4 Number Theory I: Prime Numbers

Number theory is the mathematical study of the natural numbers, the positive whole numbers such as 2, 17, and 123. Despite their ubiquity and apparent simplicity, the natural integers are chock-full of beautiful ideas and open problems. A primary focus of number theory is the study of prime numbers, which can be viewed as the elementary building blocks of all numbers.

4.1 Number Theory

The natural numbers are those basic abstraction of quantity we first learn about as children; in particular they are the positive whole numbers:

$$\mathbb{N} = \{1, 2, 3, \ldots\}. \tag{36}$$

Although simple in some sense, the patterns and relationships that appear among these numbers have intrigued and challenged generations of the mathematicians. Despite hundreds of years of progress, there is still many areas we know very little about. We begin by very briefly considering three kinds of problems that arise in number theory, and which highlight different aspects of the subject.

1. Remainders of Large Numbers

Since elementary school, readers of these notes have known how to divide two integers and calculate whole numbers plus remainders. For example, we can divide 17 by 3 and obtain 5, remainder 2. If we use R to indicate the remainder after division, we have:

$$\begin{aligned} 83/9 &= 9, R1 \\ 23/16 &= 1, R7 \\ 107/27 &= 3, R26. \end{aligned}$$

All of these calculations can be made on a simple four-function calculator without much trouble.

When the numbers we are dividing become slightly larger, similar calculations can be made with slightly more effort. For example, we have:

$$\begin{aligned} 83^2/9 &= 765, R4 \\ 23^2/16 &= 33, R1 \\ 107^2/27 &= 424, R1. \end{aligned}$$

These examples too can be calculated using a simple four-function calculator. If we were so inclined, we could also solve these division problems by hand using long division.

However, when the number become significantly larger, conventional methods can no longer help us. Consider for example the following problems:

$$\begin{aligned} 83^{2019313}/9 &= ?, R2 \\ 23^{1323122}/16 &= ?, R1 \\ 107^{8723039}/27 &= ?, R26. \end{aligned}$$

Here, even the most most powerful calculators and computers will have significant trouble computing the correct answers. You may have noticed that half of each question was left blank, where the correct whole number is indicated by a ?, but the remainders in each question are still filled in. The correct whole number itself is quite long, well over a million digits long, and even could easily compute the number, writing it down would take a very long time. Is it somehow possible, however, to only compute the remainder, without also knowing the whole number to its left? **Modular arithmetic**, an area of number theory we will allow us to do exactly this, and hence divide gigantic numbers by smaller ones and exactly determine the remainder, without even knowing the whole number answer.

The ability to perform these calculations results in our ability to encrypt data and communicate secularly over the internet. Every time you order something online, your computer uses modular arithmetic to calculate remainders of gigantic numbers. We will discuss how this works towards the end of the semester.

2. Integer Solutions of Pythagorean-like Equations

Consider the set $\mathbb{N}$ and the following equations:

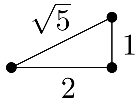
$$\begin{aligned} 2+3 &= 5 \\ 4+7 &= 11 \\ 8+9 &= 17. \end{aligned}$$

In each equation, we have two elements of $\mathbb{N}$ that are combined through addition to form another element of $\mathbb{N}$. The reader will likely find nothing surprising in any of these equations – by this point, we have been adding together whole numbers to make other whole numbers for many, many years.

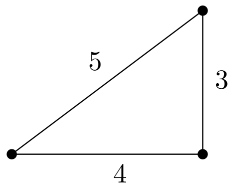
Next, consider the set of squares, $S = \{1^2, 2^2, 3^2, 4^2, \ldots\}$, and the following simple equations:

$$\begin{aligned} 3^2+4^2 &= 5^2 \\ 5^2+12^2 &= 13^2 \\ 20^2+21^2 &= 29^2. \end{aligned}$$

In each equation here, we have two elements of S that are combined to form another element of S. To some, these numbers may rings bells reminding of us the Pythagorean theorem. This theorem states that if two numbers a and b are side lengths of a right triangle (a triangle one of whose internal angles is 90°), and if c is the length the triangle's hypotenuse, then $a^2 + b^2 = c^2$. For example, consider the triangle illustrated below. Its two sides have lengths 1 and 2, and its



hypotenuse has length $\sqrt{5}$. These satisfy the equation $1^2 + 2^2 = \sqrt{5}^2 = 5$, which the reader can readily verify. In this particular situation not all three sides are integers, or even rational numbers. However, it is possible to find some right triangles such that all three sides (including the hypotenuse) are integers. For example, consider the triangle with side lengths 3 and 4 and hypotenuse length 5, illustrated below. Here is an example in which all three sides (including the



hypotenuse) are whole numbers. Although it might not be clear at this point, we can in fact make infinitely many triangles with integer length sides.

In any case, we point out that the Pythagorean theorem describes all right triangles, not only those with integer sides. At this point, however, we restrict ourselves to sets of natural numbers $\{a, b, c\}$ that satisfy the equation $a^2 + b^2 = c^2$. It turns out that there are infinitely many such sets, though we will not prove this here.

Finally, consider the set of cubes, $C = \{1^3, 2^3, 3^3, 4^3, \ldots\}$. Any attempt to find two elements of C that can be added together to create a third element of C will end in failure. Although we were able to find numbers a, b, and c, such that $a^2 + b^2 = c^2$, there are no sets of natural numbers $\{a, b, c\}$ so that $a^3 + b^3 = c^3$. In fact, there are also sets such that $a^4 + b^4 = c^4$. More generally, there are no sets of natural numbers $\{a, b, c\}$ such that $a^n + b^n = c^n$ if n is an integer greater than 2. This result is commonly known as Fermat's Last Theorem. Pierre de Fermat was a tremendous 17th century French mathematician who proved many deep results in many area of mathematics, including geometry, algebra, analysis, probability, and number theory. Fermat wrote this "theorem" in the margin of a book he was reading (a book called *Arithmetica*, written by the Greek mathematician Diophantus) and indicated that the margin was too small for him to record in it a proof of this beautiful theorem. Nowhere else did Fermat describe his proof of the theorem, and hundreds of years went by before anyone else was able to finally establish this result. Andrew Wiles, a Brittish mathematician, finally did so in the early 1990's. Whether Fermat himself actually had a simple proof of the simple-sounding theorem is unknown, though it is certain that he could not have discovered the proof of Wiles, which required mathematical tools which took hundreds more years to develop.

3. Perfect Numbers

Every natural number has a set of divisors, the numbers which can evenly divide the number. For example, the natural numbers $1, 2, 3, 4, 6$, and 12 all divide the number 12 itself. The number 33 has fewer divisors, which are 1, 3, 11, and 33 itself. For each number n, let's consider the set D_n of positive integers that divide n and which are also smaller than n. Here are several examples:

$$\begin{aligned}
D_4 &= \{1, 2\} \\
D_5 &= \{1\} \\
D_6 &= \{1, 2, 3\} \\
D_7 &= \{1\} \\
D_{26} &= \{1, 2, 13\} \\
D_{27} &= \{1, 3, 9\} \\
D_{28} &= \{1, 2, 4, 7, 14\}
\end{aligned}$$

Two simple observations can be made. First, notice that $|D_n|$, the number of elements in D_n does not depend in a simple way on n. However, notice that when n is a prime number, then $D_n = \{1\}$, since it is the only positive integer smaller than n which divides n.

For each n we can also consider the sum of all elements in D_n. If n is a prime number, than this sum is 1, because that is the only number in D_n. For other numbers, though, this number can be bigger. Notice that for some particular numbers, this number is equal to n. For example, $D_6 = \{1, 2, 3\}$, and if we sum the numbers in D_6, we obtain $1 + 2 + 3 = 6$. Likewise, when $n = 28$ we have $1 + 2 + 4 + 7 + 14 = 28$. Such numbers, for which the sum of the divisors equals the number itself, are called **perfect numbers**. Although we are familiar with several examples of perfect numbers (for example 6, 28, 496, and 8128), it is not known whether there are an infinite number of these, or whether any of them are odd.

These sorts of questions are somewhat abstract, but they highlight some of the complications that can arise in studying relatively simple objects such as whole numbers. Number theory is filled with questions of patterns and structure in whole numbers. One of the most important subsets of the natural numbers are the prime numbers, to which we now turn our attention.

4.2 Prime Basics

Prime numbers can be thought of as the building blocks of all natural numbers, and we now take a look at what they are and some of their properties. We begin with a definition.

Definition 11. *A natural number larger than 1 is called* **prime** *if it can be evenly divided only by 1 and itself; other natural numbers greater than 1 are called* **composite***.*

To give a intuitive description, we might think of a group of objects and ask whether we can divide the group of objects into several small groups, each with an equal number of objects. Depending on the number of objects in the original group, we might be able to divide the group in several ways, or in no ways at all. If we have 20 people in a room, we might break them into 4 groups of 5, or perhaps 2 groups of 10. If there are 25 people in the room, then the only way we can evenly divide them is by separating them into five groups of 5 people each. For some groups, though, there is no way at all divide them into separate groups. For example, if there are 13 people in the room, there is no way to evenly divide them, except if want to divide them into 13 "groups" with one person each. Natural numbers which cannot be "broken up" into products of smaller natural numbers (greater than 1) are called prime. In some sense, the prime numbers 2, 3, 5, etc. are the "atoms" (taken in the classical sense, meaning indivisible) that make up all natural numbers, in the way that hydrogen, helium, lithium, etc make up the matter of our universe. Unlike the periodic table of the elements, however, the list of prime numbers goes on indefinitely.

Infinitude of Primes

Euclid of Alexandria was a Greek mathematician who lived several centuries before the common era. Aside from his many contributions to geometry, Euclid also made important contributions to our understanding of numbers. In particular, Euclid showed that for any finite number n, there are more than n prime numbers. This is equivalent to what we would say, "There are infinitely many primes". Euclid proved this by showing that if we take any finite set of prime numbers, we can always find another prime number that is not in that set.

Theorem 4. *There are infinitely many prime numbers.*

Proof. Suppose that there are only a finite number n prime numbers. We can then make a complete list of all them – let's call these primes $p_1, p_2, \dots p_n$, so that p_i is the ith prime number, and p_n is the last one; for example, the first several prime numbers are: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ (remember that we don't usually count 1 as a prime number). As far we now know, this is a complete list of all prime numbers. Euclid showed that for any such list of prime numbers, there is always at least one prime number that is not on that list; this shows that there is no such thing a complete finite list of prime numbers.

Consider the number

$$M = p_1 \times p_2 \times p_3 \times \dots \times p_n, \tag{37}$$

obtained by multiplying together all prime numbers on our list. Of course M itself is a composite number, since it is divisible by many numbers other than 1 and itself.

Although M is composite, the number $M + 1$ might not be. For starters, it is certainly not divisible by any of $p_1, p_2, \ldots p_n$. To see why this is, notice that dividing M by p_1 gives us $p_2 \times p_3 \times \ldots \times p_n$, and no remainder. If we add 1 to it, then after dividing by p_1 we have a remainder of 1, meaning that p_1 does not evenly divide $M + 1$; the same is true for all p_i on that list.

At this point we have a number $M + 1$ that is not divisible by any prime number in our set $\{p_1, p_2, \ldots, p_n\}$. This leaves us with two options: (a) $M + 1$ is divisible by some *other* prime number not in on that list. If that is the case, then $\{p_1, p_2, \ldots, p_n\}$ is certainly not a complete list of all prime numbers. (b) $M+1$ is not divisible by any other prime number. If that is the case, then $M+1$ itself must be a prime number! In either case, we find out that $\{p_1, p_2, \ldots, p_n\}$ is not a complete list of all prime numbers, showing us that it is not possible to have a complete finite list of all prime numbers. □

4.3 Finding Primes

Although we have proven that there are an infinite number of primes, we have not yet said anything about finding them. Is 101 a prime number? Is 17,213? We might also wonder about how many prime numbers are smaller than a million? What are those numbers? These are basic questions we would like to understand after learning about prime numbers and their infinitude.

To give some context for what we are trying to do, imagine that you were interested in finding multiples of 7. We could do that by starting with the number 7 and then adding 7 over and over. We would then easily determine that 7, 14, 21, 28, etc. are all multiples of 7. If someone would tell us that 91 were a multiple of 7, then we could just add another 7 and know that 98 is a multiple as well. Moreover, suppose we knew that a and b were both multiples of 7, then we know immediately that so is $a + b$! That is, we have simple methods of finding as many multiples of 7 as we'd like, given one or two initial multiples.

We might ask a similar question about prime numbers. Is there some way in which we could find as many prime numbers as we want? Suppose that p and q are both prime numbers, is there some way we could use p and q to find more prime numbers? Later in the semester we will learn about some applications for which finding large prime numbers is critical. Here we consider several approaches to finding prime numbers, some of which work successfully and others which do not. Even those that fail, however, can help us understand prime numbers in greater depth.

Trial and Error

Let us consider several possible ways of generating new prime numbers using ones we already know. Suppose we have two prime numbers p and q, is it possible that $p + q$ is also a prime? One example in which this works is if $p = 2$ and $q = 3$, since $p + q = 5$, and 5 is also a prime number. It also works when $p = 2$ and $q = 5$, since $p + q = 7$ is also a prime number. It would certainly be wrong, however, to make a generalization based on only two examples. If we use $p = 2$ and $q = 7$, for example, then we immediately see that this rule fails, since $p + q = 9$, which is not a prime number. The reader can quickly verify for him- or herself that although we can often generate new primes using this rule, there are also many cases in which it fails.

We might consider several additional "rules" for generating new primes from ones we know already. Here is one more suggestion – let us consider $p \times q + 2$, when we know that p and q are primes. We have $3 \times 5 + 2 = 17$, $3 \times 7 + 2 = 23$, and $5 \times 7 + 2 = 37$ – in which this "rule" works, but we also have $11 \times 13 + 2 = 145$ and $17 \times 19 + 2 = 325$, neither of which is a prime number.

These two suggestions highlight the importance of caution when attempting to derive general rules from particular examples. The following example provides another such example, this time where one of history's greatest mathematicians made a wrong guess.

Fermat Primes

The great 17th century French mathematician Pierre de Fermat considered prime numbers of the form $2^{(2^n)} + 1$, for natural numbers n. For $n = 1, 2, 3, 4$ we have:

$$\begin{aligned}
2^{(2^1)} + 1 &= 2^2 + 1 = 5 \\
2^{(2^2)} + 1 &= 2^4 + 1 = 17 \\
2^{(2^3)} + 1 &= 2^8 + 1 = 255 \\
2^{(2^4)} + 1 &= 2^{16} + 1 = 65537
\end{aligned}$$

Fermat conjectured that indeed for all natural numbers n the number $2^{(2^n)} + 1$ would be prime; such numbers are called **Fermat primes**. In part owing to his limited computing resources, Fermat did not carefully test whether or not $2^{(2^5)} + 1 = 4{,}294{,}967{,}297$ was prime or not. Had he done so, he would have known that his conjecture was false. Roughly a century after Fermat, the great Swiss mathematician Leonhard Euler showed that $2^{(2^5)} + 1$ could be factored as the product: $641 \times 6{,}700{,}417$, and hence not a prime number. Indeed, little else is known about Fermat primes, including whether there exist any more such primes. The Fermat primes is another example in which a pattern might continue for several cases but then stop, reminding us of the importance of proving statements rigorously, and not merely relying on intuition possibly gleaned by considering examples.

Euler Polynomials

Euler himself, one of the most prolific mathematicians of all time, suggested another way of generating prime numbers using a polynomial. For our purposes, we can think of polynomials as expressions that look like $5x^2 - 3x + 12$; polynomials with higher powers, and with more than one variable, are also possible. Euler suggested the polynomial

$$n^2 - n + 41, \tag{38}$$

which gives prime numbers for natural numbers $n = 1$ through $n = 40$. The first few primes that result from this equation are 41, 43, 47, 53, 61, and 71.

The fact that for the first 40 natural numbers we obtain a prime number might suggest that this pattern is true for all natural numbers. Indeed, if you were to conduct a scientific experiment to test a hypothesis, and the first 40 trials confirmed your hypothesis, you might conclude that indeed your hypothesis is correct, and that subsequent experiments should yield the same results. However, it is straightforward to see that if $n = 41$, then the given polynomial will result in a composite number, since $41^2 - 41 + 41 = 41^2$, which of course is not a prime number. These examples again illustrate the care that must be taken when generalizing from particular examples, both in mathematics and more generally.

Sieve of Eratosthenes

Of course it not practically possible to find *all* prime numbers, since we have already seen that there are an infinite number of them. However, suppose we wanted to find all prime numbers up to a certain number. What would be a good way to go about doing that? For any given natural number, of course we could just attempt to divide it by all smaller natural numbers. For example, if we wanted to know whether 43 was prime or composite, we could try dividing it by 2, then by 3, then by 4, then by 5, and so on. In this particular case, we will eventually reach 42 and realize that 43 is indeed not divisible by any natural numbers aside from 1 and 43 itself, making it a prime. However, if we wanted to find all prime numbers less than 100, this process would take a very long time.

The ancient Greek mathematician, poet, and scientist Eratosthenes (third century BCE) suggested a relatively efficient method of determining all prime numbers up to a certain number. Eratosthenes was a chief librarian in the famous Library of Alexandria, and made scholarly contributions to several fields. Among his other contributions, he is known for having been the first person to calculate the circumference of the Earth.

To find all prime numbers up to a certain number, Eratosthenes developed what later became known as the Sieve of Eratosthenes. To help illustrate his method, we consider how we might find all prime numbers up to 50. For our purposes, we ignore the number 1, for a reason that will become momentarily clear. We begin by circling 2 and then crossing off all subsequent numbers that are multiples of 2. We then find the next smallest number that is not crossed out, which in the case is 3. Since 3 is not crossed out, it must not be a multiple

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

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

of any number smaller than it (besides 1), so it is by definition a prime number. We circle 3 and cross out all multiples of it. We continue this process circling the first number not yet crossed out and crossing out all multiples of it. This allows us to determine all primes up to a certain number, without needing to check each number individually. This method of finding primes is called the sieve of Eratosthenes, because of the way in which we begin with many numbers and sift many away, leaving only the primes.

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

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

How many primes?

Although we have seen that there are an infinite number of prime numbers, we might wonder how many primes are there up to a certain number. For example, how many prime numbers are there that are smaller than 100? or a 1000? or a million? or 10^{23}? To help understand how the number of prime numbers grow as we go up with the numbers, Figure 3 plots the number of primes up to N for a range of N. Notice that the slope of the curve decreases with increasing N; roughly speaking this can be understood to mean that as we proceed further along the number line, the "average number" of primes decreases, and finding primes becomes increasingly more difficult. One of the great achievements of 19th century number theory was proving what is called the **prime number theorem**. This theorem, proven separately by the French mathematician Jacques Hadamard and the Belgian mathematician Charles de la Valle-Poussin, states that the number of primes up to a certain number N is "roughly" equal to $N/\log N$. Although we will not explore this theorem in depth, we mention it because of its importance and centrality in the study of prime numbers.

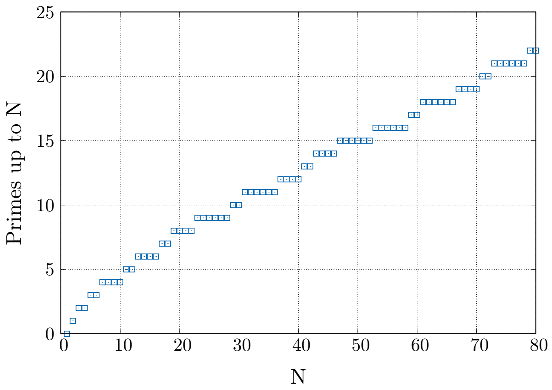


Figure 3: A graph of the number of prime numbers up to N for various N.

4.4 Fundamental Theorem of Arithmetic

One of the central results in the study of natural numbers is called the Fundamental Theorem of Arithmetic. In some sense, this theorem states that prime numbers serve as the atomic building-blocks of all natural numbers. Much in the way that we can think of complex molecules as being composed of constituent atomic elements, so too we can think about natural numbers as being composed of constituent prime numbers. Water is composed of two hydrogen atoms and one oxygen atom, and the number 12 is composed of two 2's and one 3, all multiplied together.

Breaking Numbers Apart

Let's consider how we can "break down" natural numbers into smaller pieces. Consider the number 18. We can break this down into smaller numbers by writing it as 2×9 or 3×6. You might notice that in both cases, one of the two numbers is prime, whereas the other is composite. We can also write 18 as the product $2 \times 3 \times 3$, that is, of three prime numbers. These are various ways in which we can decompose 18 into smaller constituent pieces. We can conclude that there is no unique way in which we can break a number down into smaller numbers. However, we should point out that in only one of these three ways were all smaller numbers prime.

This exercise raises two important questions. **Question 1:** Can every natural number be broken down into smaller numbers all of which are prime? **Question 2:** For numbers that can be broken down, in how many ways can we do that? Notice that we broke down 18 in two different ways when we used composite numbers, namely as 2×9 and as 3×6. However, we only showed one way in which we can break 18 down if we considered only prime numbers. Is it possible to break 18 down another way using only primes? The Fundamental Theorem of Arithmetic addresses both of these questions.

Theorem 5 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than 1 is either a prime number, or else a product of prime factors, and this product is unique up to the ordering of the prime factors.*

This statement makes two claims about prime-factor decompositions, one about their *existence* and one about their *uniqueness*. First, for every integer $n > 1$ there **exists** at least one way of writing n as a product of one or more primes. For example, 35 can be written as a product of prime numbers, $35 = 5 \times 7$. The number 42 is also composite, and can be written $42 = 2 \times 3 \times 7$. The number 43 is itself prime and can be thought of as the product of one prime number, itself. Note that the theorem does not require that all the prime factors be unique. For example, $72 = 2 \times 2 \times 2 \times 3 \times 3$ and $27 = 3 \times 3 \times 3$.

The second part of the theorem states that there is *at most one* way to break up a number into primes, i.e., the prime-factor decomposition is **unique**. For example, since $35 = 5 \times 7$, and since 5 and 7 are both prime numbers, then there are no other primes $p_1, p_2, \ldots, p_n$ such that $35 = p_1 \times p_2 \times \ldots \times p_n$. There is at most one way in which we can write any natural number greater than 1 as a product of prime numbers. As a second example, consider the number 374,699, which can be written as the product $13 \times 19 \times 37 \times 41$. The consequence of the second part of the theorem is that there are no other set of prime numbers whose product is 374,699.

In contrast to prime decompositions, consider what happens when we break up a number into composite numbers. When we do this we have no guarantee of uniqueness. For example, consider the number 48. We can write

$$4 \times 12 = 48 = 3 \times 16. \tag{39}$$

We have two distinct factorizations; these are possible because the factors 4, 12, and 16 are not prime numbers.

Finally, when we say "unique", we mean unique up to rearrangements of the prime factors. Since $a \times b = b \times a$ for any integers a and b, we do not count different orderings of the same primes as different decompositions. For example, we can write

$$2 \times 2 \times 2 \times 5 \times 5 \times 5 = 1000 = 2 \times 5 \times 2 \times 5 \times 2 \times 5. \tag{40}$$

These two prime factorizations are unique if we ignore the way in which we order the primes.

Divisibility

A basic concept that arises in studying numbers, especially in studying prime and composite numbers, is that of divisibility. The numbers 18 and 24 can be "evenly divided" by 2 and 3, but not by 5 or 7. The following definition makes this idea precise.

Definition 12. *We say that a* **divides** *b if there exists some integer $k \in \mathbb{Z}$ such that $b = k \times a$. We write $a|b$ to indicate that a divides b; we write $a \nmid b$ if a does not divide b.*

This notation is probably unfamiliar to most readers; its purpose is to make precise what we mean by saying that a number a is a divisor of b, and to simplify statements such as "5 goes evenly into 100". We mean the same thing by saying a divides b or a is a divisor of b.

Example 1. It is the case that $3|15$ and $5|15$, but it is not the case that $3|5$ or $15|3$; we can write $3 \nmid 5$, $15 \nmid 3$, and $5 \nmid 3$.

Example 2. Negative numbers can also be considered. For example, we have $-3|15$ because there exists an integer k (in this case $k = -5$) such that $15 = k \times -3$.

Example 3. For every integer $a \in \mathbb{Z}$, we have $a|a$, since $1 \times a = a$.

Example 4. For every integer $a \in \mathbb{Z}$, we have $1|a$, since $a \times 1 = a$.

Example 5. For every integer $a \in \mathbb{Z}$, we have $1|a$ and $-a|a$. The divisors 1, -1, a and $-a$ are sometimes called trivial divisors, because without knowing anything about a we can know that they are among its divisors.

Example 6. For every integer $a \in \mathbb{Z}$, we have $a|0$, since $0 \times a = 0$. It might sound strange to say something like 7 goes evenly into 0, but in the sense of Definition 12, we can say that 7 is a divisor of 0. In this sense 0 *is* a multiple of any integer a.

Example 7. Since for any $a \neq 0$, there is no integer k such that $k \times 0 = a$, we have $0 \nmid a$ for all non-zero integers a. If $a = 0$, then we can have $0|a$, since for any integer k we have $k \times 0 = 0$.

Euclid's Lemma

To prove the Fundamental Theorem of Arithmetic we will need what is called Euclid's Lemma, a theorem about prime divisors of a product of numbers.

Lemma 6 (Euclid's Lemma)**.** *For a prime number p and natural numbers a and b, if $p|a \times b$ then either $p|a$ or $p|b$.*

That is, if a prime p divides $a \times b$, then it must divide either a or b (or both). For example, if we know that 7 divides $462 = 14 \times 33$, then it must divide either 14 or 33; in this case $7|14$. Likewise if we know that $17|1{,}790{,}219$, and we know that $1{,}790{,}219 = 1333 \times 1343$, then 17, which is prime, must divide either 1333 or 1343. We will not prove Euclid's Lemma here.

It is important to understand that this lemma only holds when p is a prime number. If p is composite, however, then even though it divides $a \times b$, there is no guarantee that it divides either a or b. For example, consider $36 = 4 \times 9$. Although 6 divides 36, it does not divide either 4 or 9. Euclid's Lemma makes claims only about prime numbers that divide products $a \times b$.

Although Euclid's Lemma is usually stated for products of the form $a \times b$, it is also true for products $a \times b \times c \times \ldots$ with any finite number of multiplying terms. For example, if we know that $13|29{,}938{,}870$, and we know that $29{,}938{,}870 = 190 \times 221 \times 713$, then we know that 13 must divide either 190, 221, or 713.

Existence of Prime Factorizations

Here we prove the first part of the Fundamental Theorem of Arithmetic – that every integer greater than 1 is the product of one or more primes. To do this, we first consider a hypothetical number that is not the product of one or more primes and then show that such a number cannot exist. In particular, let's consider the smallest integer greater than 1 that *cannot* be written as the product of one or more primes; we call that number N. Since N is not a prime, then it is a composite, which means that there exist two integers $a, b > 1$ such that $N = a \times b$. Since we defined N to be the smallest integer that cannot be written as a product of primes, and since a and b are both smaller than N, it must be that both of them *can* be written as products of primes. For example, we might have:

$$a = q_1 \times q_2 \times \ldots \times q_m \tag{41}$$

$$b = r_1 \times r_2 \times \ldots \times r_n, \tag{42}$$

where all of the q's and r's are prime numbers. Since $N = a \times b$, then we also have $N = a \times b = q_1 \times q_2 \times \ldots \times q_m \times r_1 \times r_2 \times \ldots \times r_n$. But this shows that N can, in fact, be written as a product of primes! If a smallest number that cannot be written as the product of primes cannot exist, then there cannot exist any such numbers. Instead, any number greater than 1 *can* indeed be written as the product of primes.

Although we now know that every natural number (greater than 1) can be written as a product of prime numbers, we don't yet know in how many ways this can be done. Of course we know that $15 = 3 \times 5$ can only be written in one way, but perhaps there exist some larger natural number that can be written in several ways as the product of prime numbers. The next proof shows that the prime factorization of a number is indeed unique, and hence there is only one way to write a number as the product of primes.

Uniqueness of Prime Factorizations

The second part of the Fundamental Theorem of Arithmetic states that there is *at most one* way to write every integer greater as a product of primes. Proving this uniqueness of prime factorization runs along similar lines as the proof of existence of prime factorizations. We will consider a number that can be written in several ways, and show that such a number cannot exist. In particular, let us consider the smallest natural number that can be written as a product of primes in at least two distinct ways. If we call that number N, then we can write it in two different ways:

$$N = q_1 \times q_2 \times \ldots \times q_m \tag{43}$$

$$= r_1 \times r_2 \times \ldots \times r_n, \tag{44}$$

where all of the q's and all of the r's are primes; note that m and n need not be the same. If any q were identical to any r, then we could divide N by that number to obtain a smaller integer written in two different ways. For example, suppose that $q_2 = r_1$, we could then divide N by that number to obtain:

$$\begin{aligned} N/q_2 &= q_1 \times q_3 \times \ldots \times q_m & (45) \\ &= r_2 \times r_3 \times \ldots \times r_n. & (46) \end{aligned}$$

This number, $N/q_2 = N/r_1$, would then be a natural number smaller than N that can be written in at least two different ways, but by its definition N is the smallest such number. If there exists a smallest such number, then it must be that $q_2 \neq r_1$, and likewise that none of the p's are identical to any of the q's.

So far we have shown that if there exists a smallest number N that can be written as a product of primes in two different ways, then all primes in the first factorization must be distinct from all primes in the second factorization. We now use Euclid's lemma to show that we can not have two such factorizations.

Let's consider q_1, a prime factor of N. Since $q_1|N$ and since $N = r_1 \times r_2 \times \ldots \times r_n$, then by Euclid's Lemma, q_1 must divide at least one of the r's. However, since the r's are all prime numbers, then since q_1 divides one of the r's, it must be identical to it. In other words, we have shown that if there exists a smallest number N that can be factorized in two different ways (using primes p's and q's), then at least one of the primes must be the same as one of the q's.

The problem is that we have already shown that all q's must be distinct from all r's. This contradiction shows that there is no smallest natural number that can be written as a product of primes in two distinct ways. If there is no smallest such natural number, then there cannot exist any such natural number.