Abstract

This is an introduction to more advanced topics in number theory suitable for an advanced Grade 4 audience. These notes were prepared for the Grand River Chinese School. The content covered is not typically presented to elementary school students. It is hard and designed to challenge even the strongest students, while being accessible for everyone. Each chapter (excluding the introduction) may take two to four hours to deliver entirely, depending on the level of detail.

These notes are intended to be a rough outline of what is taught, and not a rigorous and complete reference. I do not necessarily cover all the material written in these notes in any particular year. In particular, the more abstract algebraic concepts are often abbreviated or left out, and are included for completeness. I may occasionally cover material beyond that written in the notes.

Although the notes are intended to be presented to a young audience, they are written for a teacher and not for a student. Many of the terms used will not be familiar to the students. They require explanation.

Number Theory

Fengyang Wang

March 25, 2017

Contents

Chapter 1

Introduction

Number Theory is the study of integers and problems based on the integers. Firstly, what is an integer? We are familiar with the whole numbers, which can be drawn on the number line (see Figure 1.1). The whole numbers begin with 0 and continue 1, 2, 3, and so on.

We may now add in the negative numbers, -1, -2, -3, and so on. If these numbers are considered together with the whole numbers, then we have a full number line that contains all the integers (see Figure 1.2). For most of this unit, we will work with positive integers only, which start at 1 and continue 2, 3, 4, and so on. Note, in particular, that 0 is neither a positive integer nor a negative integer.

Many of the topics in number theory are based off the operations of multiplication and division. Consider a multiplication expression, such as

$$7 \times 9 = 63$$

In this expression, 7 is the multiplicand, 9 is the multiplier, and 63 is the product. An important property of multiplication is that it is commutative, which means we may switch the order. That is,

$$9 \times 7 = 7 \times 9$$

Before we continue, it is important to have a good grasp of what remainders are, and to introduce some new notation. Recall first that division is the operation of repeated subtraction, like how multiplication is the operation of repeated addition.

When we divide 20 by 4, we count how many groups of 4 are needed to make 20. We know that $4 \times 5 = 20$. This means that it takes 5 groups of 4 to make 20. So $20 \div 4 = 5$.

Sometimes the numbers might not work out perfectly. Let's try dividing 20 by 3. If we make 7 groups of 3, the total number would be $3 \times 7 = 21$. But this is too big. If we make 6 groups of 3, the total number would be $3 \times 6 = 18$. But this is too small. So we can make six groups, but we'd then have $20 - 18 = 2$ left over.

We say that when we divide 20 by 3, our *quotient* is 6 because we can make 6 groups of 3 in total. And then we say that our *remainder* is 2 because after

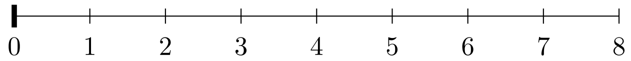

Figure 1.1: The whole numbers on a number line

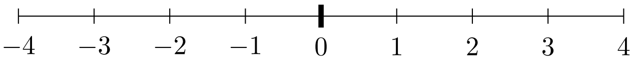

Figure 1.2: The integers on a number line

making 6 groups of 3, we have 2 left over. We can also write this as $20 \div 3 = 6\,\mathrm{R}\,2$. The "R" stands for "remainder".

Suppose we didn't care what the quotient was; only the remainder is important. Then we can write that as $16 \bmod 5 = 1$. We don't care how many groups we made, but we do care that one was left over after making those groups.

The study of remainders is very useful for several major applications, some of which we will see later this unit. Recalling the patterning unit, we used remainders to compute future terms in repeating sequences. Many of the applications of remainders are based off this application.

Example 1a. **Guess the Number**

A number yields a remainder of 1 when divided by 2, a remainder of 2 when divided by 3, a remainder of 3 when divided by 4, and a remainder of 4 when divided by 5.

a. What is the smallest positive number to have this property?

b. Give two other positive numbers to have the above property.

Solution:

a. The important pattern to see here is that each remainder is one less than the number being divided by: $1 = 2 - 1$, $2 = 3 - 1$, and so forth. That means that if we add one to a number that has this property, then it should be divisible by all of 2, 3, 4, and 5. The smallest positive number divisible by all of these is 60, so $60 - 1 = \boxed{59}$ is the smallest positive number having the property.

b. As seen in the solution to part a., any number having the property is one less than a number divisible by 2, 3, 4, and 5. Other numbers that work therefore include $120 - 1 = \boxed{119}$ and $180 - 1 = \boxed{179}$.

Chapter 2

Parity & Divisibility

2.1 Parity

Parity is a property of integers that classifies integers into even integers and odd integers. In this section, we will study the differences between even and odd integers, and also study several important properties. We will also approach the problem algebraically. Do not be alarmed by the presence of letters along with numbers. Unless otherwise stated, a letter is simply a placeholder for a number.

An even number is a number of the form $2n$, where n is any integer. The expression $2n$ means $2 \times n$; we omit the $\times$ so that it is faster to read and write. What are some examples? For instance, 6 is an even number, because we can write $6 = 2 \times 3$.

Is 2 even? Yes. We can write $2 = 2 \times 1$, so 2 is an even number. Is 0 even? Yes. We can write $0 = 2 \times 0$, so 0 is also an even number. What about -10? This is also an even number, because we can write $-10 = 2 \times -5$.

Now let's consider 5. Can we find an integer n so that $5 = 2n$? The answer is no. If we try $n = 2$, we get $2 \times 2 = 4$, which is too small. But if we try $n = 3$, we get $2 \times 3 = 6$, which is too big. Since there are no integers between 2 and 3, the conclusion is that there is no integer n with $5 = 2n$.

Then, 5 is not even. We say that 5 is odd: that simply means that it is not even. All integers, then, are either even or odd, never neither and never both.

The numbers -4, -2, 0, 2, and 4 are even, while the numbers -3, -1, 1, and 3 are odd. Notice that in between every two even numbers is an odd number, and in between every two odd numbers is an even number. Indeed, if we add 1 to an even number, we will always get an odd number; if we add 1 to an odd number, we will always get an even number.

Furthermore, any odd number is exactly 1 more than some even number. What we conclude is that any odd number can be written as $2n + 1$, where n is some integer. In addition, any integer of the form $2n + 1$, where n is some integer, is odd. (The expression $2n + 1$ means $(2 \times n) + 1$. We perform the multiplication first because of the order of operations.)

2.1.1 Determining Parity

It is easy to determine whether a number is even or odd. Let's start with small examples first. We know $4 = 2 \times 2$, so it's even. We know $7 = 2 \times 3 + 1$, so it's odd. A number is either even or odd, but it's never both. We only need to divide by 2: if it evenly divides, then it's even, and otherwise, it's odd.

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

Figure 2.1: Result of adding numbers, by parity

Example 2a. **Odd or Even I**

Are each of the following numbers even or odd?

- 10 [✓ Even] Odd
- 0 [✓ Even] Odd
- 19 Even [✓ Odd]
- -1 Even [✓ Odd]

If the numbers are very big, it is convenient to simply observe the last digit. If the last digit is even, then the whole number is even. If the last digit is odd, then the whole number is odd. Why does this work? We will see very soon.

2.1.2 Sums & Differences

What happens if we add two odd numbers? Two even numbers? Let's find out. Say $2n + 1$ and $2m + 1$ are two odd numbers. We're using letters here as placeholders; n and m can both take the value of any integer. Then

$$(2n + 1) + (2m + 1) = 2n + 2m + 1 + 1 = 2n + 2m + 2 = 2(n + m + 1)$$

but $n + m + 1$ is an integer, and therefore the sum is even.

We can use a very similar strategy to find the sum of two even numbers. This is even easier. Say $2n$ and $2m$ are two even numbers. Then

$$2n + 2m = 2(n + m)$$

but $n + m$ is an integer, and therefore the sum is even.

Say $2n$ is an even number, and $2m + 1$ is an odd number. Then

$$2n + 2m + 1 = 2(n + m) + 1$$

which is an odd number. So the sum of an even number and an odd number is odd. And because we can rearrange the order of addition, therefore the sum of an odd number and a even number is also odd. These results can be summarized in a table (see Figure 2.1).

The rules for subtracting are exactly the same. The difference of two odds is even. The difference of two evens is even. The difference of an odd and an even is odd. These results are summarized in Figure 2.2. Feel free to work these out yourself.

−	Even	Odd
Even	Even	Odd
Odd	Odd	Even

Figure 2.2: Result of subtracting numbers, by parity

×	Even	Odd
Even	Even	Even
Odd	Even	Odd

Figure 2.3: Result of multiplying numbers, by parity

Example 2b. **Odd or Even II**

Are each of the following numbers even or odd?

- $100 + 200$ [✓ Even] Odd
- $1273 + 19023$ [✓ Even] Odd
- $19082 - 1911$ Even [✓ Odd]
- $109291 + 8329 + 9107$ Even [✓ Odd]

2.1.3 Products

We can use a similar technique to develop rules for the product of even and odd numbers. It turns out that the product of two odd numbers is odd. Say $2n + 1$ and $2m + 1$ are two odd numbers. Observe:

$$\begin{aligned}(2n+1)(2m+1) &= 2n(2m+1) + (2m+1)\\ &= 4nm + 2n + 2m + 1\\ &= 2(2nm + n + m) + 1\end{aligned}$$

which is odd.

But the product of an even number with any integer is even. Say $2n$ is an even number, and k is any integer. Then:

$$(2n)k = 2(nk)$$

which is even. We may summarize these results in another table (see Figure 2.3)

At this point we have enough knowledge to see why our rule for determining parity by looking at the last digit works. In a number written in the place value system, such as 76103, we can split the number into the ones' digit, the tens' digit, hundreds' digit, and so on. Another way to think about it is, by splitting off the ones' digit,

$$76103 = 3 + 7610 \times 10$$

But we know that $10 = 2 \times 5$ is even, so by the rules covered above, we know that anything mutliplied by 10 remains even. Then if we add it to an odd number, we obtain an odd number, but if we add it to an even number, then we obtain an even number. Therefore, just by looking at the last digit, we can figure out whether a number is odd or even.

2.2 Divisibility

We will begin today's topic with a few definitions.

The symbol $|$ means "divides". If n and m are two numbers, then n divides m when $m \div n$ has no remainder; that is, when $m \bmod n = 0$. We write this as $n \mid m$.

A number is a *factor* of another number if it divides that number. For example, 3 is a *factor* of 9 because $3 \mid 9$. A number is a *multiple* of another number if the other number divides it. For example, 9 is a *multiple* of 3. Another word for factor, which we will see later on, is *divisor*.

We can see that if n and m are integers, then the following conditions are equivalent:

1. n is a factor of m
2. n divides m
3. m is a multiple of n
4. $m \bmod n = 0$
5. There exists integer k such that $m = nk$

Observe that 1 is a *factor* of every whole number, and 0 is a *multiple* of every whole number.

We also introduce the symbol $\nmid$ for "does not divide"; that is, for n and m two integers, $n \nmid m$ whenever it is not the case that $n \mid m$.

Example 2c. **Factors and Multiples**

Let a, b, and c be integers such that $c = ab$. Then

1. a must divide c [✓ True] False
2. b must be a multiple of c True [✓ False]

Solution: Since $c = a \times b$, and b is an integer, therefore $a \mid c$, so the first statement is always $\boxed{\text{true}}$.

But there is no requirement that $c \mid b$—take $a = b = 2$ and $c = 4$, for example. Here $4 \nmid 2$, so the second statement is $\boxed{\text{false}}$.

2.2.1 Finding Factors

One class of problem that we may be interested in solving is to list the factors for a number. When the number is small, this is easy. For example, listing the factors of 6 is as simple as trying out all smaller (or equal) positive integers, and finding that only 1, 2, 3, and 6 divide 6 evenly.

Note that -1, -2, -3, and -6 are also factors of 6. However, because these are redundant with the positive factors we found above, we typically only care about finding the positive factors of a number.

For larger numbers, we may exploit the fact that factors always come in pairs. If $a \mid c$, then there is some number b so that $a \times b = c$. But then we can just flip the order of the multiplication, and we see that $b \times a = c$ and therefore $b \mid c$. Therefore a convenient way to find big factors is to divide the original number by the smaller factors.

We will revisit this topic, and obtain a faster way to do this type of problem, in the future.

Example 2d. **Positive Factors of 30**

Find the first 4 positive factors of 30.

Solution: It is clear that $1 \mid 30$, $2 \mid 30$, and $3 \mid 30$. But since $30 \bmod 4 = 2$, then $4 \nmid 30$. So we check that $30 \bmod 5 = 0$, so $5 \mid 30$. Hence the first four factors are $\boxed{1, 2, 3, 5}$.

2.2.2 Revisiting Parity

Using our new definitions, we see that the topic we covered last class—even and odd numbers—is really just the study of numbers that are and aren't divisible by 2. Even numbers are the multiples of 2, and all even numbers have 2 as a factor. Be careful! Note that odd numbers do not necessarily have 3 as a factor (for example, 5 is not a mutliple of 3), and even numbers might (for example, 6 is a multiple of 3 and is also even.)

2.2.3 Divisibility Rules

Earlier we have already seen rules for divisibility by 2. We have a similar rule for divisibility by 5. The reason that this rule is correct will be discussed later in this unit, but please feel free to think about it. To figure out whether a number is divisible by 5, simply look at the last digit. If it is 0 or 5, then the number is divisible by 5.

For divisibility by 10, the rule is even simpler. A number is divisible by 10 if and only if the last digit is 0. A number is divisible by 100 if the last two digits are 0. (Note that 0 is a bit of a special case, since it only has one digit, but it is still divisible by 100.)

For divisibility by 3, the rule is a little complicated. A number is divisible by 3 if and only if the sum of its digits is divisible by 3. For example, 123456 is divisible by 3, because the sum of digits $1 + 2 + 3 + 4 + 5 + 6 = 21$ is.

2.2.4 Transitivity

The transitivity principle of divisiblity says that if a, b, and c are integers, and if $a \mid b$ and $b \mid c$, then $a \mid c$. Let's do an example. We know that $3 \mid 12$, and that $12 \mid 36$. Then by transitivity, $3 \mid 36$. Here is a simple exercise that is easily done using transitivity:

Example 2e. **Multiples of 12 and 3**

Does 3 divide *every* multiple of 12? [✓ True] False

Solution: Say a is some multiple of 12. By definition, $12 \mid a$. Here we are using a as a placeholder—it can stand for *any* multiple of 12.

Since $12 \div 3 = 4\,\mathrm{R}\,0$, we know that $3 \mid 12$. But if $3 \mid 12$ and $12 \mid a$, then by transitivity, $3 \mid a$. Therefore, the statement that 3 divides every multiple of 12 is $\boxed{\text{true}}$.

2.3 Review

There is a quiz for this chapter (Quiz 3: Parity and Divisibility). The anticipated length for the quiz is 15 minutes. Three review questions follow. Quiz questions will be very similar in nature.

Example 2f. **Factor Pairs**

Complete the factor pairs.

- $6 = 1 \times \boxed{6}$
- $6 = 2 \times \boxed{3}$
- $6 = 3 \times \boxed{2}$
- $6 = 6 \times \boxed{1}$

Example 2g. **Factors and Multiples**

Use the word “factor” or “multiple” to complete each blank.

- 1 is a $\boxed{\text{factor}}$ of every whole number.
- 0 is a $\boxed{\text{multiple}}$ of every whole number.
- 3 is a $\boxed{\text{factor}}$ of 9.
- All even numbers are $\boxed{\text{multiple}}$s of 2.

Example 2h. **Divisibility**

Circle factors of each number. More than one factor may be circled.

- 25 $\boxed{1}$ 2 $\boxed{5}$ 10 100
- 172 $\boxed{1}$ $\boxed{2}$ 5 10 100
- 1793 $\boxed{1}$ 2 5 10 100
- 2000 $\boxed{1}$ $\boxed{2}$ $\boxed{5}$ $\boxed{10}$ $\boxed{100}$

Chapter 3

Prime Numbers

A *prime number* is a positive integer that has exactly two positive factors: 1 and itself. We care about prime numbers because they are the basic building blocks for all other positive integers, a fact which we will look at in more depth later on.

3.1 Testing for Primality

We can easily check whether small numbers are prime. First, note 1 is not prime, because it has just one factor. However, 2 is prime, because it has exactly two factors: 1 and itself.

Example 3a. **The First Few Primes**

Is each number prime or not prime?

- 2 [✓ Prime] Not Prime
- 3 [✓ Prime] Not Prime
- 4 Prime [✓ Not Prime]
- 5 [✓ Prime] Not Prime
- 6 Prime [✓ Not Prime]
- 7 [✓ Prime] Not Prime
- 8 Prime [✓ Not Prime]
- 9 Prime [✓ Not Prime]
- 10 Prime [✓ Not Prime]

Don't get caught in the trap that every odd number is prime! $9 = 3 \times 3$ is not. Neither are 15, 21, 25, and many others. In fact, as the numbers get bigger and bigger, prime numbers get rarer and rarer. However, do note that there is only one even prime: 2.

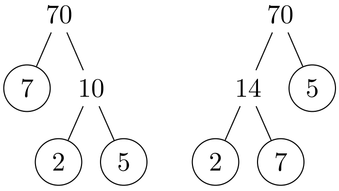

Figure 3.1: Two different factor trees for 70

3.2 Composite Numbers

A *composite* number is a number that can be written as the product of two smaller positive numbers. Thus $4 = 2 \times 2$ is composite. It turns out that every non-prime positive whole number except 1 is composite.

Composite numbers have at least three distinct factors. Usually, they have at least four (such as 6, which has factors 1, 2, 3, and 6), but there is a special category of numbers that have exactly 3. These are the squares of prime numbers. (Recall that a square is a number multiplied by itself.) For instance, 4 has factors 1, 2, and 4, and 9 has factors 1, 3 and 9. This happens when the only prime factor of a number is paired with itself.

When numbers get quite large, composite numbers vastly outnumber prime numbers. Many classes of numbers contain only one prime number and infinitely many composite numbers. For instance, among the powers of 2 (2, 4, 8, 16, . . .), only 2 is prime.

3.3 The Fundamental Theorem of Arithmetic

One of the most important facts about whole numbers, one that forms the basis for much of number theory, is the Fundamental Theorem of Arithmetic. This theorem is a result that states that every positive whole number can be factored uniquely into primes. What does that mean?

If we have a whole number, say, 70, we see that we can write it as 7×10. Furthermore, $10 = 2 \times 5$. So we can factor $70 = 7 \times 2 \times 5$. Each of these numbers is now prime, and so we cannot factor this further, except by introducing copies of 1, which is pointless. (We could always write a number as itself times 1, but since multiplying by 1 does not do anything, we might as well leave them out.)

But what if we had factored it a different way, first writing $70 = 5 \times 14$? Then we notice that $14 = 2 \times 7$, so we can change to $70 = 5 \times 2 \times 7$. The important thing is that this is the same factorization as last time, except in a different order. In fact, no matter, how we factor 70, we will always arrive at the same prime factorization (with possibly a different order).

One way to quickly determine the prime factorization is to use a factor tree. We draw the number we want to factor on top, and split it up into two children. If any child is prime, we leave it be; otherwise, we split that up further into two children. We repeat this procedure until all leaves are prime (see Figure 3.1 and Figure 3.2 for examples). The product of these leaves is the prime factorization.

Example 3b. **Prime Factorization I**

Find the prime factorization for each number.

- $12 = \boxed{2 \times 2 \times 3}$

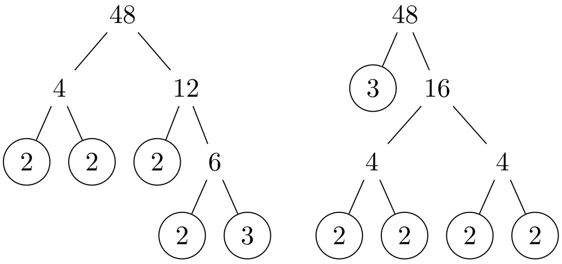

Figure 3.2: Two different factor trees for 48

- $70 = \boxed{2 \times 5 \times 7}$
- $100 = \boxed{2 \times 2 \times 5 \times 5}$

Example 3c. **Small Prime Factors I**

Find one prime factor for each number. Do not try to find additional factors.

- 99959386 Factor: $\boxed{2}$
- 521976505 Factor: $\boxed{5}$

3.3.1 Factoring Large Numbers

As we will see, it may be difficult to factor very large numbers. In fact, much of modern cryptography, including the popular RSA encryption scheme, relies on the fact that nobody has yet discovered a fast way to factor large numbers.

First, notice that checking whether large numbers are prime is quite hard to do on paper. However, it is sometimes easy to see that some numbers are composite. For example, if a number ends in 0, 2, 4, 5, 6, or 8, then it is probably composite—the only two exceptions are 2 and 5.

But given a large number, like 8644255723, how do we know whether it is prime or not? And how do we figure out its prime factorization? One way is to use *trial division*—just divide by all numbers starting from 1 until you find one that leaves no remainder. It turns out $8644255723 = 90907 \times 95089$, which are both prime numbers and cannot be factored further.

Then how many divisions do we have to do before we found the first number that works? We had to do 90907 divisions! That's a lot. If it took us one minute to do each division on paper, then it would take over two months of continuous work to find it.

Luckily, there are quicker ways to do factorization, and there are computers that can do it much faster than humans can. But even computers have their limits. Modern computers have a very hard time factoring numbers with thousands of digits. But there is a fast way of checking whether a number is prime.

The implication is that it is easy to find two two big prime numbers with a computer, and it is easy to multiply them, but it takes a long time to reverse that operation and break the big number back down into its prime factors.

As an interesting note, which we will not explore further in this class, there are actually infinitely many prime numbers. That means that no matter how big our prime numbers get, we can always find another bigger prime number.

3.3.2 Applications to Problem Solving

So far in this unit, we have not done so many applications to problems of the sort typically seen in math contests. However, this does not mean that the Fundamental Theorem of Arithmetic is not useful for contest math. Many questions can be simplified greatly by factorizing numbers into their prime factorizations. It is even useful for mental arithmetic. We will see some examples below.

Example 3d. **Mental Arithmetic**

Find, without using a calculator, 1875×48.

Solution: We compute

$$1875 = 5 \times 5 \times 5 \times 5 \times 3$$

and

$$48 = 2 \times 2 \times 2 \times 2 \times 3$$

so

$$\begin{aligned} 1875 \times 48 &= 5 \times 5 \times 5 \times 5 \times 3 \times 2 \times 2 \times 2 \times 2 \times 3 \\ &= 10 \times 10 \times 10 \times 10 \times 3 \times 3 \\ &= \boxed{90000} \end{aligned}$$

Factorizing numbers into primes before multiplying them is a common technique in mental math.

3.3.3 History

The Fundamental Theorem of Arithmetic is known to be true. But for most people, it is not obviously true. Why is it that all positive integers can be broken down *uniquely* into prime numbers? In mathematics, claims like the Fundamental Theorem of Arithmetic require proof. That is, we need a convincing argument that it is true for all numbers. The argument should depend only on facts that are known and accepted to be true, or facts that also have proofs. The first known proof for the Fundamental Theorem of Arithmetic was in book VII (7) of Euclid's Elements, propositions 30 and 32. This proof is not covered in the course.

3.4 The Sieve of Eratosthenes

Earlier, we found the first few prime numbers simply by finding factors. This is unfortunately quite a slow way to find prime numbers. With a few observations, we can find prime numbers much faster. Firstly, we noted earlier that all factors come in pairs. For example, $8 \mid 56$ (i.e. 8 is a factor of 56), so there is some number that we can multiply with 8 to get 56. This number is 7. We have $8 \times 7 = 7 \times 8 = 56$.

In the case of a perfect square, a factor could be paired with itself. For example, $10 \mid 100$, and indeed $10 \times 10 = 100$, so 10 is paired with itself. But being paired with itself still counts has being part of a factor pair.

You may have noticed that when we search for factors of numbers, we find the same factor pair possibly more than once. For instance, suppose we construct a factor table for 21, trying out all the numbers from 1 to 21. See Figure 3.3 for an example. This is a lot of work! It may seem at first like all the work is necessary, because we don't find the last factor, 21, until the last row. But notice that we have encounted all the factors by the third row: some of them are just on the right.

Indeed, this is where the idea of pairs comes in. Instead of checking every number, and try to get every pair of numbers $a \times b = 21$, we could only check the pairs $a \times b = 21$ where $a \leq b$. That is to say, once the left hand number exceeds the right hand number, then we don't need to check any more. The right hand side of Figure 3.3 shows an abbreviated table where we stop after checking 4. Why 4? Well, $5 \times 5 = 25$, which is already bigger than 21. So we know that if 5 did divide 21 (which it does not), then the factor it pairs with must be less than 5. But then we would have already found it.

This significantly reduces the amount of work we have to do. But is there an even quicker way? Over 2000 years ago, Eratosthenes of Cyrene devised an idea. First, notice that you can find all the prime factors, then you can find all the other factors. If we think of factorizing a number as breaking it down into the pieces that make it up, then the prime factorization is the most broken down state. We can recombine the prime factors to create the other factors.

For example, with $21 = 3 \times 7$, and this is the prime factorization. We can see that every factor of 21 is just 3, 7, or some combination. (Think of 1, the special case, as using no pieces.) See Figure 3.4 for a diagram showing this process.

This means that a good way to factor larger numbers might be to find all the prime factors first. That is, first find the prime factorization and then combine the primes to find the other factors. We saw the method of factor trees earlier, but in general we will need to have a list of prime numbers to do that in a reasonable amount of time.

Let's consider the problem of making such a list of prime numbers. Say we're interested in all the prime numbers between 2 and 100. An obvious way to go about making the list is to go through the integers, and decide whether each is a prime number. We can do that by testing whether it is divisible by any smaller prime number; if it is composite, then it must have a smaller prime that divides it. This means that we need to use the list as we make it.

This can take a long time, so let's consider an example finding just the prime numbers between 2 and 5 first. The steps for doing this using our current procedure are:

- Start with 2. It is prime. Our list is [2] right now.
- Now consider 3. We check that $2 \nmid 3$, since $3 \bmod 2 = 1$. So 3 is prime.
- Our list is now $[2, 3]$.
- Now consider 4. We check that $2 \nmid 4$, since $4 \bmod 2 = 0$. So 4 is not prime.
- Our list is still $[2, 3]$.
- Now consider 5. We check $2 \nmid 5$ and $3 \nmid 5$. So 5 is prime.

	21 =
✓	1×21
	$2 \times \ldots$
✓	3×7
	$4 \times \ldots$
	$5 \times \ldots$
	$6 \times \ldots$
✓	7×3
	$8 \times \ldots$
	$9 \times \ldots$
	$10 \times \ldots$
	$11 \times \ldots$
	$12 \times \ldots$
	$13 \times \ldots$
	$14 \times \ldots$
	$15 \times \ldots$
	$16 \times \ldots$
	$17 \times \ldots$
	$18 \times \ldots$
	$19 \times \ldots$
	$20 \times \ldots$
✓	21×1

	21 =	
✓	1×21	✓
	$2 \times \ldots$	
✓	3×7	✓
	$4 \times \ldots$	
	5 **stop**	

Figure 3.3: On the left, a factor table used to find the factors of 21; while this works, it's a lot of work, not all necessary. On the right, an abbreviated factor table that still finds all the factors, but is much less work to draw.

Use 3?	Use 7?	Factor
		1
✓		3
	✓	7
✓	✓	$3 \times 7 = 21$

Figure 3.4: A table listing all factors of 21 by combining subsets of the prime numbers

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

Figure 3.5: A grid of numbers between 1 and 25

$\cancel{1}$	②	③	$\cancel{4}$	⑤
$\cancel{6}$	⑦	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
⑪	$\cancel{12}$	⑬	$\cancel{14}$	$\cancel{15}$
$\cancel{16}$	⑰	$\cancel{18}$	⑲	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	㉓	$\cancel{24}$	$\cancel{25}$

Figure 3.6: A completed Sieve of Eratosthenes for numbers between 1 and 25

- Our list is now $[2, 3, 5]$.

This procedure is quite long and tedious. A better way is given by the Sieve of Eratosthenes, which involves crossing off all the multiples of each number we find, because those numbers aren't prime. The numbers left over must be prime.

We start with a grid like that in Figure 3.5. Then we do the following steps, to cross off all the non-prime numbers:

1. Cross off 1. It is not prime.
2. Circle 2, because it is a prime number. Cross off all bigger multiples of 2 (4, 6, 8, ...), because they are composite.
3. Circle the smallest number that hasn't been crossed off. Since it isn't divisible by any smaller prime (otherwise, it would have been crossed off), it must be prime. Now cross off all multiples of the number you just circled.
4. Repeat the last step until all numbers are crossed off or circled.

After completing these steps, the grid will look like Figure 3.6. The circled numbers are all the primes. This algorithm is much more efficient than trial division, because we can cross off multiples, which is easier to do than find remainders.

3.5 Review

Example 3e. **Small Prime Factors II**

Find one prime factor for each number. Do not try to find additional factors.

- 999958 Factor: $\boxed{2}$
- 999993 Factor: $\boxed{3}$
- 999995 Factor: $\boxed{5}$

Example 3f. **Prime Factorization II**

Find the unique prime factorization of each number.

- 55 $\boxed{5} \times \boxed{11}$
- 30 $\boxed{2} \times \boxed{3} \times \boxed{5}$
- 42 $\boxed{2} \times \boxed{3} \times \boxed{7}$
- 24 $\boxed{2} \times \boxed{2} \times \boxed{2} \times \boxed{3}$

Chapter 4

Greatest Common Divisor

4.1 Introduction

In this chapter, we will discuss two very important topics that have many applications: the greatest common divisor, and another similar operation, the least common multiple.

4.1.1 Greatest Common Divisor

Given two positive integers, we define their GCD (greatest common divisor) to be the largest positive integer that's a factor for both those numbers. For instance, the factors of 24 are 1, 2, 3, 4, 6, 8, 12, 24, and the factors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36. The greatest factor that these have in common is 12. Therefore we denote

$$\gcd(24, 36) = 12$$

Example 4a. **Examples**

- $\gcd(10, 20) = \boxed{10}$
- $\gcd(15, 25) = \boxed{5}$
- $\gcd(7, 11) = \boxed{1}$

4.1.2 Least Common Multiple

Similarly, given two positive integers, we define their LCM (least common multiple) to be the smallest positive integer that's a multiple of both those numbers. For instance, the positive multiples of 24 are 24, 48, 72, and so on, and the positive multiples of 36 are 36, 72, 108, and so on. The smallest multiple that these have in common is 72. Therefore we denote

$$\operatorname{lcm}(24, 36) = 72$$

An intriguing connection between the GCD and the LCM is given by the following identity, which we will not justify in this class, but you may see again in the future:

$$\gcd(a, b) \times \operatorname{lcm}(a, b) = a \times b \tag{4.1}$$

Roughly speaking, this identity says that the product of two numbers is the same as the product of their GCD and their LCM.

4.2 Application to Rational Numbers

The GCD and the LCM have many applications across mathematics. An important application is to the study of rational numbers, or fractions. Recall that a fraction is a pair of two integers, the numerator and the denominator. Additionally, the denominator is not allowed to be zero, because we cannot split any quantity into zero parts.

Note that a fraction does not have a unique representation as a numerator and denominator. Two fractions may be equal even if the numerator and the denominators differ. For instance, the fraction $\frac{1}{2}$ is equal to fractions $\frac{2}{4}$, $\frac{3}{6}$, and so on.

We may *simplify* a fraction by writing it as an equivalent fraction with least possible (positive) denominator. Simplifying fractions makes it easy to determine whether two fractions are equivalent, and also makes fractions easier to work with. There exists a simple algorithm to simplify a fraction. Given $\frac{n}{m}$, compute $d = \gcd(n, m)$, and then $\frac{n \div d}{m \div d}$ is the simplest form.

Example 4b. **Simplify Fraction**

Simplify. Note that the fraction may possibly already be in simplest form.

- $\frac{20}{15} = \boxed{\frac{4}{3}}$
- $\frac{24}{36} = \boxed{\frac{2}{3}}$
- $\frac{7}{13} = \boxed{\frac{7}{13}}$

When we add or subtract fractions, it helps often to write the fractions with equal denominator. To select a compatible denominator, we may use the least common multiple. For example, to add $\frac{a}{b} + \frac{c}{d}$, we may compute $\ell = \operatorname{lcm}(b, d)$ and then compute

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{a\ell \div b}{\ell} + \frac{c\ell \div d}{\ell}\\ &= \frac{a\ell \div b + c\ell \div d}{\ell}\end{aligned}$$

which then we may simplify with the algorithm described above.

Example 4c. **Adding and Subtracting Fractions**

Add or subtract. Then simplify.

- $\frac{1}{2} + \frac{1}{3} = \boxed{\frac{5}{6}}$
- $\frac{3}{4} + \frac{1}{6} = \boxed{\frac{11}{12}}$

- $\frac{23}{36} - \frac{11}{24} = \boxed{\frac{13}{36}}$

4.3 Euclidean Algorithm

An algorithm is a "step-by-step procedure for performing a calculation according to well-defined rules" (Wikipedia).

In this lesson we will cover a useful algorithm that allows us to find the greatest common divisor of two large numbers. This algorithm has been known for thousands of years. It was discovered by the Ancient Greeks, and is named after Euclid, one of the most famous mathematicians in history.

This algorithm is based on the fact that the greatest common denominator does not change if the smaller number is subtracted from the larger one. That is, $\gcd(a, b) = \gcd(a, b - a)$ for all positive integers a and b, with $b > a$. Proving this fact is beyond the scope of this course. However, we will look at an example.

Consider $\gcd(8, 12) = 4$. If we subtract 8 from 12, we get $\gcd(8, 4) = 4$. If we subtract now 4 from 8, we get $\gcd(4, 4) = 4$. We notice that the GCD is unchanged despite these subtractions.

To avoid subtracting potentially many times, we can change the repeated subtraction into a remainder operation. Thus we arrive at the most commonly stated version of the Euclidean algorithm:

4.3.1 The Euclidean Algorithm

To find the Greatest Common Divisor of two numbers, a and b:

1. If $a = 0$, then terminate. The greatest common divisor is b.
2. Otherwise, apply the Euclidean Algorithm to find the GCD of $b \bmod a$ and a. That is, $\gcd(a, b) = \gcd(b \bmod a, a)$.

4.3.2 Properties

This algorithm is an example of a recursive algorithm. More specifically, it is a "tail recursive" algorithm. That means that the algorithm either produces a result, or it requires running the algorithm another time on simpler numbers. We may need to run the Euclidean algorithm several times on progressively simpler numbers before finishing the computation.

Although the Euclidean algorithm may take some time to compute by hand, it is very easy for a computer to do. In fact, the algorithm is so efficient that computers can easily calculate the greatest common divisors of numbers with thousands of digits, in a matter of milliseconds!

4.3.3 Examples

Here is a quick example of using the Euclidean algorithm to compute the greatest common divisor of medium-sized numbers:

Example 4d. **GCD of Two Numbers**

Compute $\gcd(60, 84) = \boxed{12}$.

Solution:

$$\begin{aligned}
\gcd(60, 84) &= \gcd(84 \bmod 60, 60) \\
&= \gcd(24, 60) \\
&= \gcd(60 \bmod 24, 24) \\
&= \gcd(12, 24) \\
&= \gcd(24 \bmod 12, 12) \\
&= \gcd(0, 12) \\
&= 12
\end{aligned}$$

We may alternatively seek to find the GCD of multiple (more than two) numbers. This means the largest number that is a divisor of all the numbers we're interested in. We can do this by finding the GCD of the first two, and then finding the GCD of that number and the third, and so on. That is, we use the formula

$$\gcd(a, b, c, d, \dots) = \gcd(\gcd(a, b), c, d, \dots)$$

This computation may require several long and tedious applications of the Euclidean algorithm. Luckily, in practice, when GCDs for large numbers must be computed, computers can typically be used. You will not be required to do problems of this sort on your homework or quizzes.

Example 4e. **GCD of Three Numbers**

Compute $\gcd(3636, 3948, 4056) = \boxed{12}$.

Solution:

$$\begin{aligned}
\gcd(3636, 3948, 4056) &= \gcd(\gcd(3636, 3948), 4056)\\
&= \gcd(\gcd(3948 \bmod 3636, 3636), 4056)\\
&= \gcd(\gcd(312, 3636), 4056)\\
&= \gcd(\gcd(3636 \bmod 312, 312), 4056)\\
&= \gcd(\gcd(204, 312), 4056)\\
&= \gcd(\gcd(312 \bmod 204, 204), 4056)\\
&= \gcd(\gcd(108, 204), 4056)\\
&= \gcd(\gcd(204 \bmod 108, 108), 4056)\\
&= \gcd(\gcd(96, 108), 4056)\\
&= \gcd(\gcd(108 \bmod 96, 96), 4056)\\
&= \gcd(\gcd(12, 96), 4056)\\
&= \gcd(\gcd(96 \bmod 12, 12), 4056)\\
&= \gcd(\gcd(0, 12), 4056)\\
&= \gcd(12, 4056)\\
&= \gcd(4056 \bmod 12, 12)\\
&= \gcd(0, 12)\\
&= \boxed{12}
\end{aligned}$$

We may cover a few assorted problems to reinforce your ability to compute the GCD using the Euclidean algorithm. However, in general, this computation is not difficult, but is brainless and long, and I do not recommend you do many of these problems for practice.

Example 4f. **Assorted GCD Problems**

Use the Euclidean Algorithm to compute the following:

- $\gcd(12, 28) = \boxed{4}$
- $\gcd(147, 392) = \boxed{49}$
- $\gcd(319, 920) = \boxed{1}$
- $\gcd(2635, 4515) = \boxed{5}$
- $\gcd(12936, 25256) = \boxed{616}$
- $\gcd(399, 1533, 1659, 2016) = \boxed{1}$

4.3.4 Computer Algorithm

One advantage of an algorithm is that we can run them on a computer. For your interest, in Figure 4.1 we have an implementation of the Euclidean algorithm

```
gcd(a, b) = if a == 0
    abs(b)
else
    gcd(rem(b, a), a)
end
```

Figure 4.1: An implementation of the Euclidean algorithm in Julia

in the Julia programming language. In the Julia language, `abs` represents the absolute value, and `rem` represents the remainder.

As mentioned earlier, the Euclidean algorithm is quite efficient. But in fact, there are even more efficient algorithms for finding the GCD of two large numbers on a computer. Computers can find the GCD of two huge numbers almost instantly—even if the numbers involved have thousands of digits.

Chapter 5

Modular Arithmetic

The final chapter in this unit will be brief, and you will not be quizzed on the material. However, the content of this chapter will certainly be interesting.

In earlier chapters we discussed briefly remainders and some applications. In this chapter, we will develop new powerful techniques to simplify the solution to these problems.

5.1 Generalizing Parity

When we talked about even and odd numbers, we came up with rules about the result of adding, subtracting, and multiplying even and odd numbers. We can come up with similar strategies for divisibility by any number, not just 2. For the purposes of discussing this with greater ease, we will consider 7 as our base.

All positive integers (in fact, all integers, including zero and negative ones) can be categorized into 7 distinct buckets based on their remainder when divided by 7. Let us call these buckets [0], [1], [2], [3], [4], [5], and [6]. In the following table we have categorized the numbers from 0 to 30 into these buckets:

[0]	0	7	14	21	28
[1]	1	8	15	22	29
[2]	2	9	16	23	30
[3]	3	10	17	24	
[4]	4	11	18	25	
[5]	5	12	19	26	
[6]	6	13	20	27	

We can see a few patterns in the above table. When we add 1 to a number, we move to the next bucket. But [6] has no next bucket, so what happens when we add 1 to a number in bucket [6]? We move to bucket [0]! In some sense, these buckets form a sort of cycle. After we reach the last bucket, we loop around and return to the first bucket (Figure 5.1).

This behaviour should make sense when starting at buckets [0] to [5]. But for bucket [6], why is it that we move to bucket [0] by adding one more? We can find the solution using algebra, just like how we did when talking about parity. Any number in bucket [6] looks like $7n+6$ for some integer n. If we add 1 to this,

$$7n + 6 + 1 = 7n + 7 = 7(n + 1)$$

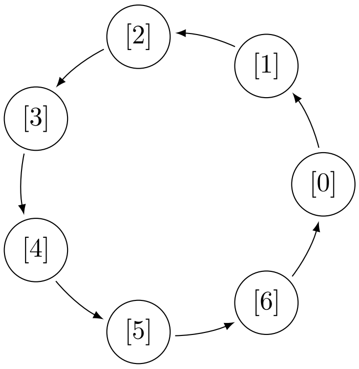

Figure 5.1: When we add 1 to a number in a bucket, we move to the next bucket in this diagram.

and we can see that this is a multiple of 7, and so belongs in bucket [0].

We now consider what happens if we add 2 to a number. In which bucket would the new number be in? This is the same as adding 1 twice. So, for example, [0] goes to [2], [4] goes to [6], [5] goes to [0] and [6] goes to [1]. Again, we are just moving around in circles. It is similar to addition on the number line, but instead of going in a line, we are going in a cycle.

The process of addition is moving numbers from one remainder bucket to the next several times. What happens if we add 7? Well, we would have gone one whole cycle around, and so our result should be in the same bucket. And indeed, that is what we would expect, since adding 7 should not change the remainder when dividing by 7.

The same goes for any multiple of 7. If we add 21, we would go around one whole cycle 3 times, and then arrive back where we started. For bigger numbers that are not multiples of 7, we can think of the addition as moving around the whole cycle several times, then moving some extra steps. How many extra steps do we move? Why, the remainder when divided by 7, of course.

To recap, we have devised a system where we can predict the remainder of a sum when divided by 7, knowing just the remainders of the two summands when divided by 7. We simply start at the bucket for the first number and advance a number of buckets in the cycle equal to the remainder of the second number when divided by 7. We introduce the following notation:

$$[1] + [2] = [3]$$

to mean that the sum of a number in bucket [1] and a number in bucket [2] is a number in bucket [3].

We can return to algebra to provide a justification for this behaviour. Say $n \bmod 7 = i$, and $m \bmod 7 = j$. Then let $n = 7k + i$ and $m = 7\ell + j$. We see that

$$\begin{aligned}(n + m) \bmod 7 &= (7k + i + 7\ell + j) \bmod 7\\ &= (7(k + \ell) + i + j) \bmod 7\\ &= (i + j) \bmod 7\end{aligned}$$

which is the same as saying that the remainder of the sum of two numbers when divided by 7 is the same as the remainder of the sum of the remainders when divided by 7. In other words, the bucket of the result is determined only by the buckets of the summands.

By now we have come up with a generalization of the concept of parity (for divisibility by 2) to divisibility by 7. Instead of categorizing numbers into even and odd numbers, we categorize them into the 7 buckets depending on their remainder when divided by 7. But we could have chosen any positive integer to start with, not just 7. By using the same techniques we applied above, we can create a new way of analyzing numbers using any positive integer as our base.

5.2 Introducing Multiplication

For simplicity, we'll continue to use 7 as our base, but keep in mind that the interesting results we will notice are valid in other bases also. Above, we saw the important fact that the remainder of the sum of two numbers is the same as the remainder of the sum of the remainders of two numbers. There is a similar fact for multiplication. Indeed,

$$ab \bmod 7 = (a \bmod 7)(b \bmod 7) \bmod 7$$

That is, instead of multiplying two numbers and then taking the remainder of the product, we can instead multiply their remainders and take the remainder of that. While above we gave an algebraic explanation for the sum of two numbers, for the sake of time we will not do that for the product. But a similar algebraic explanation is possible, and if you are interested, you may try to devise it yourself.

We are able to solve advanced problems easily by applying the techniques shown above. Let us consider, for example, the following problems:

Example 5a. **A Million Days**

Today is Sunday. 1000 days later, it will be Saturday. 1000000 days later, what day will it be?

Solution:

The question tells us that 1000 days later, it will be Saturday. Since Saturday is 6 days past Sunday, we know that 1000 mod 7 = 6.

We need to compute 1000000 mod 7. We can use the technique developed above to simplify:

$$\begin{aligned}1000000 \bmod 7 &= (1000 \times 1000) \bmod 7\\ &= ((1000 \bmod 7) \times (1000 \bmod 7)) \bmod 7\\ &= (6 \times 6) \bmod 7\\ &= 36 \bmod 7\\ &= 1\end{aligned}$$

so after 1000000 days, the day of the week will be 1 past Sunday, hence $\boxed{\text{Monday}}$.

Example 5b. **A Large Power of 2**

Find 2^{32} mod 7.

Solution:

We could find the product, but that would take a long time. Since 16 is a power of 2, it may be useful to consider the remainders of 2^1, 2^2, 2^4, 2^8, 2^{16}, and then finally 2^{32}.

First, note that $2 \bmod 7 = 2$. Then note $2^2 \bmod 7 = 4 \bmod 7 = 4$. Next, note that

$$\begin{aligned} 2^4 \bmod 7 &= (2 \times 2 \times 2 \times 2) \bmod 7 \\ &= 16 \bmod 7 \\ &= 2 \end{aligned}$$

and so far, all the calculations have been short and easy.

For $2^8 \bmod 7$, instead of calculating the product, we could apply the above result:

$$\begin{aligned} 2^8 \bmod 7 &= (\underbrace{2 \times 2 \times \cdots \times 2}_{\text{8 twos}}) \bmod 7 \\ &= (2 \times 2 \times 2 \times 2)(2 \times 2 \times 2 \times 2) \bmod 7 \\ &= 16 \times 16 \bmod 7 \\ &= (16 \bmod 7)(16 \bmod 7) \bmod 7 \\ &= 2 \times 2 \bmod 7 \\ &= 4 \bmod 7 \\ &= 4 \end{aligned}$$

Next, for $2^{16} \bmod 7$, we do the same thing again:

$$\begin{aligned} 2^{16} \bmod 7 &= (\underbrace{2 \times 2 \times \cdots \times 2}_{\text{16 twos}}) \bmod 7 \\ &= (\underbrace{2 \times 2 \times \cdots \times 2}_{\text{8 twos}})(\underbrace{2 \times 2 \times \cdots \times 2}_{\text{8 twos}}) \bmod 7 \\ &= 2^8 \times 2^8 \bmod 7 \\ &= (2^8 \bmod 7)(2^8 \bmod 7) \bmod 7 \\ &= 4 \times 4 \bmod 7 \\ &= 16 \bmod 7 \\ &= 2 \end{aligned}$$

And finally, one more time for $2^{32} \bmod 7$:

$$\begin{aligned} 2^{32} \bmod 7 &= (\underbrace{2 \times 2 \times \cdots \times 2}_{\text{32 twos}}) \bmod 7 \\ &= (\underbrace{2 \times 2 \times \cdots \times 2}_{\text{16 twos}})(\underbrace{2 \times 2 \times \cdots \times 2}_{\text{16 twos}}) \bmod 7 \\ &= 2^{16} \times 2^{16} \bmod 7 \\ &= (2^{16} \bmod 7)(2^{16} \bmod 7) \bmod 7 \\ &= 2 \times 2 \bmod 7 \\ &= 4 \bmod 7 \\ &= \boxed{4} \end{aligned}$$

5.3 Notation

The kind of computation we were doing above is known as *modular arithmetic*. Sometimes it is convenient to use specialized notation to describe operations. Now we will take look at the commonly used notation, and how it can be used to solve problems.

First, we introduce the concept that two numbers are *congruent* modulo some base k if they have the same remainder when divided by k. For example, 17 and 10 are congruent modulo 7, because

$$17 \bmod 7 = 3 = 10 \bmod 7$$

.

We can write this as:

$$17 \equiv 10 \pmod{7}$$

or alternatively without the brackets, but keeping the additional space, as

$$17 \equiv 10 \mod 7$$

By working with congruences, we can solve complex problems in relatively few lines of work. For instance, consider the following.

Example 5c. **Huge Number, Small Remainder**

Define $10! = 10 \times 9 \times 8 \times \cdots \times 1$. Find $10! \bmod 72$.

Solution: We see that

$$\begin{aligned} 10! &\equiv 10 \times 9 \times 8 \times \cdots \times 1 \mod 72 \\ &\equiv 9 \times 8 \times 10 \times 7 \times 6 \times \cdots \times 1 \mod 72 \\ &\equiv 72 \times 10 \times 7! \mod 72 \\ &\equiv 0 \times 10 \times 7! \mod 72 \\ &\equiv 0 \mod 72 \end{aligned}$$

so $10! \bmod 72 = \boxed{0}$.

Example 5d. **Units Digit**

Find the ones' digit of the following sum:

$$40 + 7874 + 648 + 56 + 338$$

Solution: We seek

$$(40 + 7874 + 648 + 56 + 338) \bmod 10$$

It is straightforward to compute this:

$$\begin{aligned} 40 + 7874 + 648 + 56 + 338 &\equiv 0 + 4 + 8 + 6 + 8 \\ &\equiv 26 \\ &\equiv 6 \pmod{10} \end{aligned}$$

and hence the ones' digit of the desired sum is $\boxed{6}$.

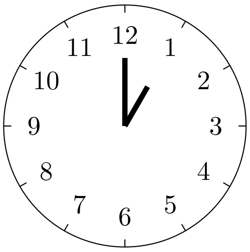

Figure 5.2: A 12-hour clock displaying the time 1:00.

Example 5e. **Clock Arithmetic**

A 12-hour analog clock (which are increasingly rare nowadays) is a time-keeping device numbered from 1 to 12 (see Figure 5.2). There are two hands. The longer one is the minute hand, which measures minutes, and the shorter one is the hour hand, which measures hours. Each hour, the hour hand of the clock moves clockwise (that is, up one number) by one labelled segment. Every 12 hours, the clock returns to its original orientation. For the purposes of this question, we'll ignore the minute hand and focus only on the hour hand.

If a clock's hour hand is pointing to the 5 right now, to where was it pointing 13 × 29 hours ago?

Solution: We seek $5 - 13 \times 29 \bmod 12$. It is straightforward to calculate this with modular arithmetic:

$$\begin{aligned} 5 - 13 \times 29 &\equiv 5 - 1 \times 5 \\ &\equiv 5 - 5 \\ &\equiv 0 \pmod{12} \end{aligned}$$

Of course, there is no 0 on the clock—in its place is $\boxed{12}$, which was where the hour hand was pointing.

5.4 Further Study

We do not have time to further discuss modular arithmetic in this course. But this subject is very powerful, and you will see it again and again in the future.

Glossary

algorithm step-by-step procedure for performing a calculation according to well-defined rules (Wikipedia). 18, 22

equivalent two statements are equivalent when they occur in exactly the same situations; for example, being even and being divisible by 2 are equivalent. 8

even a property of numbers divisible by 2; m is even whenever $m = 2n$ for some integer n. 5

implementation an algorithm that has been realized in some programming language and can be executed by a computer. 24

integer positive or negative whole number, or 0; for example, -8, 2000. 3

multiplicand the number that is being multiplied; for instance, in $2 \times 3 = 6$, the multiplicand is 2. 3

multiplier the factor to multiply a number by; for instance, in $2 \times 3 = 6$, the multiplier is 3. 3

odd a property of numbers not divisible by 2; m is odd whenever there is no integer n for which $m = 2n$. 5

parity decribes whether an integer is even or odd. 5

product the result of a multiplication; for instance, in $2 \times 3 = 6$, the product is 6. 3

programming language a structured grammar and syntax written by and understandable by humans but for the purpose of execution by a machine. 25

summand something which is being added; for instance, in $1 + 2 = 3$, the two summands are 1 and 2. 27

transitivity the property of certain relations that specifies if an element a is related to b, and the element b is related to c, then a is similarly related to c. 9

List of Figures