If $r = 0$, then b divides a, so $\gcd(a, b) = b$, and we are done.
(b) If $r \neq 0$, then by Fact 6.3, we have

$$\gcd(a, b) = \gcd(b, r),$$

so we can replace the problem of computing $\gcd(a, b)$ with the problem of computing $\gcd(b, r)$.

(4) Define our new value of a to be the old value of b, and our new value of b to be r. Return to Step (2) with these new values of a and b.

At each step we get a new pair (a, b). Each new a is strictly less than the old a, and each new b is strictly less than the old b. Because a and b are positive integers, we eventually will find $r = 0$ (do you see why?). Therefore this process will terminate in finitely many steps.

It is much easier to follow this process by working through an example or two than it is to try to read the above algorithm. Let's begin with a problem we already know the answer to.

Example 6.5. Let's use the Euclidean Algorithm to compute $\gcd(24, 60)$. First we swap 24 and 60 because we need $b < a$. So let $a = 60$ and $b = 24$. If we divide 60 by 24, we get 2 with a remainder of 12. In other words, we can write

$$60 = 24 \cdot 2 + 12.$$

In the context of the Division Theorem, this means $q = 2$ and $r = 12$. Now by Fact 6.3,

$$\gcd(60, 24) = \gcd(24, 12).$$

Now let $a = 24$ and $b = 12$, and let's return to the beginning. This time, however, b divides a:

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

Then $\gcd(24, 12) = 12$. Putting this together we have

$$\gcd(60, 24) = \gcd(24, 12) = 12.$$

So the gcd of 60 and 24 is 12, which we already knew.

Example 6.6. Let's try a much harder example: let's compute $\gcd(2261, 1275)$. Let $a = 2261$ and $b = 1275$. Dividing 2261 by 1275, we find

$$2261 = 1275 \cdot 1 + 986.$$

Then by Fact 6.3, we have

$$\gcd(2261, 1275) = \gcd(1275, 986).$$

Now let $a = 1275$ and $b = 986$. Then, dividing a by b, we see

$$1275 = 986 \cdot 1 + 289.$$

So again Fact 6.3 tells us

$$\gcd(1275, 986) = \gcd(986, 289)$$

Repeating this process we have

$$\begin{aligned} 986 &= 289 \cdot 3 + 119 \\ 289 &= 119 \cdot 2 + 51 \\ 119 &= 51 \cdot 2 + 17 \\ 51 &= 17 \cdot 3. \end{aligned}$$

In the end, we have

$$\begin{aligned} \gcd(2261, 1275) &= \gcd(1275, 986) \\ &= \gcd(986, 289) \\ &= \gcd(289, 119) \\ &= \gcd(119, 51) \\ &= \gcd(51, 17) \\ &= 17. \end{aligned}$$

Exercise 6.7. Compute the following, using the Euclidean Algorithm as in Example 6.6:

(a) $\gcd(112, 32)$
(b) $\gcd(130, 91)$
(c) $\gcd(350, 126)$
(d) $\gcd(497, 175)$

Sage also has a command for computing the gcd of two numbers. Simply type in "gcd(a,b)" and click "Evaluate" to find the gcd of a and b.

Example 6.8. To find the gcd of 2261 and 1175 using Sage, we type

$$\gcd(2261, 1175)$$

and click Evaluate. The output should be 17, which matches Example 6.6.

Exercise 6.9. Use Sage to check your answers for Exercise 6.7.

7. Bézout's Identity

An interesting by-product of the Euclidean Algorithm is the following fact, sometimes called Bézout's Identity.

Fact 7.1 (Bézout's Identity)**.** Let a and b be positive integers with $\gcd(a, b) = d$. Then there exist integers x and y such that

$$ax + by = d.$$

The way we find the x and y in Bézout's Identity is by carefully following the procedure outlined in the previous section, and by keeping track of the numbers as we go. We'll explain the procedure by means of the two examples from the previous section.

Example 7.2. We know $\gcd(60, 24) = 12$. Then Bézout's Identity tells us that there are some positive integers x and y such that

$$60x + 24y = 12. \tag{7.1}$$

What are x and y? Well we found in Example 6.5 that

$$60 = 24 \cdot 2 + 12.$$

If we rearrange this equation, we get:

$$60 \cdot 1 + 24 \cdot (-2) = 12.$$

Matching this with Equation 7.1, we see that $x = 1$ and $y = -2$.

Most examples will not be quite so easy, so the next example outlines a general method for finding x and y.

Example 7.3. Let's return to Example 6.6. There we found that $\gcd(2261, 1275) = 17$. Then by Bézout's Identity, we know that there is some x and y such that

$$2261x + 1275y = 17. \tag{7.2}$$

What are x and y? We'll find them by returning to the steps in Example 6.6. In that example, we first found

$$2261 = 1275 \cdot 1 + 986.$$

We can rewrite this as follows:

$$986 = 2261 \cdot 1 + 1275 \cdot (-1). \tag{7.3}$$

In the next step, we found

$$1275 = 986 \cdot 1 + 289.$$

Rewriting this, we get

$$289 = 1275 \cdot 1 + 986 \cdot (-1). \tag{7.4}$$

But remember, our ultimate goal is to write $2261x + 1275y = 17$ for some x and y. So let's rewrite Equation 7.4 using Equation 7.3 to replace the 986 with something in terms of 2261 and 1275:

$$289 = 1275 \cdot 1 - (2261 \cdot 1 + 1275 \cdot (-1)) \cdot (-1) = 2261 \cdot (-1) + 1275 \cdot 2.$$

Now we keep repeating this process. The next equation is

$$986 = 289 \cdot 3 + 119.$$

Rewriting and using the previous equations, we use this to find

$$\begin{aligned} 119 = 986 \cdot 1 + 289 \cdot (-3) &= (2261 \cdot 1 + 1275 \cdot (-1)) + (2261 \cdot (-1) + 1275 \cdot 2) \cdot (-3) \\ &= 2261 \cdot 4 + 1275 \cdot (-7). \end{aligned}$$

Next we have

$$289 = 119 \cdot 2 + 51.$$

This tells us

$$\begin{aligned} 51 = 289 \cdot 1 + 119 \cdot (-2) &= (2261 \cdot (-1) + 1275 \cdot 2) + (2261 \cdot 4 + 1275 \cdot (-7)) \cdot (-2) \\ &= 2261 \cdot (-9) + 1275 \cdot 16. \end{aligned}$$

Finally, we have

$$119 = 51 \cdot 2 + 17,$$

which turns into

$$17 = 119 \cdot 1 + 51 \cdot (-2) = (2261 \cdot 4 + 1275 \cdot (-7)) + (2261 \cdot (-9) + 1275 \cdot 16) \cdot (-2)$$
$$= 2261 \cdot 22 + 1275 \cdot (-39).$$

So in the end we get

$$2261 \cdot 22 + 1275 \cdot (-39) = 17.$$

Matching this with Equation 7.2, we see $x = 22$ and $y = -39$.

Exercise 7.4. In the following exercises, follow the above example to find x and y such that $ax + by = d$, where $d = \gcd(a, b)$. Hint: look at Exercise 6.7.

(a) $a = 112$, $b = 32$, $d = 16$
(b) $a = 130$, $b = 91$, $d = 13$
(c) $a = 350$, $b = 126$, $d = 14$
(d) $a = 497$, $b = 175$, $d = 7$.

Sage can also compute x and y as above. The command "xgcd(a,b)" computes the greatest common divisor d of a and b, along with x and y such that $ax + by = d$.

Example 7.5. If we go to Sage and type in

xgcd(2261,1275)

the output is $(17, 22, -39)$, which tells us that $\gcd(2261, 1275) = 17$, and that

$$2261 \cdot 22 + 1275 \cdot (-39) = 17,$$

which is what we found in Example 7.3.

Exercise 7.6. Use Sage to verify your answers to Exercise 7.4.

8. Modular Arithmetic

Modular arithmetic is fundamental in number theory, and we will use it throughout the rest of this packet. The basic idea behind modular arithmetic is that sometimes we only care about the remainder of some number divided by another number. Let's begin with an example that you are already familiar with: time.

Example 8.1. *Problem:* Suppose it is 10 am right now. What time will it be in 6 hours?

Solution: To find the time, we add 6 to 10:

$$10 + 6 = 16.$$

However, when we give the hour, it should always be between 1 and 12. So what time is 16 o'clock? We can figure this out a few ways. One way is to subtract 12. Another is to count more carefully up from 10, remembering that after 12 we have to loop back around to 1:

Hours after 10	Time
0	10 : 00
1	11 : 00
2	12 : 00
3	1 : 00
4	2 : 00
5	3 : 00
6	4 : 00

Either way, in 6 hours it will be 4 pm.

Problem: If it is 10 o'clock now, what time will it be in 47 hours?

Solution: This one is a little trickier. It may take us a while to make a chart like the one in the previous problem. Let's start by adding 10 to 47 to get 57. Now, we can't just subtract 12 since 57 - 12 is still greater than 12. Instead, we keep subtracting 12 until we get a number between 1 and 12:

$$57 - 12 = 45$$
$$45 - 12 = 33$$
$$33 - 12 = 21$$
$$21 - 12 = 9.$$

So in 47 hours, it will be 9 o'clock. Notice we can phrase this slightly differently. We have subtracted 12 from 57 four times. In other words,

$$57 - 4 \cdot 12 = 9.$$

If we rewrite this, we get something in the form of the Division Theorem:

$$57 = 12 \cdot 4 + 9.$$

This expression tells us 57 divided by 12 is 4, with a remainder of 9. The remainder here is what is important, since it tells us the hour.

This is an example of arithmetic modulo 12. In arithmetic modulo some number n, whenever we do an operation like addition or multiplication, we take as our answer the remainder of the actual answer divided by n. By the Division Theorem, if we divide any number by n, the remainder will always be between 0 and $n - 1$. This allows us to consider only the numbers between 0 and $n - 1$ when we do arithmetic modulo n. As a set, we write

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-2, n-1\}.$$

These are the *integers modulo* n.

Let's make this a little more precise.

Mathematical Definition 8.2. Let a and n be integers with $n \geq 0$. Then the number a mod n is the unique integer r such that

$$a = n \cdot q + r$$

' with $0 \leq r \leq n - 1$. Notice that the Division Theorem guarantees that we can always find such an r.

In other words, to find the value of a mod n, we divide a by n and take the remainder.

Example 8.3. Let's return to the clock example above. If it is 10 o'clock now, what time will it be in 47 hours? Since $10 + 47 = 57$, this questions is really asking: "what time is 57 o'clock?" Or, in mathematical terms, what is 57 mod 12? Well, if we divide 57 by 12 we get

$$57 = 12 \cdot 4 + 9.$$

The remainder here is 9, so 57 mod 12 = 9. Hence, if it is 10 o'clock now, in 47 hours it will be 9 o'clock.

Exercise 8.4.
(a) If it is 3 o'clock now, what time will it be in 13 hours?
(b) If it is 11 o'clock now, what time will it be in 100 hours?

Challenge Problem 8.5. Suppose it is 10 am right now. In 47 hours we know it will be 9 o'clock. Will it be 9 o'clock am or 9 o'clock pm? Can you think of a general method for solving problems like this? That is, if it is n o'clock now, what time will it be m hours from now? Will it be in the morning or afternoon? How can you find this from the given values of m and n?

The following fact will be very important to us:

Fact 8.6. If a and n are integers, then

$$a \bmod n = 0 \text{ if and only if } n \text{ divides } a.$$

Sometimes it is easier to use other information to compute the value of a mod n than it is to factor a. This fact says that we can still determine if n divides a, even without factoring a. This will be handy later on when we talk about divisibility rules.

Challenge Problem 8.7. Prove Fact 8.6.

Example 8.8. Let's give a few examples of situations where we might like to use integers mod n.
(a) In the clock example above, we are using arithmetic mod 12, so we are considering the set

$$\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \ldots, 11\}.$$

Notice that this convention is slightly different from the time example above, where we consider numbers from 1 to 12. In that case you should think of 12 as being the same as 0.
(b) One particularly simple example is the integers mod 2. This is

$$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$$

When we add or multiply numbers in $\mathbb{Z}/2\mathbb{Z}$, we only keep track of the remainder after division by 2. So some addition is the same as usual: $0+0 \bmod 2 = 0$ since 0 divided by 2 is zero with a remainder 0, and similarly $0 + 1 \bmod 2 = 1$. But now we get new weird relationships like $1 + 1 \bmod 2 = 0$, because $1 + 1 = 2$, and the when we divide 2 by 2 the remainder is zero.

It turns out, the value of an integer n mod 2 is determined entirely by whether the number is odd or even. If n is odd, then $n = 2k$ for some integer k, so n mod $2 = 0$. If n is odd, then $n = 2k + 1$ for some integer k, so n mod $2 = 1$.

Example 8.9. (a) $7 \bmod 2 = 1$, because $7 = 2 \cdot 3 + 1$, and $1 \leq 1$.
(b) $50 \bmod 4 = 2$, because $50 = 4 \cdot 12 + 2$, and $2 \leq 4$.
(c) $1001 \bmod 25 = 1$, because $1001 = 25 \cdot 40 + 1$, and $1 \leq 25$.

Exercise 8.10. (a) What is 16 mod 3?
(b) What is 27 mod 4?
(c) What is 122 mod 11?
(d) What is 1001 mod 4?
(e) What is 1,000,000 mod 10?

Of course, Sage can also compute mod. The symbol we use in Sage for mod is %.

Example 8.11. Let's use Sage to compute 277 mod 6. Go to Sage, type in

$$277\%6$$

and click Evaluate. The output should be 1, which means 277 mod 6 = 1. Indeed, we can check that $277 = 46 \cdot 6 + 1$.

Exercise 8.12. Check your answers to Exercise 8.10 using Sage.

Example 8.13. Let's study arithmetic modulo 5. The numbers mod 5 are

$$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\},$$

and when we add or multiply numbers, we only care about the remainder after division by 5.

For example $1 \cdot 2 = 2$, and 2 divided by 5 is 0, with a remainder of 2. Hence $1 \cdot 2$ mod $5 = 2$.

For another example, let's take 3 times 4 mod 5. We have $3 \cdot 4 = 12$, and 12 divided by 5 is 2, with a remainder of 2. Hence

$$3 \cdot 4 \bmod 5 = 2.$$

We can do the same process for addition. For example, $3 + 3$ mod 5 is 1 (do you see why?).

Below are the addition and multiplication tables for addition modulo 5:

$+$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exercise 8.14. Let's try some arithmetic modulo 4.

(i) What is 2+5 modulo 4?
(ii) What is $2 \cdot 5$ modulo 4?
(iii) Fill out addition and multiplication tables for arithmetic modulo 4, as in the example above.

Here are some fundamental facts about modular arithmetic:

Fact 8.15. When we are adding (or multiplying) numbers modulo n is that it doesn't matter whether we add (or multiply) first, or if we take the remainder modulo n first. The result is the same either way. More precisely, if a, b, and n are integers,

(a) $(a + b) \bmod n = (a \bmod n) + (b \bmod n)$.
(b) $(a \cdot b) \bmod n = (a \bmod n) \cdot (b \bmod n)$.

Fact 8.16. In modular arithmetic, multiplication and addition are compatible. That is, we can still use the distributive property we are used to using from ordinary arithmetic. If a, b, c, and n are integers, then

$$a \cdot (b + c) \bmod n = a \cdot b + a \cdot c \bmod n.$$

Example 8.17. For example, suppose we want to look at 11 times 5 modulo 6. We could imagine two ways to do this:

(i) We could first reduce everything modulo 6, and then multiply. We have

$$11 \bmod 6 = 5,$$

and

$$5 \bmod 6 = 5.$$

Now $5 \cdot 5 = 25$, and $25 \bmod 6 = 1$. So $11 \cdot 5 \bmod 6 = 1$. Written out step-by-step, this looks like:

$$\begin{aligned}(11 \bmod 6) \cdot (5 \bmod 6) &= (5 \cdot 5) \bmod 6 \\ &= 25 \bmod 6 \\ &= 1.\end{aligned}$$

(ii) On the other hand, we could multiply the numbers first, and then take the result mod 6. Now

$$11 \cdot 5 = 55,$$

and $55 \bmod 6 = 1$ because 55 divided by 6 is 9 with a remainder of 1. Written step-by-step, this looks like

$$\begin{aligned}11 \cdot 5 \bmod 6 &= 55 \bmod 6 \\ &= 1.\end{aligned}$$

So we see that either way, we get the same result. In this case, the second method is easier, but sometimes, when we are multiplying big numbers together, it is easier to first reduce, and then multiply.

Example 8.18. Let's do 1001 times 1003 mod 4. We can first take the numbers mod 4, and then multiply them together. Now

$$1001 \bmod 4 = 1, \text{ and } 1003 \bmod 4 = 3.$$

Then

$$1001 \cdot 1003 \bmod 4 = 1 \cdot 3 \bmod 4 = 3.$$

We could also do this by first multiplying 1001 and 1003, but this is much harder, and it probably will require us to use a calculator (or Sage).

Exercise 8.19. Compute the following:

(a) $10 + 47 \bmod 12$
(b) $16 \cdot 256 \bmod 5$
(c) $57 + 38 \bmod 17$
(d) $2223 \cdot 2225 \bmod 4$

Challenge Problem 8.20. Prove Fact 8.15.

9. Divisibility Tests

One interesting application of modular arithmetic is to divisibility tests. You may (or may not) be familiar with the following fact:

Fact 9.1. A number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Remark 9.2. "If and only if" is a technical mathematical phrase. It is used to link two statements, and it means that the two statements are equivalent, in some sense. In Fact 9.1 above, the "if and only if" means that the following two statements both hold:

(1) *If* a number is divisible by 3, *then* the sum of its digits is divisible by three.
(2) *If* the sum of the digits of some number is divisible by 3, *then* the number is itself divisible by 3.

The "if and only if" means the two statements are linked; you never get one without the other.

Fact 9.1 allows you to quickly identify whether or not a number is divisible by 3. This fact can be very fun, and you can use it to impress your friends and family!

Example 9.3. Let's do a few examples:

(a) 12 is divisible by 3 because the sum of its digits is $1 + 2 = 3$.
(b) 111 is divisible by 3 because the sum of its digits is $1 + 1 + 1 = 3$.
(c) 4,444 is not divisible by 3, because the sum of its digits is $4 + 4 + 4 + 4 = 16$, which is not divisible by 3.
(d) 123,456,789 is divisible by 3 because the sum of its digits is

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45,$$

which is divisible by 3.

Exercise 9.4. Which of the following numbers are divisible by 3?

(a) 34
(b) 36
(c) 222
(d) 5432
(e) 987,654,321
(f) 12,345,678,910

You may be wondering: why is Fact 9.1 true? We can show why using modular arithmetic!

First we need to remember something about place value. Remember that when we write a number in digits, we are really saying that the number is 1 times the ones digit, plus 10 times the tens digit, plus 100 times the hundreds digit, and so on. For example,

$$12,345 = 1 \cdot 10,000 + 2 \cdot 1,000 + 3 \cdot 100 + 4 \cdot 10 + 5 \cdot 1.$$

Now suppose n is some number whose ones digit is n_1, hundreds digit is n_2, and so on. Then

$$n = n_1 \cdot 1 + n_2 \cdot 10 + n_3 \cdot 100 + \cdots + n_r \cdot 10^{r-1}, \tag{9.1}$$

where each n_i is an integer between 0 and 9.

Looking back at Fact 8.6, we remember that checking whether n is divisible by 3 is the same as checking whether or not $n \bmod 3 = 0$. So we need to compute $n \bmod 3$, and see if we get zero. By Fact 8.15, we can first take the summands on the

right-hand side of equation (9.1) mod 3, and then add them. But notice,

$$1 \bmod 3 = 1$$
$$10 \bmod 3 = 1$$
$$100 \bmod 3 = 1$$

We claim that this pattern continues, that is, that $10^m \bmod 3 = 1$ for any m. How would we show this? Well

$$10^m = 1\underbrace{00\ldots0}_{m\text{-times}}. \tag{9.2}$$

In other words, 10^m is 1 followed by m zeros. Then it follows that

$$10^m - 1 = \underbrace{99\ldots9}_{m\text{-times}}. \tag{9.3}$$

Now $\underbrace{99\ldots9}_{m\text{-times}}$ is divisible by 3, since

$$(\underbrace{33\ldots3}_{m\text{-times}}) \cdot 3 = \underbrace{99\ldots9}_{m\text{-times}}.$$

Then we have

$$10^m - 1 = 3 \cdot (\underbrace{33\ldots3}_{m\text{-times}}).$$

Rewriting, this becomes

$$10^m = 3 \cdot (\underbrace{33\ldots3}_{m\text{-times}}) + 1.$$

But notice, this is exactly the form of the Division Theorem, so this tells us that 10^m divided by 3 is $\underbrace{33\ldots3}_{m\text{-times}}$ with a remainder of 1. In other words, $10^m \bmod 3$ is 1!

Keep in mind that this works for any m. Let's return now to equation (9.1):

$$n = n_1 \cdot 1 + n_2 \cdot 10 + n_3 \cdot 100 + \cdots + n_r \cdot 10^{r-1}.$$

Using Fact 8.15 and the claim that we just proved, when take this equation mod 3 we get

$$\begin{aligned} n \bmod 3 &= (n_1 \cdot 1 \bmod 3) + (n_2 \cdot 10 \bmod 3) + \cdots + (n_r \cdot 10^{r-1} \bmod 3) \\ &= (n_1 \cdot 1 \bmod 3) + (n_2 \cdot 1 \bmod 3) + \cdots + (n_r \cdot 1 \bmod 3), \end{aligned}$$

since $10^m \bmod 3$ is always 1. Cleaning this up, we have

$$n \bmod 3 = n_1 + n_2 + n_3 + \cdots + n_r \bmod 3. \tag{9.4}$$

Now we can prove Fact 9.1. Since $n \bmod 3 = n_1 + \cdots + n_r \bmod 3$, if one side is 0, the other side will be zero. So if n is divisible by 3, then $n \bmod 3 = 0$, so by the above equation $n_1 + \cdots + n_r \bmod 3 = 0$, and therefore the sum of the digits of n is divisible by 3. The same logic works in reverse: if the sum of the digits is divisible by 3, then $n_1 + \cdots + n_r \bmod 3 = 0$, so $n \bmod 3 = 0$, and therefore n is divisible by 3.

In case the proof seems a little confusing, let's illustrate it with an example.

Example 9.5. Why is 12,345 divisible by 3? As we did above, we can write

$$12,345 = 1 \cdot 10,000 + 2 \cdot 1,000 + 3 \cdot 100 + 4 \cdot 10 + 5 \cdot 1.$$

In the language of the proof above, we have $n_1 = 1$, $n_2 = 2$, $n_3 = 3$, $n_4 = 4$, and $n_5 = 5$. Let's take both sides of the above equation mod 3:

$$12,345 \bmod 3 = (1 \cdot 10,000 + 2 \cdot 1,000 + 3 \cdot 100 + 4 \cdot 10 + 5 \cdot 1) \bmod 3.$$

Now we can take each individual summand on the right-hand side mod 3, but remember that every power 10 becomes 1 when we mod out by 3. Then

$$12,345 \bmod 3 = (1 + 2 + 3 + 4 + 5) \bmod 3.$$

But 1+2+3+4+5 = 15, so 12,345 mod 3 = 15 mod 3 = 0. This means that 3 divides 12,345.

Let's try now to come up with some other divisibility rules. Let's start by trying to figure out when a number is divisible by 9.

Exercise 9.6. (a) List out the first 10 multiples of 9. Do you see any similarities between their digits? Can you guess a condition that can be used to determine when a number is divisible by 9?
(b) Find some other multiples of 9 (try some really big numbers!). Does the condition you came up with in (a) still work? If not, can you adjust it and find a new condition? (Hint: consider trying a variation of Fact 9.1).

Let's try to prove that the rule you came up with in the previous exercise.

Exercise 9.7. (a) What is 10 mod 9?
(b) What is 100 mod 9?
(c) What is 1000 mod 9?
(d) If m is any positive integer, what is 10^m mod 9? (Hint: check out equations (9.2) and (9.3).)

Exercise 9.8. Prove the rule you came up with in Exercise 9.6.

Challenge Problem 9.9. Can you come up with a rule for divisibility by 11? Here are some hints:
(a) List all multiples of 11 between 0 and 121. What can you say about their digits?
(b) 10 mod 11 is the same as -1 mod 11. What is 100 mod 11? What is 1000 mod 11?
(c) What is 10^m mod 11 if m is even? What if m is odd?

Exercise 9.10. You probably already know a rule for divisibility by 5. Can you prove it in the same way as we proved the rule for 3?

Exercise 9.11. Let's think for a moment about divisibility by 4.
(a) What is 100 mod 4?
(b) What is 1000 mod 4?
(c) What is 10^m mod 4 if $m \geq 2$?
(d) Can you use (a)-(c) to come up with a divisibility rule for 4?

There are divisibility rules along these lines for every number, although for most numbers the rules are not very nice.

Challenge Problem 9.12. Can you come up with a divisibility rule for 7? For 17?

For more information about divisibility rules, check out https://en.wikipedia.org/wiki/Divisibility_rule.

10. Congruences

Very closely related to modular arithmetic is the concept of *congruence*. Let's begin with a formal definition.

Mathematical Definition 10.1. Let a, b, and n be integers. We say a *is congruent to* b *modulo* n if n divides $a - b$. When a is congruent to b modulo n, we write

$$a \equiv b \pmod{n}.$$

What it *really* means for two numbers to be congruent mod n is that the result is the same after performing the mod n operation. In other words, $a \equiv b \pmod{n}$ if and only if $(a \bmod n) = (b \bmod n)$.

Challenge Problem 10.2. Prove $a \equiv b \pmod{n}$ if and only if $(a \bmod n) = (b \bmod n)$.

Congruences can also be used to show some amazing and surprising relationships between numbers. As an example, we have the following famous theorem.

Theorem 10.3 (Fermat's little theorem)**.** *If p is a prime number and a is any integer which is not divisible by p, then*

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

Example 10.4. Let's test out the theorem with the prime number 3. The theorem says if I take any number a, then $a^2 \equiv 1 \pmod{3}$. Let's try some values of a.

(1) Let $a = 1$. Then $a^2 = 1$, and $1 \equiv 1 \pmod{3}$.
(2) Let $a = 2$. Then $a^2 = 4$, and $4 \equiv 1 \pmod{3}$ because $4 - 1 = 3$ is divisible by 3.
(3) Let $a = 4$. Then $a^2 = 16$, and $16 \equiv 1 \pmod{3}$ because $16 - 1 = 15$ is divisible by 3.

Notice that in the theorem there is a condition that a is *not divisible by* p. This is necessary because, for example, $3^2 \equiv 0 \pmod{3}$, not 1.

Exercise 10.5. Verify Fermat's little theorem for the following values of a and p by showing that $a^{p-1} \equiv 1 \pmod{p}$:

(1) $p = 5$, $a = 3$
(2) $p = 5$, $a = 4$
(3) $p = 7$, $a = 2$
(4) $p = 3$, $a = 11$

We can use Fermat's little theorem to help us compute congruences. Let us first point out that the analog of Fact 8.15 holds for congruences, so it doesn't matter whether we add or multiply first or if we apply the mod operation first.

Example 10.6. Let's try to find 3^8 mod 7. To do this by hand is difficult, because 3^8 is very large. However, Fermat's little theorem tells us

$$3^6 \equiv 1 \pmod{7}.$$

Then

$$3^8 \equiv 3^6 \cdot 3^2 \pmod{7}$$

But now, using Fact 8.15, we can break up the right-hand side. Since 3^6 mod 7 is 1, we see

$$3^6 \cdot 3^2 \equiv 1 \cdot 3^2 \pmod{7}.$$

Simplifying, this becomes

$$\begin{aligned} 3^2 &\equiv 9 \pmod 7 \\ &\equiv 2 \pmod 7. \end{aligned}$$

So $3^8 \equiv 2 \pmod 7$. We can check this by multiplying everything out. We get

$$3^8 = 6561$$

and $6561 = 937 \cdot 7 + 2$.

Example 10.7. We can even work with numbers that seem impossibly big. For example, let's compute $2^{10,000,000,001} \bmod 3$. Using Fermat's little theorem, we know

$$2^2 \equiv 1 \pmod 3.$$

Then

$$\begin{aligned} 2^{10,000,000,001} &\equiv 2^{10,000,000,000} \cdot 2 \pmod 3 \\ &\equiv (2^2)^{5,000,000,000} \cdot 2 \pmod 3 \\ &\equiv 1^{5,000,000,000} \cdot 2 \pmod 3 \\ &\equiv 2 \pmod 3. \end{aligned}$$

Then $2^{10,000,000,001} \equiv 2 \pmod 3$.

Exercise 10.8. Use Fermat's little theorem to help you compute the following:

(1) What is $5^{12} \bmod 11$?
(2) What is $2^8 \bmod 5$?
(3) What is $2^{17} \bmod 5$?
(4) What is $3^{31} \bmod 7$?
(5) What is $5^{261} \bmod 3$?
(6) What is $2^{5,001} \bmod 3$?

Notice that in Fermat's little theorem we are always taking the result modulo a prime number p. This leads us to a natural question: what if we work modulo a number which is not a prime? Does Fermat's little theorem still hold? The answer is yes and no. The next exercise shows that the theorem doesn't work when we work modulo a number which is not prime. However, we will soon see that, by changing the statement slightly, we can come up with a more general version of Fermat's little theorem.

Exercise 10.9. Find two integers a and n such that

$$a^{n-1} \not\equiv 1 \pmod n.$$

Before we can improve Fermat's little theorem to take into account non-prime numbers, we need to define Euler's φ-function. The letter φ is a Greek letter which is used frequently in math, and it is pronounced (at least by mathematicians) as "fee".

Mathematical Definition 10.10 (Euler's φ-function)**.** If n is a natural number, then $\varphi(n)$ is defined to be the number of integers a between 1 and n such that a and n are relatively prime.

Remember, two numbers a and n are called *relatively prime* if $\gcd(a, n) = 1$. So equivalently, $\varphi(n)$ is the number of integers a between 1 and n with $\gcd(a, n) = 1$. This definition can seem a little confusing at first, so let's do a few examples.

Example 10.11. The steps to compute $\varphi(n)$ for a positive integer n are the following:

1. Find all integers between 1 and n.
2. Determine which of the integers between 1 and n are relatively prime to n.
3. $\varphi(n)$ is equal to the number of numbers in Step 2.

Using this method, let's find $\varphi(n)$ for all n between 1 and 5.

$n = 1$

1. The numbers between 1 and 1 are: 1
2. From the list above, the numbers relatively prime to 1 are: 1
3. There is 1 number in the list in Step 2, so $\varphi(1) = 1$.

$n = 2$

1. The numbers between 1 and 2 are: 1, 2
2. From the list above, the numbers relatively prime to 2 are: 1
3. There is 1 number in the list in Step 2, so $\varphi(2) = 1$.

$n = 3$

1. The numbers between 1 and 3 are: 1, 2, 3
2. From the list above, the numbers relatively prime to 3 are: 1, 2
3. There are 2 numbers in the list in Step 2, so $\varphi(3) = 2$.

$n = 4$

1. The numbers between 1 and 4 are: 1, 2, 3, 4
2. From the list above, the numbers relatively prime to 4 are: 1, 3
3. There are 2 numbers in the list in Step 2, so $\varphi(4) = 2$.

$n = 5$

1. The numbers between 1 and 5 are: 1, 2, 3, 4, 5
2. From the list above, the numbers relatively prime to 5 are: 1, 2, 3, 4
3. There are 4 numbers in the list in Step 2, so $\varphi(5) = 4$.

Exercise 10.12. Compute $\varphi(n)$ for the remaining positive integers n less than or equal to 10.

Exercise 10.13. Compute $\varphi(p)$ for all prime numbers p less than 20. Do you notice a pattern? Does the pattern continue for all prime numbers p? That is, can you find $\varphi(p)$ if p is any prime number?

This exercise leads us to the following fact:

Fact 10.14. If p is a prime number, then $\varphi(p) = p - 1$.

Challenge Problem 10.15. Prove Fact 10.14.

This fact helps us to see the connection between the Euler φ-function and Fermat's little theorem. Namely, if p is a prime number we can rewrite Fermat's little theorem as follows: if a is any integer, then

$$a^{\varphi(p)} \equiv 1 \pmod{p}.$$

This suggests the "right" way to generalize Fermat's little theorem. We saw that the theorem was false when we tried to replace the $p-1$ exponent with an $n-1$ for any arbitrary integer n, but what if we replace $\varphi(p)$ with $\varphi(n)$?

Theorem 10.16 (Euler's theorem)**.** *If n is a positive integer, and a is any integer which is relatively prime to n, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Notice that we also had to replace the phrase "a is not divisible by p" in Fermat's little theorem with the new phrase "a is relatively prime to n". This makes sense because when p is a prime number, a is relatively prime to p if and only if p does not divide a.

Example 10.17. Let's test Euler's theorem with $n = 4$. We know from Example 10.11 that $\varphi(4) = 2$, so Euler's theorem says that if a is an integer such that $\gcd(a, 4) = 1$, then

$$a^2 \equiv 1 \pmod 4.$$

Some examples of integers which are relatively prime to 4 are $3, 5$, and 17. Let's check Euler's theorem for each of these:

(1) Let $a = 3$. Then $a^2 = 9$, and $9 \equiv 1 \pmod 4$.
(2) Let $a = 5$. Then $a^2 = 25$, and $25 \equiv 1 \pmod 4$.
(3) Let $a = 19$. Then $a^2 = 289$, and $289 = 4 \cdot 72 + 1$, so $289 \equiv 1 \pmod 4$.

We see that Euler's theorem holds in each of these examples.

Similarly to the case of Fermat's little theorem, we point out that the condition $\gcd(a, n) = 1$ is really essential to the theorem. For instance, if we take $a = 2$ and $n = 4$, then $\gcd(2, 4) = 2$, and Euler's theorem does not hold in this case, because $2^2 = 4 \equiv 0 \pmod 4$.

Exercise 10.18. Verify Euler's theorem for the following values of a and n by showing that $a^{\varphi(n)} \equiv 1 \pmod n$:

(1) $n = 4$, $a = 9$
(2) $n = 6$, $a = 7$
(3) $n = 10$, $a = 3$
(4) $n = 12$, $a = 5$

We can also use Euler's theorem to help us compute some complicated congruence relations.

Example 10.19. What is $5^{301} \bmod 9$? Euler's theorem can help us. Notice that $\gcd(5, 9) = 1$, so we can use Euler's theorem with $a = 5$ and $n = 9$. Since $\varphi(9) = 6$, we get

$$5^6 \equiv 1 \pmod 9.$$

Now, we know $300 = 6 \cdot 50$, so

$$5^{300} = (5^6)^{50},$$

and therefore

$$\begin{aligned} 5^{300} &\equiv (5^6)^{50} \pmod 9 \\ &\equiv 1^{50} \pmod 9 \\ &\equiv 1 \pmod 9. \end{aligned}$$

But $5^{301} = 5^{300} \cdot 5$, so multiplying both sides of the above equation by 5, we get

$$5^{301} \equiv 5 \pmod 9.$$

Exercise 10.20. Use Euler's theorem to help you compute the following congruences:

(1) What is $19^{231} \bmod 6$?
(2) What is $9^{66} \bmod 8$?

(3) What is 5^{1042} mod 12?

One other way we can use Euler's theorem is to find the last digit of powers of numbers. We can think of the last digit of a number as the value of the number mod 10. So when we are asked to find the last digit of a number, we are really asked to find the value of that number mod 10, which is something we often can do by using Euler's theorem. Let's try an example.

Example 10.21. Let's find the last digit of 3^{1001}. This is the same as finding 3^{1001} mod 10. Let's set $a = 3$ and $n = 10$. Since $\gcd(3, 10) = 1$, Euler's theorem applies here, and since $\varphi(10) = 4$, we get

$$3^4 \equiv 1 \pmod{10}.$$

Now, $1001 = 4 \cdot 250 + 1$, so we see

$$\begin{aligned} 3^{1001} &= 3^{4\cdot 250+1} \\ &= (3^4)^{250} \cdot 3. \end{aligned}$$

Then

$$\begin{aligned} 3^{1001} &\equiv (3^4)^{250} \cdot 3 \pmod{10} \\ &\equiv 1^{250} \cdot 3 \pmod{10} \\ &\equiv 3 \pmod{10}. \end{aligned}$$

Then the last digit of 3^{1001} is 3.

Exercise 10.22. Determine the last digit of the following:
(a) 9^{925}
(b) 7^{5446}
(c) $3^{9999999}$
(d) 17^{25}

11. The Chinese Remainder Theorem

In 4th century China, mathematicians asked questions similar to the following:

Question 11.1. There is a quantity whose number is unknown. Repeatedly dividing by 3, the remainder is 2, and by 5 the remainder is 3. What is the quantity?

In notation we are now more familiar with, the question can be stated as follows. Can you find a positive integer x which satisfies the following equstions?

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

Exercise 11.2. Find a positive integer x satisfying the above equations. Hint: try guessing and checking.

It turns out that in this type of situation we can *always* find such a number x. The official statement of this result is called the Chinese Remainder Theorem.

Theorem 11.3 (Chinese Remainder Theorem)**.** *Let a and b be integers, and let n and m be positive integers such that* $\gcd(n, m) = 1$*. Then there exists an integer x such that*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

We found a solution to the first example by guess and check. But if we use bigger numbers, it is no longer so straightforward. Imagine we want to find a positive integer x which satisfies the following equations:

$$x \equiv 16 \pmod{51},$$
$$x \equiv 31 \pmod{64}.$$

It turns out that $x = 2719$ works. However, it might take you a long time to find 2719 by guessing and checking! Then how do we find this number? The key is the following fact:

Fact 11.4. Let m and n be relatively prime, so $\gcd(m, n) = 1$. If a and b are any integers, and t is an integer such that

$$a + mt \equiv b \pmod{n},$$

then

$$a + mt \equiv a \pmod{m}.$$

In other words, $x = a + mt$ is the number we are looking for in the Chinese Remainder Theorem.

Challenge Problem 11.5. Prove Fact 11.4.

In our situation, we want to solve

$$z \equiv 16 \pmod{51},$$
$$z \equiv 31 \pmod{64},$$

so in the notation of Theorem 11.3, we want $a = 16, b = 31, m = 51$, and $n = 64$. Notice that $\gcd(51, 64) = 1$, so Fact 11.4 applies here. Then Fact 11.4 tells us that if we can find t with

$$16 + 51t \equiv 31 \pmod{64},$$

then $z = 16+51t$ will solve our problem. Subtracting 16 from both sides, this becomes

$$51t \equiv 15 \pmod{64}. \tag{11.1}$$

So the first step in solving this problem is finding a t that satisfies $51t \equiv 15 \pmod{64}$:

Goal 11.6. Find t such that

$$51t \equiv 15 \pmod{64}. \tag{11.2}$$

How do we find such a t? To find it we need to recall Bézout's Identity (see 7.1). Bézout's Identity says that since $\gcd(51, 64) = 1$, there exists some x and y such that

$$64x + 51y = 1. \tag{11.3}$$

Imagine we know what x and y are. Then Equation 11.3 tells us that

$$51y \equiv 1 \pmod{64}.$$

This almost looks like Equation 11.2, but in that equation the right hand side is 15. So to get closer to what we want, let's multiply both sides by 15:

$$51 \cdot (15y) \equiv 15 \pmod{64}.$$

Now, compare this with Equation 11.2. What we notice is that $15y$ gives us a solution to Equation 11.2. So the problem all boils down to finding x and y as in Bézout's Identity:

Goal 11.7. Find x and y such that

$$64x + 51y = 1.$$

This is something we know how to do (see §7 for more examples). First, we divide 64 by 51, and get

$$64 = 51 \cdot 1 + 13,$$

which turns into

$$13 = 64 \cdot 1 + 51 \cdot (-1).$$

Then we divide 51 by 13 to see

$$51 = 13 \cdot 3 + 12,$$

which we can rewrite as

$$\begin{aligned} 12 = 51 \cdot 1 + 13 \cdot (-3) &= 51 \cdot 1 + (64 \cdot 1 + 51 \cdot (-1)) \cdot (-3) \\ &= 64 \cdot (-3) + 51 \cdot 4. \end{aligned}$$

Finally, we divide 13 by 12 to get

$$13 = 12 \cdot 1 + 1,$$

from which we obtain

$$\begin{aligned} 1 = 13 \cdot 1 + 12 \cdot (-1) &= (64 \cdot 1 + 51 \cdot (-1)) + (64 \cdot (-3) + 51 \cdot 4) \cdot (-1) \\ &= 64 \cdot 4 + 51 \cdot (-5). \end{aligned}$$

Comparing with Equation 11.3, we get $x = 4$ and $y = -5$. This solves Goal 11.7. Now, to solve Goal 11.6, we let $t = 15 \cdot (-5) \bmod 64 = 53$. We can check (using Sage, for example), that

$$51 \cdot 53 \equiv 15 \pmod{64}.$$

Finally, we use Fact 11.4 and let

$$z = 16 + 51 \cdot 53 = 2719.$$

Then

$$\begin{aligned} 2719 &\equiv 16 \pmod{51}, \text{ and} \\ 2719 &\equiv 31 \pmod{64}, \end{aligned}$$

so $z = 2719$ solves the problem.

Exercise 11.8. Following the above example, solve the following systems of congruence equations for x:

(a)

$$\begin{aligned} x &\equiv 5 \pmod{7} \\ x &\equiv 2 \pmod{17} \end{aligned}$$

(b)

$$\begin{aligned} x &\equiv 16 \pmod{24} \\ x &\equiv 4 \pmod{15} \end{aligned}$$

(c)

$$x \equiv 2 \pmod{19}$$
$$x \equiv 20 \pmod{21}$$

Sage can also solve problems relating to the Chinese Remainder Theorem. The relevant command is "CRT(a,b,m,n)", where a, b, m, and n have the same meaning as in the statement of Theorem 11.3.

Example 11.9. Let's use Sage to find x such that

$$x \equiv 16 \pmod{51},$$
$$x \equiv 31 \pmod{64}.$$

Go to Sage and type in

$$\text{CRT}(16,31,51,64).$$

The output should be 2719, which is the same solution that we found above.

Exercise 11.10. Check your solutions to exercise 11.8 using Sage.