2 Prime Numbers

2.1 Primes and factorizations

For further reading on the material in this subsection, consult **Rosen 3.1; PMF 3.2, Stein 1.1.1, 1.1.3**.

We've talked about relatively prime–when a number shares no divisors with another number. Is it possible to have a number that is absolutely prime–it has no common divisors with any number?

Well, not really. After all, a number has common divisors with itself. And it has common divisors with any of its multiples. But we can *almost* make this work.

Definition 2.1. A natural number $n > 1$ is *prime* if it is not divisible by any natural numbers other than 1 and itself.

A natural number $n > 1$ that is not prime is *composite*.

Example 2.2. $2, 3, 5, 11, 97, 127$ are all prime.

$4, 8, 57, 91, 255$ are all composite.

Remark 2.3. 1 is neither prime nor composite, by definition. During this course we will see how this continually makes definitions and theorems simpler to state.

Remark 2.4. It's perfectly reasonable to talk about negative numbers being prime or composite; in this context -2 and -3 would be prime, -4 composite, and -1 neither (technically, a "unit"). However, none of our references do so. We will mostly restrict ourselves to positive integers, but on occasion may (perhaps inadvertently) abuse our terminology to discuss negative primes.

Exercise 2.5. *Let p be a prime and n and integer such that p does not divide n. Prove that* $\gcd(p, n) = 1$.

We said on the first day that a major theme of this course will be understanding the distribution of the prime numbers. We will finish this section by proving that there are infinitely many prime numbers, which is the first major result on this subject.

Lemma 2.6. *Every integer greater than 1 can be written as a product of primes.*

This is a very important theorem (and in fact is half of the Fundamental Theorem of Arithmetic, which we will discuss later in this section). We can prove this either using the well-ordering property, or using strong induction. Since these are both important techniques, I will present both proofs.

Proof by well-ordering. Suppose (for contradiction) that there is an integer greater than 1 with no prime factors. Then the set of all such integers must have a least element, by the well-ordering property. So let n be the smallest integer > 1 that cannot be written as a product of primes.

If n is prime, then it can be written as a product of 1 prime; thus n must be composite. Thus it must have some other divisor, and we can write $n = ab$ with $1 < a, b < n$.

Since $1 < a, b < n$ and n is the smallest integer that cannot be written as a product of primes, we know that a and b can both be written as products of primes. Since $n = ab$ we can write n as a product of primes, yielding a contradiction. □

Proof by induction. Let $n > 1$ be a number, and suppose the lemma holds for every $k < n$. We consider two cases:

Suppose n is prime. Then n can be written as a product of one prime, n.

Now suppose $n > 1$ is not prime. Then n is composite, and we can write $n = ab$ for $1 < a, b < n$. Then by our inductive hypothesis, a and b can both be written as a product of primes, since $1 < a, b < n$.

But $n = ab$ and a and b can be written as a product of primes, so n can also be written as a product of primes.

Question for the reader: where is the base case here? □

Remark 2.7. This is stronger than Lemma 3.1 in Rosen. It is proved later, after Lemma 3.5 in Rosen, instead. But 3.1 is a clear corollary of this lemma, and the proofs are essentially the same.

Theorem 2.8 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose there are only finitely many primes; call them $p_1, \dots, p_n$. Consider the number

$$Q_n = p_1 p_2 \dots p_n + 1 = \prod_{k=1}^{n} p_k + 1.$$

By the previous lemma 2.6 we know that Q_n can be written as a product of primes, and in particular has at least one prime factor q.

Suppose $q = p_j$ for some p_j in our finite list of primes. We know that

$$Q_n - p_1 \dots p_n = 1$$

and q divides both Q_n and $p_1 \dots p_n$ (the first by hypothesis; the second because $q = p_j$. Then by lemma 1.13 on linear combinations we see that q divides 1.

But no prime divides 1, so this is a contradiction. Thus there must be infinitely primes.

Question: where did we use the assumption that the set of primes is finite? □

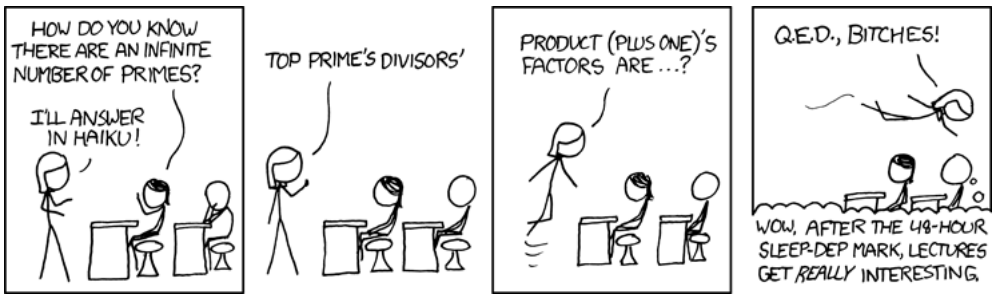

Figure 2.1: `http://xkcd.com/622`

Remark 2.9. If we have some finite list of primes $p_1, \ldots, p_n$, we do not know that $p_1 \ldots p_n + 1$ is prime. We just know that there is some prime that was not on our list.

For instance, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 * 509$.

2.2 The Fundamental Theorem of Arithmetic

For further reading on the material in this subsection, consult **Rosen 3.5, PMF 6.1–6.2, Stein 1.1.4**.

In the previous section we showed that every natural number greater than 1 can be written as a product of primes. Further, if we allow "empty products" with zero factors, then 1 is also a product of primes; and it's clear that if we allow multiplication by ± 1 we have a prime factorization of any non-zero integer.

However, if we wish to reliably decompose integers into their prime factorizations, we would like to get the same factorization every time. Thus we would like to show that there is only one possible prime factorization of any given number.

There is one roadblock we need to be careful of. We can factor $6 = 2 \cdot 3$ or $6 = 3 \cdot 2$. We can write $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$. So these numbers have two or three "different" factorizations. But we intuitively want to treat these as the same, "up to order."

Conveniently, working in the integers we can use the natural total order to remove any ambiguity.

Theorem 2.10 (Fundamental Theorem of Arithmetic)**.** *Every natural number can be written uniquely as a product of primes in non-decreasing order.*

We can write this theorem in a more general and precise form.

Theorem 2.11 (Fundamental Theorem of Arithmetic, General Form)**.** *Every non-zero integer can be written uniquely as a product*

$$n = \pm p_1^{e_1} \dots p_n^{e_n}$$

for some primes p_i with $p_i < p_{i+1}$, and $e_i \in \mathbb{N}$.

In order to prove this theorem we will first need a couple of lemmas.

Lemma 2.12 (Euclid's Lemma)**.** *Suppose a, b, c are integers such that $(a, b) = 1$ and $a|bc$. Then $a|c$.*

Proof. Because $(a, b) = 1$, there are integers m, n such that $ma + nb = 1$. Multiplying by c gives the equation $mac + nbc = c$. Then a divides mac (clearly) and divides nbc since it divides bc; by Lemma 1.13 on linear combinations we see that a divides $mac + nbc = c$. □

Lemma 2.13. *Let p be a prime number and let a, b be integers. If $p|ab$ then $p|a$ or $p|b$.*

Proof. Suppose $p|ab$. If $p|a$ we're done, so we will suppose $p \not| a$ and prove that $p|b$.

Since p is prime, $(p, a) = 1$ by exercise 2.5. Then by Euclid's Lemma 2.12, we know that $p|b$.

□

Exercise 2.14 ($\star$)**.** *Let $a_1, \dots, a_n$ be integers, and let p be a prime. Prove that if $p|a_1 \dots a_n = \prod_{i=1}^{n} a_i$, then $p|a_i$ for some i.*

Remark 2.15. We can actually take the property in Lemma 2.13 as the definition of a prime number. In the integers the two concepts are the same; in larger collections of numbers this is not the case.

In algebraic number theory, this divisibility property becomes the definition of a "prime", and our original definition becomes the definition of an "irreducible."

Exercise 2.16. *Let $p > 1$ be an integer with the following property: whenever a, b are integers and $p|ab$, then $p|a$ or $p|b$. Prove that p is prime.*

We are now ready to prove the Fundamental Theorem. We will prove the simpler version; the more general version is an obvious extension.

Proof of the Fundamental Theorem of Arithmetic. Let $n > 1$ be a natural number. In Lemma 2.6 we showed that n can be written as a product of primes, so we only need to show that any factorization is unique.

Suppose n can be written as a product of nondecreasing primes in two different ways; that is, suppose

$$n = p_1 \dots p_s = q_1 \dots q_t$$

with p_i, q_i prime, and $p_i \leq p_{i+1}, q_i \leq q_{i+1}$. (We cannot guarantee $p_i < p_{i+1}$ since some numbers have repeated factors; for instance we would write $36 = 2 \cdot 2 \cdot 3 \cdot 3$.)

We may divide through by all the common factors in the two lists, and get an equation

$$p_{i_1} \dots p_{i_e} = q_{j_1} \dots q_{j_f}$$

which still holds, and has no prime present on both sides of the equation. But then we have

$$p_{i_1} | q_{j_1} \dots q_{j_f}$$

and by Exercise 2.14 we see that $p_{i_1} | q_{j_k}$ for some k. Since q_{j_k} is prime, it is divisible only by 1 and itself; since $p_{i_1} \neq 1$, we must have $p_{i_q} = q_{j_k}$, which is a contradiction.

Thus we cannot have two distinct such prime factorizations, and the prime factorization must be unique. □

2.3 Where are the primes?

For further reading on the material in this subsection, consult **Rosen 3.1-2, PMF 3.3**.

We've now proven that multiplicatively, we can reduce all natural numbers uniquely into primes. Thus, if we understand the prime numbers completely, we will understand the multiplicative structure of the natural numbers. Unfortunately, understanding of the primes has been notoriously elusive.

2.3.1 The Sieve of Eratosthenes

One of the earliest attempts to find the prime numbers was by Eratosthenes of Cyrene in the third century BCE. Eratosthenes realized that we can make a list of prime numbers by an iterative process.

We make a list of the first, say, hundred numbers, and cross off one because it a unit. The first uncrossed on the list, 2, is prime; we write it down, and then discard it and all its multiples (which of course aren't prime since they're divisible by 2).

Now the first uncrossed number, 3, is prime, since it's not divisible by any smaller prime. Now we can cross 3 and all its multiples. The first uncrossed number, 5, is prime, and we can repeat the process; at the end we will know all the primes on our list.

A process like this is called a "sieve" because it sifts the primes out of a larger set of numbers. There is a substantial body of research known as "sieve theory" which formulates better sieves and arguments based on sieves. Some of these more sophisticated sieves and sieve arguments could make a good paper. These advanced sieving methods have allowed us to build large lists of primes; as of August 2019, the largest known prime is the *Mersenne Prime* $2^{74,207,281} - 1$.

Unfortunately, sieve theory has a major weakness known as the "parity problem":

Fact 2.17 (Parity Problem)**.** *It is not possible for a purely sieve-theory-based argument to differentiate primes from numbrs which are the product of two primes.*

We shall discuss an example problem where this is an issue shortly. Of course, there is a great deal of work trying to get around this limitation of sieve theory.

This technique also gives us a (very!) rough estimate for how many primes there are up to a given number. In the first step of the sieve of Eratosthenes, we throw away about half of our numbers. In the second step, we throw away a third–but wait, we've counted some of them twice, so add a sixth of our numbers back in. In the third step we throw out a fifth, but then we need to add back in a tenth and a fifteenth, but then we have to throw out a thirtieth again.

In the limit, we expect the fraction of numbers which are prime to be roughly

$$1 - \sum_p \frac{1}{p} + \sum_{p \neq q} \frac{1}{pq} - \sum_{p \neq q \neq r} \frac{1}{pqr} + \dots$$

Unfortunately, error terms in this approximation build quickly enough that getting good data out of this is hard–in particular we run up against the parity problem very hard.

2.3.2 Counting Primes and the Prime Number Theorem

Based on data from algorithms like the sieve of Eratosthenes, mathematicians in the 1700s and 1800s wished to estimate the density of primes.

Definition 2.18. The function $\pi(x)$ is the number of prime numbers less than or equal to x. Thus $\pi(10) = 4$ and $\pi(100) = 25$.

Legendre (1798) used counts of prime numbers by Vega to estimate that $\pi(x)$ was approximated by

$$\frac{\log x}{x - 1.08366}.$$

This was not quite correct, and Gauss came up with a more accurate conjecture, that

$$\pi(x) \sim \frac{x}{\log x} \sim Li(x) = \int_2^x \frac{dt}{\log t}.$$

Chebyshev (1850) produced a great deal of work towards this, but the result was not proven until Hadamard and de la Vallée-Poussin (1896) independently proved the Prime Number Theorem:

Theorem 2.19 (Prime Number Theorem)**.**

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1.$$

2.3.3 Riemann Zeta Function

Though several proofs exist today, including elementary proofs by Selberg and Erdős (1949), the Prime Number Theorem was originally proved using results from complex analysis. Riemann (1859) defined the *Riemann Zeta Function*

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p \frac{1}{1-p^{-s}}$$

(and the equality of the two formulas can be proved using the Fundamental Theorem of Arithmetic).

The Riemann Zeta Function underlies a number of the most sought-after results in number theory today. It controls and describes a great deal of the "deep structure" of the distribution of prime numbers, and I hope to return later in the course and discuss it in more detail. Of particular note is the famous Riemann Hypothesis:

Conjecture 2.20. *If s is a complex number with $\zeta(s) = 0$, then either s is a negative even integer, or the real part of s is equal to $1/2$.*

Proving this result would imply a number of important facts about the primes; in particular, it would imply that the error in the approximation given in the Prime Number Theorem is very small. People often say that the Riemann Hypothesis would essentially imply that the primes are distributed randomly.

2.3.4 Arithmetic Progressions

Let's examine this idea of random distribution a bit more. It's pretty clear that there are very few primes that are, say, multiples of three. However, if the primes are "random" we shouldn't expect there to be more primes of the form $3n+1$ than $3n+2$. Similarly, there

are no primes of the forms $4n$ or $4n+2$ but we would expect "equally many" of the forms $4n+1$ and $4n+3$. Indeed, our data seem to imply this.

There are some very precise formulations of this idea (and again, exploring these could make a good paper). But the simplest version of the idea would simply expect all of these sets to be infinite. This was indeed proven by Dirichlet in 1837.

Theorem 2.21 (Dirichlet)**.** *If $a, b \in \mathbb{N}$ with $(a,b) = 1$, then the set $\{an+b : n \in \mathbb{N}\}$ has infinitely many primes.*

An *arithmetic progression* is just a set of this form $\{an+b : n \in \mathbb{N}\}$, in which the difference between consecutive elements is constant. Thus Dirichlet proved that all non-trivial arithmetic progressions that don't start at 0 have infinitely many primes. Note we could also phrase this in terms of modular arithmetic: the set of primes equivalent to b mod a is infinite if $(a,b) = 0$.

We can also turn this question around and approach from the other angle. Dirichlet proved that every (reasonable) arithmetic progression contains infinitely many primes. We can ask instead whether the set of primes contains arithmetic progressions.

Green and Tao (2004) proved that the set of primes contains arithmetic progressions of any length–thus if you want a set of thirty consecutive primes which are equal distances apart, you can find one.

2.3.5 Prime Gaps

We just said that there are infinitely many times when the primes are spaced reasonably closely. But if each number has a $1/\log n$ chance of being prime, then *on average* we would expect the space p_n and p_{n+1} to be about $\log(p_n)$.

However, there is dramatic variance in both directions. It's clear that the smallest possible gap that can occur regularly is of size 2. In fact, we suspect that this happens infinitely often.

Conjecture 2.22 (Twin Primes)**.** *There are infinitely many prime numbers p such that $p+2$ is also prime.*

Sieve theory has gotten us halfway to proving this result:

Theorem 2.23 (Chen)**.** *There are infinitely many primes p such that $p+2$ is either prime or the product of two primes.*

You might note that this is as close as we can get before running into the parity problem again.

We do know that twin primes are considerably rarer than primes. In particular, the sum of the reciprocals of the primes $\sum \frac{1}{p}$ diverges, similar to the harmonic series. But the sum of the reciprocals of the twin primes converges–thus while they may be infinite, they are not very infinite.

Recently, it was proven that there is some constant c so that there are infinitely many pairs of primes $p, p+N$. The polymath project has proven the smallest such N is at most 246.

Notice that we can't really look for triples $p, p+2, p+4$, since one of those will be divisible by 3. Thus any triple of such primes must contain 3, and the only one is $3, 5, 7$.

We can also look in the other direction: how *large* can the gaps between consecutive primes get? It turns out that these gaps also get infinitely large, as you will prove on your homework.

Exercise 2.24. *Prove that for any $n \in \mathbb{N}$, there are at least n consecutive composite integers. Hint: consider $(n+1)! + 2$.*

2.4 Primality Testing and Factorization

For further reading on the material in this subsection, consult **Rosen 3.1,3.6**.

The previous subsection stated a lot of results about the general distribution of prime numbers. Now we will scale down a bit and figure out how to look at individual numbers–to determine if they are primes, and factor them if they are not.

If we want to factor a natural number n, or just tell whether it's prime, the obvious idea is to try dividing by all the numbers smaller than n; an obvious optimization is to just divide by all the primes, if we have a list of primes, since every composite number has a prime factor.

One more optimization is not too hard to see:

Lemma 2.25. *If n is a composite number, then n has a prime factor no larger than $\sqrt{n}$.*

Proof. Since n is composite, we can write $n = ab$ for $1 < a \leq b < n$. Then if $a > \sqrt{n}$ then $ab \geq a^2 > (\sqrt{n})^n = n$. Thus $a \leq \sqrt{n}$, and a has at least one prime factor p (which might be the same as a). Thus $1 < p \leq a \leq \sqrt{n}$. □

Thus to test if n is prime, or to attempt to factor it, we only need to try dividing by every prime smaller than $\sqrt{n}$.

2.4.1 Fermat Factorization

Fermat developed a factorization technique that is often better than the naive approach, although substantially limited. The basic idea comes from the following lemma:

Lemma 2.26. *If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers, and pairs of squares whose difference is n.*

Proof. Let n be an odd positive integer, and suppose $n = s^2 - t^2$. Then we can factor $n = (s-t)(s+t)$ and thus we have a factorization into two positive integers.

Conversely, let$n = ab$ be a factorization into two positive integers. Then we can observe that if we set $s = (a+b)/2$ and $t = (a-b)/2$, then

$$s^2 - t^2 = \frac{a^2 + 2ab + b^2}{4} - \frac{a^2 - 2ab + b^2}{4} = \frac{ab}{2} - \frac{-ab}{2} = ab = n.$$

□

Thus if we can write $n = x^2 - y^2$ as a difference of squares, we have a factorization. This might not seem like a huge advance, since we've replaced one non-obviously-easy problem with another, but it leads to a more straightforward algorithm:

Set t to be the least integer greater than $\sqrt{n}$ so that t^2 is the least square larger than n. Then start computing the sequence

$$t^2 - n, (t+1)^2 - n, (t+2)^2 - n, \dots$$

and examine it for squares; if we find a square s^2 in this sequence, we have a factorization of $n = t^2 - s^2 = (t-s)(t+s)$.

This algorithm always terminates, because it will eventually reach $t = (n+1)/2$ and yield the equations

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = n \cdot 1.$$

Example 2.27. Let's factor 16899. We use a calculator to compute that $\sqrt{16899} \approx 129.996$, so we start at 130. We compute

$$130^2 - n = 16900 - 16899 = 1 = 1^2$$

So we have

$$16899 = 130^2 - 1^2 = (130-1)(130+1) = 129 \cdot 131.$$

Example 2.28. Let's factor 3827. We compute $\sqrt{3827} \approx 61.8$, so we start at 62. We compute

$$62^2 - 3827 = 3844 - 3827 = 17$$
$$63^2 - 3827 = 3969 - 3827 = 142$$
$$64^2 - 3827 = 4096 - 3827 = 269$$
$$65^2 - 3827 = 4225 - 3827 = 398$$
$$66^2 - 3827 = 4356 - 3827 = 529 = 23^2$$

so we have $t = 66, s = 23$, and thus

$$3827 = 66^2 - 23^2 = (66 - 23)(66 + 23) = 43 \cdot 89.$$

Unfortunately, the worst-case performance of this algorithm is actually pretty bad; in the worst case, we have to check $(n+1)/2 - \sqrt{n}$ integers. But this algorithm works well in "good" cases where our integer n has two factors of similar size. And many more advanced factorization techniques are based on this idea.

2.4.2 Efficient Factorization Algorithms

There are of course more efficient factorization methods, some of which we will see later in the course, after we study modular arithmetic. There are a few that are outside of the scope of this course, but which I want to mention now.

The second most efficient known classical algorithm is the *quadratic sieve* of Carl Pomerance (1981), which takes approximately $e^{\sqrt{\log n \log\log n}}$ operations to factor an integer n. This algorithm is basically a method for making Fermat factorization efficient by trying many possible square differences in parallel. Explaining this algorithm would probably make a good paper. This algorithm is in fact the most efficient for numbers smaller than 10^{100} and is still in wide use.

The most efficient known classical algorithm is the *general number field sieve* of Buhler, Lenstra, Pomerance. This takes approximately

$$e^{\sqrt[3]{64/9}(\log n)^{1/3}(\log\log n)^{2/3}}$$

operations to factor an integer n. This algorithm holds the record for the largest computed prime factorization; in 2009 a group of researchers used hundreds of computers to factor a 232-digit number called "RSA-768" used for some cryptographic applications.

Remark 2.29. Note that you could write both of these as polynomials in n, but for complexity reasons we actually want to count the number of *bits* it takes to represent n, which is approximately $\log n$. So rather than writing the times as polynomial in n we write them as exponential in $\log n$.

Thus there is no known classical algorithm that factors a large integer in polynomial time; we say that we do not believe integer factorization is "in P".

The most efficient known algorithm at all is Shor's Algorithm, formulated by Peter Shor in 1994. This algorithm runs only on quantum computers, and takes approximately $(\log n)^2(\log\log n)(\log\log\log n)$ steps to factor an integer n. Thus *on a quantum computer* it is possible to to factor an integer in polynomial time (we say the integer factorization problem is "in BQP").

2.4.3 Prime testing and prime certificates

While it is generally difficult to factor a large number, it turns out that it is much easier if we just want to know whether a number is prime. We can in fact (somewhat frustratingly) prove a number is or isn't prime, while having no idea what its factors are if it is composite.

In 2002, Agrawal, Kayal, Saxena found an algorithm that can prove an integer to be prime in about $(\log n)^{12}$ operations. In fact this algorithm has been improved to work in $(\log n)^{6+\epsilon}$ operations for any $\epsilon > 0$; if a certain widely believed conjecture is true, it in fact works in $(\log n)^6$ operations.

A different algorithm by Miller (1975) will in fact work in $(\log n)^5$ operations, if the Generalized Riemann Hypothesis is true.

Remark 2.30. These results imply that the prime factorization problem is definitely in NP, which roughly means that a proposed solution can be *checked* in polynomial time, even if it takes longer to generate a solution. Given a factorization of a large integer, it is easy to check it is correct by multiplying all the numbers together, and by these results we can also confirm that every factor is in fact prime in polynomial time.

However, prime factorization is *not* (known to be) NP-complete. Many researchers believe that it is simultaneously impossible to solve in polynomial time, but easier in some sense than problems like the Travelling Salesman or the Shortest Vector Problem.

In all of this section, we've been studying "deterministic" algorithms, that definitely return the correct answer. But if we only want answers that are "probably" right, then prime testing becomes much easier. In order to understand this, we need to develop some tools from modular arithmetic.