Prime Numbers

Prime numbers are the basic building blocks of number theory. That's what the Fundamental Theorem of Arithmetic, tells us. Every number is built up in a unique fashion by multiplying together prime numbers. There are analogous situations in other areas of science, and without exception the discovery and description of the building blocks has had a profound effect on its discipline. For example, the field of chemistry was revolutionized by the discovery that every chemical is formed from a few basic elements and by Mendeleev cataloging these elements into families whose properties recur periodically. We will do something similar below when we split the set of prime numbers into various subsets, for example, into the set congruent to 1 modulo 4 and the set congruent to 3 modulo 4. Similarly, a tremendous advance in physics occurred when scientists discovered that the atoms comprising every element are made up of three basic particles, protons, neutrons, and electrons,[1] and that the number of each determines the chemical and physical attributes of the atom. For example, an atom made up of 92 protons and only 143 neutrons has properties that clearly distinguish it from its cousin with three additional neutrons.

The fact that prime numbers are basic building blocks is sufficient reason to study their properties. Of course, this doesn't imply that those properties will be interesting. Studying how to conjugate irregular verbs is important when learning a language, but that doesn't make it very appealing. Luckily, the more one studies prime numbers, the more interesting they become, and the more beautiful and surprising become the relationships that one discovers. In this brief chapter we will only have time to mention a few of the many remarkable properties of prime numbers.

[1] This description of an atom is a simplification, but it is a fairly accurate portrayal of the original atomic theories advanced in the early part of the twentieth century.

To begin with, let's list the first few primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots.$$

What can we glean from this list? First, it looks like 2 is the only even prime. This is true, of course. If n is even and larger than 2 then it factors as $n = 2 \cdot (n/2)$. This makes 2 somewhat unusual among the set of primes, so people have been known to say that

"2 is the oddest prime!"[2]

A more important observation from our list of primes is signified by the ellipsis (three dots) appended at the end. This means that the list is not complete. For example, 67 and 71 are the next two primes. However, the real issue is whether the list ends or whether it continues indefinitely. In other words, are there infinitely many prime numbers? The answer is yes. We now give a beautiful proof that appeared in Euclid's *Elements* more than 2000 years ago.

Theorem 1 (Infinitely Many Primes Theorem)**.** *There are infinitely many prime numbers.*

Euclid's Proof. Suppose that you have already compiled a (finite) list of primes. I am going to show you how to find a new prime that isn't in your list. Since you can then add the new prime to the list and repeat the process, this will show that there must be infinitely many primes.

So suppose we start with some list of primes $p_1, p_2, \ldots, p_r$. We multiply them together and add 1, which gives the number

$$A = p_1 p_2 \cdots p_r + 1.$$

If A itself is prime, we're done, since A is too large to be in the original list. But even if A is not prime, it will certainly be divisible by some prime, since every number can be written as a product of primes. Let q be some prime dividing A, for example, the smallest one. I claim that q is not in the original list, so it will be the desired new prime.

Why isn't q in the original list? We know that q divides A, so

$$q \text{ divides } p_1 p_2 \cdots p_r + 1.$$

If q were to equal one of the p_i's, then it would have to divide 1, which is not possible. This means that q is a new prime that may be added to our list. Repeating

[2]Naturally, I would never even consider repeating such a weak joke! Notice that this is one of those jokes that is language specific. For example, it doesn't work in French, since an odd number is *impair*, while an odd person or event is *étrange* or *bizarre*.

this process, we can create a list of primes that is as long as we want. This shows that there must be infinitely many prime numbers. □

Euclid's proof is very clever and beautiful. We will illustrate the ideas in Euclid's proof by using them to create a list of primes. We start with a list consisting of the single prime $\{2\}$. Following Euclid, we compute $A = 2 + 1 = 3$. This A is already prime, so we append it to our list. Now we have two primes, $\{2, 3\}$. Again using Euclid's argument, we compute $A = 2 \cdot 3 + 1 = 7$, and again A is prime and can be added to the list. This gives three primes, $\{2, 3, 7\}$. Repeating the argument gives $A = 2 \cdot 3 \cdot 7 + 1 = 43$, another prime! So now our list has four primes, $\{2, 3, 7, 43\}$. Into the breach once more, we compute $A = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$. This time, A is not prime, it factors as $A = 13 \cdot 139$. We add 13 to our list, which now reads $\{2, 3, 7, 43, 13\}$. One more time, we compute $A = 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 + 1 = 23479$. This A also factors, $A = 53 \cdot 443$. This gives the list $\{2, 3, 7, 43, 13, 53\}$, and we will stop here. But in principle we could continue this process to produce a list of primes of any specified length.

We now know that the list of primes continues without end, and we also observed that 2 is the only even prime. Every odd number is congruent to either 1 or 3 modulo 4, so we might ask which primes are congruent to 1 modulo 4 and which are congruent to 3 modulo 4. This separates the set of (odd) primes into two families, just as the periodic table separates the elements into families having similar properties. In the following list, we have boxed the primes congruent to 1 modulo 4:

$$3, \boxed{5}, 7, 11, \boxed{13}, \boxed{17}, 19, 23, \boxed{29}, 31, \boxed{37}, \boxed{41}, 43, 47, \boxed{53}, 59,$$
$$\boxed{61}, 67, 71, \boxed{73}, 79, 83, \boxed{89}, \boxed{97}, \boxed{101}, \ldots.$$

There doesn't seem to be any obvious pattern, although there do seem to be plenty of primes of each kind. Here's a longer list.

$p \equiv 1 \pmod 4$	$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109,$ $113, 137, 149, 157, 173, 181, 193, 197, \ldots$
$p \equiv 3 \pmod 4$	$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103,$ $107, 127, 131, 139, 151, 163, 167, 179, \ldots$

Is it possible that one of the lines in this list eventually stops, or are there infinitely many primes in each family? It turns out that each line continues indefinitely. We will use a variation of Euclid's proof to show that there are infinitely many primes congruent to 3 modulo 4.

Theorem 2 (Primes 3 (Mod 4) Theorem)**.** *There are infinitely many primes that are congruent to 3 modulo 4.*

Proof. We suppose that we have already compiled a (finite) list of primes, all of which are congruent to 3 modulo 4. Our goal is to make the list longer by finding a new 3 modulo 4 prime. Repeating this process gives a list of any desired length, thereby proving that there are infinitely many primes congruent to 3 modulo 4.

Suppose that our initial list of primes congruent to 3 modulo 4 is

$$3, p_1, p_2, \ldots, p_r.$$

Consider the number

$$A = 4p_1p_2 \cdots p_r + 3.$$

(Notice that we don't include the prime 3 in the product.) We know that A can be factored into a product of primes, say

$$A = q_1q_2 \cdots q_s.$$

I claim that among the primes $q_1, q_2, \ldots, q_s$ at least one of them must be congruent to 3 modulo 4. This is the key step in the proof. Why is it true? Well, if not, then $q_1, q_2, \ldots, q_s$ would all be congruent to 1 modulo 4, in which case their product A would be congruent to 1 modulo 4. But you can see from its definition that A is clearly congruent to 3 modulo 4. Hence, at least one of $q_1, q_2, \ldots, q_s$ must be congruent to 3 modulo 4, say $q_i \equiv 3 \pmod 4$.

My second claim is that q_i is not in the original list. Why not? Well, we know that q_i divides A, while it is clear from the definition of A that none of $3, p_1, p_2, \ldots, p_r$ divides A. Thus, q_i is not in our original list, so we may add it to the list and repeat the process. In this way we can create as long a list as we want, which shows that there must be infinitely many primes congruent to 3 modulo 4. □

We can use the ideas in the proof of the Primes 3 (Mod 4) Theorem to create a list of primes congruent to 3 modulo 4. We need to start with a list containing at least one such prime, and remember that 3 is not allowed in our list. So we start with the list consisting of the single prime $\{7\}$. We compute $A = 4 \cdot 7 + 3 = 31$. This A is itself prime, so it is a new $3 \pmod 4$ prime to add to our list. The list now reads $\{7, 31\}$, so we compute $A = 4 \cdot 7 \cdot 31 + 3 = 871$. This A is not prime; it factors as $A = 13 \cdot 67$. The proof of the theorem tells us that at least one of the prime factors will be congruent to 3 modulo 4. In this case, the prime 67 is $3 \pmod 4$, so we add it to our list. Next we take $\{7, 31, 67\}$, compute $A = 4 \cdot 7 \cdot 31 \cdot 67 + 3 = 58159$, and factor it as $A = 19 \cdot 3061$. This time it is the

first factor 19 that is $3 \pmod 4$, so our list becomes $\{7, 31, 67, 19\}$. We will repeat the process one more time. So

$$A = 4 \cdot 7 \cdot 31 \cdot 67 \cdot 19 + 3 = 1104967 = 179 \cdot 6173,$$

which gives the prime 179 to add to the list, $\{7, 31, 67, 19, 179\}$.

Why won't the same idea work for $1 \pmod 4$ primes? This is not an idle question; it's almost as important to understand the limitations of an argument as it is to understand why the argument is valid. So suppose we try to create a list of $1 \pmod 4$ primes. If we start with the list $\{p_1, p_2, \ldots, p_r\}$, we can compute the number $A = 4p_1p_2 \cdots p_r + 1$, factor it, and try to find a prime factor that is a new $1 \pmod 4$ prime. What happens if we start with the list $\{5\}$? We compute $A = 4 \cdot 5 + 1 = 21 = 3 \cdot 7$, and neither of the factors 3 or 7 is a $1 \pmod 4$ number. So we're stuck. The problem is that it is possible to multiply two $3 \pmod 4$ numbers, such as 3 and 7, and end up with a $1 \pmod 4$ number like $A = 21$. In general, we cannot use the fact that $A \equiv 1 \pmod 4$ to deduce that some prime factor of A is $1 \pmod 4$, and that's why this proof won't work for primes congruent to 1 modulo 4.

There is no particular reason to consider only congruences modulo 4. For example, every number is congruent to either 0, 1, 2, 3, or 4 modulo 5; and except for 5 itself, every prime number is congruent to one of 1, 2, 3, or 4 modulo 5. (Why?) So we can break up the set of prime numbers into four families, depending on their congruence class modulo 5. Here's a list of the first few numbers in each family:

$p \equiv 1 \pmod 5$	$11, 31, 41, 61, 71, 101, 131, 151, 181, 191, 211, 241$
$p \equiv 2 \pmod 5$	$2, 7, 17, 37, 47, 67, 97, 107, 127, 137, 157, 167, 197$
$p \equiv 3 \pmod 5$	$3, 13, 23, 43, 53, 73, 83, 103, 113, 163, 173, 193, 223$
$p \equiv 4 \pmod 5$	$19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239$

Again there seem to be lots of primes in each family, so we might guess that each contains infinitely many prime numbers.

In general, if we fix a modulus m and a number a, when might we expect there to be infinitely many primes congruent to a modulo m? There is one situation in which this cannot happen, that is if a and m have a common factor. For example, suppose that p is a prime and that $p \equiv 35 \pmod{77}$. This means that $p = 35 + 77y = 7(5 + 11y)$, so the only possibility is $p = 7$, and even $p = 7$ doesn't work. Generally, if p is a prime satisfying $p \equiv a \pmod m$, then $\gcd(a, m)$ divides p. So either $\gcd(a, m) = 1$ or else $\gcd(a, m) = p$, which means there is at most one possibility for p. Thus, it is really only interesting to ask about primes

congruent to a modulo m if we assume that $\gcd(a, m) = 1$. A famous theorem of Dirichlet from 1837 says that with this assumption there are always infinitely many primes congruent to a modulo m.

Theorem 3 (Dirichlet's Theorem on Primes in Arithmetic Progressions[3])**.** *Let a and m be integers with $\gcd(a, m) = 1$. Then there are infinitely many primes that are congruent to a modulo m. That is, there are infinitely many prime numbers p satisfying*

$$p \equiv a \pmod{m}.$$

Earlier in this chapter we proved Dirichlet's Theorem for $(a, m) = (3, 4)$, and Exercise 2 asks you to do $(a, m) = (5, 6)$. Unfortunately, the proof of Dirichlet's Theorem for all (a, m) is quite complicated, so we will not be able to give it in this book. The proof uses advanced methods from calculus and, in fact, calculus with complex numbers!

Exercises

1. Start with the list consisting of the single prime $\{5\}$ and use the ideas in Euclid's proof that there are infinitely many primes to create a list of primes until the numbers get too large for you to easily factor. (You should be able to factor any number less than 1000.)

2. **(a)** Show that there are infinitely many primes that are congruent to 5 modulo 6. [*Hint*. Use $A = 6p_1p_2 \cdots p_r + 5$.]

(b) Try to use the same idea (with $A = 5p_1p_2 \cdots p_r + 4$) to show that there are infinitely many primes congruent to 4 modulo 5. What goes wrong? In particular, what happens if you start with $\{19\}$ and try to make a longer list?

3. Let p be an odd prime number. Write the quantity

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1}$$

as a fraction A_p/B_p in lowest terms.

(a) Find the value of $A_p \pmod{p}$ and prove that your answer is correct.

(b) Make a conjecture for the value of $A_p \pmod{p^2}$.

(c) Prove your conjecture in (b). (This is quite difficult.)

[3] An arithmetic progression is a list of numbers with a common difference. For example, 2, 7, 12, 17, 22, ... is an arithmetic progression with common difference 5. The numbers congruent to a modulo m form an arithmetic progression with common difference m, which explains the name of Dirichlet's Theorem.

4. Let m be a positive integer, let $a_1, a_2, \ldots, a_{\phi(m)}$ be the integers between 1 and m that are relatively prime to m, and write the quantity

$$\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_{\phi(m)}}$$

as a fraction A_m/B_m in lowest terms.

(a) Find the value of $A_m \pmod{m}$ and prove that your answer is correct.

(b) Generate some data for the value of $A_m \pmod{m^2}$, try to find patterns, and then try to prove that the patterns you observe are true in general. In particular, when is $A_m \equiv 0 \pmod{m^2}$?

5. Recall that the number n *factorial*, which is written $n!$, is equal to the product

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

(a) Find the highest power of 2 dividing each of the numbers $1!, 2!, 3!, \ldots, 10!$.

(b) Formulate a rule that gives the highest power of 2 dividing $n!$. Use your rule to compute the highest power of 2 dividing $100!$ and $1000!$.

(c) Prove that your rule in (b) is correct.

(d) Repeat (a), (b), and (c), but this time for the largest power of 3 dividing $n!$.

(e) Try to formulate a general rule for the highest power of a prime p that divides $n!$. Use your rule to find the highest power of 7 dividing $1000!$ and the highest power of 11 dividing $5000!$.

(f) Using your rule from (e) or some other method, prove that if p is prime and if p^m divides $n!$ then $m < n/(p-1)$. (This inequality is very important in many areas of advanced number theory.)

6. (a) Find a prime p satisfying $p \equiv 1338 \pmod{1115}$. Are there infinitely many such primes?

(b) Find a prime p satisfying $p \equiv 1438 \pmod{1115}$. Are there infinitely many such primes?

This page intentionally left blank