3 Number Theory

Number theory is celebrated by mathematicians as a pure form of abstract thought, a distillation of reason. Carl Friedrich Gauss called it the "queen of mathematics," while G. H. Hardy, in *A Mathematician's Apology*, admired its pure, abstract isolation, praising the fact that it was unencumbered by the physical world, without use or application.

And yet, despite this, in a strange and surprising twist of fate, the theory has in contemporary times found key practical applications; deep number-theoretic ideas, for example, lie at the core of cryptography and internet security. Our dreamy iridescent theory of numbers, it turns out, supposedly without use or application, does in fact have important applications, vital for commerce and communication, so much so that number-theoretic ideas are now firmly established via cryptography in the foundations of our economy.

3.1 Prime numbers

Let us develop some elementary number theory, beginning with the prime numbers. What is a prime number? At this question, I imagine, perhaps a nervous laugh goes through the classroom—of course we are all familiar with prime numbers, right? A helpful student suggests, tentatively, that a number is prime if the only divisors of the number are 1 and itself. Is this a good definition? Let us quibble. One minor issue is that numbers can have negative divisors. We want 3 to be prime, to be sure, but does the factorization $3 = (-3) \cdot (-1)$ mean that it has -3 and -1 also as divisors? Let us therefore interpret the student's proposal to refer only to *positive* divisors. Similarly, we do not want $\frac{7}{2} \cdot 2$ to rule out 7 as prime, and so we should interpret the student's proposal as referring only to positive *integer* divisors.

A more serious issue, however, is the question of whether the number 1 should count as prime. Is 1 prime? Since 1 has no positive integer divisors other than 1 and itself, it would seem that, according to the student's proposal, we would say that, indeed, 1 is prime. Nevertheless, this would go against the advice of many mathematicians, who have come to the conclusion that we do not actually want to include 1 amongst the prime numbers. On this view, the student's suggestion is not quite exactly right.

I should like to emphasize that, as mathematicians, we are free to define our terms to mean whatever we want. We could define our notion of prime number so that 1 turns out to be prime, or we could have defined the notion differently, so that 1 would not count as prime. There is no issue here of *discovering* whether or not the number 1 is prime; we can define our technical terms as we wish. Rather, what is at stake here is what we want the word *prime* to mean and whether we want to use this word in a way that makes the number 1 prime or makes it not prime.

All things considered, mathematicians have concluded that it is more convenient in many contexts if we say that 1 is *not* prime. To give one example, if the number 1 counted as prime, then it would no longer be true that every positive integer had a unique prime factorization, as in $12 = 3 \cdot 2^2$, since we could always add more 1s the factorization, like this: $12 = 3 \cdot 2^2 \cdot 1 \cdot 1 \cdot 1$. If 1 counted as prime, we would find ourselves often having to add exceptions to many theorems about prime numbers, to say in effect, "except for 1." Ultimately, it is more convenient simply to say that 1 does not count as prime. So let us make our official definition as follows:

Definition 7. An integer p is *prime* if $p > 1$ and the only positive integer divisors of p are 1 and p.

Students of abstract algebra might recognize that this definition is actually not concerned with primality but with *irreducibility*. Specifically, in the algebraic structures known as rings, an element is defined to be irreducible if it admits no nontrivial factorization, as in the definition above. An element p of a ring is *prime*, in contrast, if it is nonzero, it has no multiplicative inverse, and whenever p divides a product ab, then either p divides a or p divides b. Although in the class of rings known as integral domains every prime element is irreducible, the converse is not always true, and many rings and integral domains have irreducible elements that are not prime. Nevertheless, it will follow from lemma 13 below that in the positive integers the prime numbers are the same as the irreducible numbers, and so it will be fine for us to stick with the traditional definition above as our official definition of what it means to be prime.

3.2 The fundamental theorem of arithmetic

The reader has likely had experience factoring numbers as a product of prime numbers. Twelve factors as $12 = 3 \cdot 2^2$, and the number 8470 can be factored first as the product $10 \cdot 847$, and then further broken into primes as $2 \cdot 5 \cdot 7 \cdot 11 \cdot 11$. Let me ask an innocent question:

Question 8. For a given number, will we always get the same prime factorization?

Of course, I mean the *same* here in the sense that $3^2 \cdot 5 \cdot 7$ counts as the same factorization as $5 \cdot 3 \cdot 7 \cdot 3$—we have simply rearranged the same prime factors. Are prime factorizations always unique in this sense? Perhaps. Can we imagine that, for extremely large numbers,

the outcome of the prime factorization might depend on how we had proceeded to compute it? Perhaps. If we had started with a slightly different product at the first step, might we have found ourselves ultimately with a different prime factorization in the end?

The number 11543, for example, can be factored as $7 \cdot 17 \cdot 97$, and these factors are each prime. Do we know that there is not also some other way to factor it into primes? For a comparatively small number like this, we might hope to try out all the other candidates and be convinced this way. That method is actually impractical, even for numbers such as 11543, and for much larger numbers like 653465345453435463456534655534354652, it is downright infeasible. Do we actually know that this number has a unique prime factorization?

When factoring numbers, to be sure, we routinely refer to *the* prime factorization. But perhaps we should be saying merely that we have *a* prime factorization? Can there be more than one? On my view, this is a serious question, more difficult than it might initially appear. The fact of the matter is that the usual naive treatment of prime factorization simply does not touch on the question of uniqueness. We have become familiar with the uniqueness of prime factorizations largely by observing many instances of prime factorization, without ever encountering a situation where a number admits more than one factorization. Does this experience constitute proof? No, of course not.

Meanwhile, prime factorizations are indeed unique, and this fact is the first deep theorem of number theory, known as the fundamental theorem of arithmetic:

Theorem 9 (Fundamental theorem of arithmetic). *Every positive integer can be expressed as a product of primes, and furthermore, this factorization is unique up to a rearrangement of these prime factors.*

We shall prove this theorem presently, but before doing so, let me remark on a certain issue arising in the statement of this theorem and a habit that mathematicians have. Namely, the theorem says that every positive integer is a product of primes; but is this right? What about the number 5? Yes, it is prime, but is it a *product* of primes?

Mathematicians will say yes, 5 is a product of primes, a product consisting of just one factor, the number 5 itself. You might reply, that is not a product at all! Should not the theorem say, "Every positive integer is either prime or a product of primes"? Mathematicians will insist, nevertheless, that it is a good idea to consider 5 and the other prime numbers as products of primes, degenerate products if you will, products consisting of just one factor. The reason is that our mathematical theories often become more robust when we incorporate the trivial or degenerate instances of a phenomenon into the fundamental definitions. Every square counts also as a rectangle; every equilateral triangle is also isosceles. This practice often leads to a smoother mathematical analysis in the end. A rectangle is precisely a quadrilateral with four right angles, for example, but this would not be true if we did not count squares also as rectangles. In the same way, we allow ourselves to refer to the product of just one number, without being multiplied by any other number.

One sometimes hears that 5^n means that we multiply 5 by itself n times. This is not really accurate, however, if what is meant is that we have n multiplications, since 5^2 means 5×5, which is only one act of multiplication; we would be more correct, therefore, to say that n refers to the number of factors, rather than to the number of times we are multiplying. This is a *fence-post* error, discussed further in chapter 5. So we regard 5^1 as a product consisting of just one factor. Similarly, we take $5^0 = 1$ as a product with no factors at all, the empty product. This is the sense in which 1 is a "product" of prime numbers.

The thing to notice here is that, even if we had stated the theorem as, "Every positive integer is either prime or a product of primes," it still would not be correct without this empty product convention, since the number 1 is a positive integer, but it cannot be expressed as a product of primes except as the empty product. Without the empty and singleton product considerations, therefore, we would have to say, "Every integer greater than 1 is either prime or a product of primes." But is it not both simpler and more elegant to state the theorem as we have in theorem 9? We have included the primes themselves each as a product with only one factor and the number 1 as the empty product.

So let us now prove the fundamental theorem, which makes two essentially different claims: an existence claim and a uniqueness claim. Namely, the existence claim is that every positive integer admits at least one prime factorization, and the uniqueness claim is that every number admits at most one prime factorization, in the sense that any two factorizations of the same number are rearrangements of one another. Let us begin with the existence claim, since this is perhaps more familiar, as well as easier to prove.

Theorem 10 (Fundamental theorem, existence). *Every positive integer can be expressed as a product of prime numbers.*

Proof. Let us prove that every positive integer has the property. The number 1 is expressed as the empty product, and so we have made a start. Suppose that all the numbers up to some number n have the property, where $n > 1$, and now consider whether n itself has the property. If n happens to be prime, then indeed, it is expressible as a product of just one prime factor, itself, and so it would have the property. Otherwise, n is not prime, and so we may factor it as $n = ab$ for some numbers a and b, both smaller than n. Because we assumed that the property holds up to n, we know that both a and b are expressible as products of primes. So $a = p_1 \cdots p_k$ and $b = q_1 \cdots q_r$ for primes p_i and q_j, where $1 \leq i \leq k$ and $1 \leq j \leq r$. By simply combining these products, we can now realize n also as a product of primes:

$$n = ab = p_1 \cdots p_k \cdot q_1 \cdots q_r.$$

So the property does indeed hold at n. We have therefore proved that whenever the property holds up to a number n, then it holds at the number n. In other words, there can be no minimal counterexample to the property; thus, there can be no counterexample at all. So every number has the property. □

We used the method of *minimal counterexamples*, by which one shows that a property holds of all positive integers by showing that there can be no smallest counterexample to the property, and hence no counterexample at all. This method is closely related to (and essentially identical to) the method of *mathematical induction*, which we shall explore more fully in chapter 4.

Some mathematicians may have preferred to cover the method of induction before proving the fundamental theorem of arithmetic, but my preference was to mount these simple minimal-counterexample arguments in this chapter, using them in part as an introduction to inductive reasoning. In chapter 4, we shall give a more thorough general account of the theory of mathematical induction.

3.3 Euclidean division algorithm

In order to prove the uniqueness part of the fundamental theorem of arithmetic, we shall rely on some classic elementary number theory, which we now develop. Let us begin with the familiar fundamental principle that we can always divide integers, possibly with remainder, in such a way that the remainder is less than the number by which we are dividing. This fact is known as the Euclidean division algorithm. This terminology, quite old and firmly established, perhaps conflates the mathematical fact that the quotient and remainder exist with the algorithms or procedures that one might use to find them.

Lemma 11 (Euclidean division algorithm). *For any two positive integers n and d, there are unique integers q and r for which $n = qd + r$ and $0 \leq r < d$.*

Note how we have chosen variable names so as to aid our understanding, since the lemma is fundamentally concerned with the operation of dividing n by d, so n stands for *numerator*, d for *denominator* or *divisor*, q for *quotient*, and r for *remainder*.

Proof. To prove uniqueness, suppose that $qd + r = q'd + r'$, where $0 \leq r, r' < d$. It follows that $r - r' = (q' - q)d$, and so $r - r'$ is a multiple of d. Since also $r - r' < d$, it follows that $r - r' = 0$ and so $r = r'$, which implies $q = q'$. So the representation is unique when it exists. For existence, we shall prove that there can be no smallest failing instance of the lemma. Specifically, we shall prove that if the lemma holds up to a number n, then it also holds at n. So suppose that n and d are numbers and that the statement of the lemma holds with d and any number smaller than n. If $n < d$, then we can write $n = 0 \cdot d + n$, and this fulfills the requirement that $0 \leq r < d$. Similarly, if $n = d$, then we may write $n = 1 \cdot d + 0$, which also verifies the desired property. So we may assume that $d < n$. In this case, $n - d$ is a positive integer smaller than n. By the assumption on n, the lemma holds for d and $n - d$, and so there are numbers q and r with $n - d = qd + r$ and $0 \leq r < d$. By adding d to both sides, we see that $n = (q + 1)d + r$, which fulfills the desired statement for n and d. So there can be no minimal counterexample to the lemma, and consequently, there can be no counterexample at all. So the lemma holds for all n and d. □

Next, we prove Bézout's identity. Recall from chapter 1 that integers are *relatively prime* if they have no common factor larger than 1.

Lemma 12 (Bézout's identity). *If integers a and b are relatively prime, then there are integers x and y for which $1 = ax + by$.*

Proof. Assume that integers a and b are relatively prime. Let d be the smallest positive integer that is expressible as an *integer linear combination* of a and b, that is, as $d = ax+by$ for some choice of integers x and y. Certainly $d \leq a$, since we can write $a = a \cdot 1 + b \cdot 0$. I claim that d divides both a and b. To see this, apply the Euclidean algorithm to express $a = kd + r$ for some integer k and remainder r, with $0 \leq r < d$.

Putting our equations together, observe that

$$r = a - kd = a - k(ax + by) = (1 - kx)a + (-ky)b.$$

We have therefore expressed r as an integer linear combination of a and b. Since $r < d$ and d was the smallest positive such combination, it follows that r must be 0. In other words, $a = kd$ is a multiple of d, as claimed. A similar argument shows that b also is a multiple of d, and so d is a common factor of a and b. Since these numbers are relatively prime, it must be that $d = 1$, and so we have achieved $1 = ax + by$, as desired. □

Lemma 13 (Euclid's lemma). *If p is prime and p divides ab in the integers, then p divides a or p divides b.*

Proof. Assume that p is prime and that p divides ab. If p does not divide a, then a and p must be relatively prime, since there are no other nontrivial factors of p. By Bézout's lemma (lemma 12), it follows that $1 = ax + py$ for some integers x and y. Multiplying both sides by b, we see that

$$b = abx + pby.$$

Since p divides ab, it follows that p divides the right-hand side of this equation, and so p divides b. So we have proved that if p does not divide a, then it divides b. And so p must divide one of them. □

We can generalize lemma 13 to the situation of many primes:

Lemma 14. *If a prime p divides a product of integers $n_1 n_2 \cdots n_k$, then p divides some n_i.*

Proof. We know by lemma 13 that this lemma is true when there are only two factors. Suppose that this lemma holds when there are fewer than k factors, and that we have a prime number p that divides a product $n_1 \cdot n_2 \cdots n_k$ with k factors. The trick is to look upon the product $n_1 n_2 \cdots n_k$ as a product of just two things, like this: $n_1 \cdot (n_2 \cdots n_k)$. Since p divides this product of two things, we may conclude by lemma 13 that either p divides n_1 or p divides the rest of the product $n_2 \cdots n_k$. In the first case, we are done immediately, and

in the second case, since there are now fewer than k factors in the product, we conclude by our assumption on k that p must divide one of the n_i for $2 \leq i \leq k$. So in any case, p divides some n_i, and the lemma is proved. □

3.4 Fundamental theorem of arithmetic, uniqueness

Finally, we can prove the uniqueness part of the fundamental theorem of arithmetic.

Theorem 15 (Fundamental theorem, uniqueness). *Every positive integer has at most one prime factorization, in the sense that any two factorizations are simply rearranging the order of the prime factors appearing in them.*

Proof. We have already proved the existence claim in theorem 10. What remains is the uniqueness claim. Suppose that all the numbers smaller than a number n have at most one representation as a product of primes (unique up to rearranging the order in which the prime factors appear in the product). Suppose that $n = p_1 \cdots p_k = q_1 \cdots q_r$ are two representations of n as a product of primes. Since p_1 divides n, it follows by lemma 14 that p_1 must divide one of the q_j, and since these are all prime, it must be equal to one of the q_j. It might as well be q_1, by rearranging the qs. But in this case, we have $p_2 \cdots p_k = q_2 \cdots q_r$, since these are both n/p_1, and by our assumption on n, these two products are a simple rearrangement of each other. So the original products also are obtained by rearranging, and we are done. □

The fundamental theorem of arithmetic (theorem 9) amounts to the combination of the existence claim of theorem 10 and the uniqueness claim of theorem 15, so it is now proved.

3.5 Infinitely many primes

Let us turn now to another classical result, the fact that there are infinitely many primes. This is a classic argument, often attributed to Euclid, known for thousands of years.

Theorem 16. *There are infinitely many prime numbers.*

Proof. Suppose that you have a list of finitely many prime numbers:

$$p_1, p_2, \ldots, p_n.$$

Let $N = (p_1 p_2 \cdots p_n) + 1$, the result of multiplying them together and adding 1. Observe that if you should divide N by any particular prime number p_i on your list, then there will be a remainder of 1. In particular, this number N is not divisible by any prime number on your list. But N is a product of primes, as every natural number is, and so there must be a prime that is not on the list. Thus, no finite list of numbers includes all the primes, and so there must be infinitely many of them. □