Section 3: Types of Primes

In the previous sections, we saw the importance of prime numbers. But how many prime numbers are there? How many primes are there less than a given number n? Do they follow any pattern? Do they all have the same structure? Are there formulas that yield the primes? These are just a few of the questions about prime numbers that have intrigued mathematicians for ages. Some have been answered and some haven't. In this section, we'll discuss these questions (and more) and answer those that we can.

How many prime numbers are there?

It was Euclid circa 350 BC who first proved that there are infinitely many primes. It has since been proved by others in different ways, but Euclid's proof is the most elegant, precisely because it is the simplest.

Theorem 1.3.1 (Euclid) There are infinitely many primes.

> **Proof**: Suppose there are finitely many primes, say $p_1, p_2, p_3, \ldots, p_n$. Define the number $N = p_1 p_2 p_3 \cdots p_n + 1$. By the FTA, this number is divisible by some prime number. Suppose without loss of generality that it is p_1. So p_1 divides N and it obviously divides $p_1 p_2 p_3 \cdots p_n$ as well. So by Exercise 1.2.2 (3), it must divide 1 also. This is clearly impossible. Therefore our initial assumption (that there were only a finite number of primes) is false. So there are infinitely many primes. ■

Once a theorem is proved the issue is settled, right? Not quite. Sometimes, people try to find a different method of proving a theorem because they are not satisfied with the method employed previously. In this case, some mathematicians objected (and in fact some still object) to Euclid's use of proof by contradiction. In the early part of the 20th century there were three competing schools of thought regarding the nature of mathematics. One of them, the intuitionist school of thought, held that proofs by contradiction were invalid. This way of thinking was not new, but this was the first time their beliefs were organized into a coherent viewpoint. The intuitionists, however, did not attempt to prove the infinitude of the primes using a different method. For one reason, this had already been done by Euler (in 1748) and Tchebeychef (in 1852). But more importantly, they did not even believe that there were an infinite number of primes. In fact, intuitionists reject infinity altogether. Needless to say, their viewpoint did not become the predominant viewpoint in mathematics.

In 1748, the Swiss mathematician Leonhard Euler (1707-1783) devised a second famous proof of the infinitude of the primes. To sketch his proof, we will need his π function. Euler defined $\pi(n)$ to be the number of primes numbers less than or equal to n. So for example, $\pi(5) = 3$, $\pi(6) = 3$, and $\pi(7) = 4$. Notice that $\pi(n)$ is a step function that jumps up by one unit

at each prime number. Now define $\lambda(n) = \prod_{i=1}^{\pi(n)} \frac{1}{1-\frac{1}{p_i}}$ where $\prod$ means product (similar to how $\sum$ means sum) and $p_1, p_2, p_3, \ldots, p_{\pi(n)}$ are the primes less than or equal to n. It can (fairly) easily be shown that this product is greater than or equal to $\sum_{k=1}^{n} \frac{1}{k}$. As $n \to \infty$, this sum approaches the harmonic series, and is therefore divergent (tends to ∞). Since Euler's λ function is larger than this, it must also tend to ∞. Therefore, there are an infinite number of primes.

While it might seem unnecessary (even a waste of time?) to prove a result that has already been proved, we shall soon see that the techniques (and functions) Euler used in his proof turned out to be very valuable and have far reaching implications.

Finally, in 1852, Russian mathematician Pafnuti Tchebeychev (1821-1894) showed that $\pi(n) \geq \ln(\ln(n))$ (for $n > 1$). Since $\ln(\ln(n)) \to \infty$ as $n \to \infty$, $\pi(n)$ must tend to ∞ also. Therefore there are an infinite number of primes. (This is a great example of a result in the field of *analytic number theory*.)

How many primes are there less than a given number n?

Ok, so it is settled. There are an infinite number of primes. But how many primes are there below 1,000,000? Putting it another way, how do we evaluate Euler's $\pi(n)$? The earliest successful method for determining the number of prime numbers less than a given number was devised by the ancient Greek mathematician Eratosthenes (276-194 BC). Eratosthenes was a "renaissance man" 1700 years before the European Renaissance. In addition to being a wonderful mathematician, he was also a geographer, astronomer, historian, poet, and athlete. Even his nickname "Beta" reflected his prowess at a wide variety of fields. Legend has it he acquired that nickname because he was considered to be the second best in the world…at everything! While this might appear to be a criticism, it would obviously still be quite an achievement. With regards to number theory, Eratosthenes is best remembered for computing $\pi(n)$ (although it wasn't called this until Euler) using his prime number sieve (now called the Sieve of Eratosthenes). It works like this: write down all the numbers from 1 to n. Cross out the number 1 (since it is not prime). Circle the number 2 and then cross out every second number (every multiple of 2). Then circle the number 3 and cross out every third number (unless it has already been crossed out). Circle the next untouched number and cross out all of its multiples. Continue until every number has been circled or crossed out. The circled numbers are all prime, so just count them up.

Exercise 1.3.2 Use the Sieve of Eratosthenes to find $\pi(400)$.

While this method works, it is obviously burdensome for large values of n. Another way to *approximate* how many prime numbers there are less than or equal to a given number n is the celebrated Prime Number Theorem.

Theorem 1.3.3 (Prime Number Theorem) For large values of n, the number of primes less than or equal to n is approximately equal to $n/\ln(n)$. In other words,

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

This was first conjectured by Gauss in 1800 and was proven the *first* time in 1896 independently by the French mathematician Jacques Hadamard and the Belgian Charles de la Vallee-Poussin. Atle Selberg of Norway and Paul Erdös of Hungary proved it again in the middle of the 20th century, this time without resorting to complex analysis as Hadamard and Vallee-Poussin had. The Prime Number Theorem is one of the most impressive results of analytic number theory.

Exercise 1.3.4 Use the Prime Number Theorem to approximate how many primes are between 2017 and 4081 inclusive.

Gauss actually found that the definite integral $\int_2^n \frac{dx}{\ln(x)}$ approximates $\pi(n)$ even better than $n/\ln(n)$. For years, this integral, named $\text{Li}(n)$, was assumed to be larger than $\pi(n)$ for all n. However, in 1914 the English mathematician J. E. Littlewood proved that this was not the case, and in 1933 a number N was found for which $\text{Li}(N) < \pi(N)$. As a fan of the power of mathematics, I want to reiterate that last point. Mathematicians thought that $\text{Li}(n) > \pi(n)$ for all n, but in 1914 Littlewood proved that was not the case. So Littlewood proved that $\text{Li}(n) \le \pi(n)$ was possible. But it took 19 years for someone to actually find a number for which this was true. Now known as Skewes' number (after the mathematician who found it), $N = 10^{10^{10^{34}}}$. This is no longer the smallest such number. It is now known that between 6.62×10^{370} and 6.69×10^{370} there are 10^{180} integers for which $\text{Li}(n) \le \pi(n)$. Simply amazing.

Exercise 1.3.5 Show that $\lim_{n\to\infty}\left(\frac{\text{Li}(n)}{\pi(n)}\right) = 1$. [Hint: Use the Prime Number Theorem, L'Hopital's Rule, and the Second Fundamental Theorem of Calculus]

Do they follow any pattern?

So we now know there are infinitely many prime numbers, and we can roughly approximate how many there are less than a given integer. What can we say about their form or structure? Anything?

Sure. First of all, except for 2, they are all odd. Stated another way, except for 2, they are all of the form $2a+1$ for some integer a. Similarly, except for 3, they are all of the form $3a+1$ or $3a+2$. Many other such statements using different "base primes" can be made. These

statements are special cases of a wonderful theorem established by Peter Dirichlet (1805-1859) of Germany.

Theorem 1.3.6 (Dirichlet) If a and b are relatively prime, then in any arithmetic progression $a, a+b, a+2b, a+3b, \ldots$, there are an infinite number of primes.

It is however, impossible that such an arithmetic sequence be made up *entirely* of primes.

Exercise 1.3.7 (a) In Drichlet's Theorem, why must a and b be relatively prime?
(b) Why is it impossible for an arithmetic progression as described in Dirichlet's Theorem to be made up entirely of prime numbers?

Ok, so an arithmetic sequence cannot be *only* prime numbers. Suppose you want an arithmetic sequence in which the first n terms are all primes. Is this possible for any n? This is unknown. The longest such string is currently 22 achieved by the arithmetic progression $11410377850553 + 4609098694200k$ for $k = 0,1,2,\ldots 21$.

In searching for patterns among the primes, arithmetic progressions (linear functions) are only the beginning. We can also consider quadratic functions. The search for prime-producing quadratic functions is very interesting. Consider the simple quadratic polynomials $f_p(n) = n^2 + n + p$.

Example 1.3.8 (a) Let $p = 3$. Then $f_3(n) = n^2 + n + 3$. This polynomial, when evaluated at integers starting with $n = 0$ yields 2 prime numbers. Namely, $f_3(0) = 3$ and $f_3(1) = 5$.

(b) Let $p = 5$. Then $f_5(n) = n^2 + n + 5$. This time we get 4 initial prime numbers, $f_5(0) = 5$, $f_5(1) = 7$, $f_5(2) = 11$, and $f_5(3) = 17$.

(c) Let $p = 13$. Then $f_{13}(n) = n^2 + n + 13$. The first 12 evaluations produce prime numbers.

See a pattern? It appears that the quadratic polynomial $f_p(n) = n^2 + n + p$ will always yield $p-1$ initial prime numbers when evaluated at the integers $0,1,2,\ldots p-2$. Could we ever get more? Will it ever be less? No, and yes. Notice that

$$f_p(p-1) = (p-1)^2 + (p-1) + p = p^2 - 2p + 1 + 2p - 1 + p = p^2,$$

so $f_p(p-1)$ will never be prime, and therefore we will never get p initial primes. Also, it has been shown that $p = 41$ is the largest prime number for which we will get $p-1$ initial primes. For example, f_{43} yields only one initial prime (since $f_{43}(1) = 45$).

Another way in which mathematicians have searched for a pattern is in looking at the distribution of the primes. There are very small intervals between consecutive primes (such as 11 and 13, 41 and 43, and 1,000,000,000,061 and 1,000,000,000,063) as well as arbitrarily long intervals. Primes in the former case are called ***twin primes***. It is an unanswered question whether there are infinitely many pairs of twin primes.

Consecutive primes can also be very far apart. In fact, it is easy to show that the numbers $(n+1)!+2,(n+1)!+3,\ldots,(n+1)!+(n+1)$ (for some fixed natural number n) are all composite. So if we wish to find 5 consecutive composite numbers (and therefore a gap in the primes of at least that big), we need only look at the numbers,

$$6!+2=722$$
$$6!+3=723$$
$$6!+4=724$$
$$6!+5=725$$
$$6!+6=726$$

Of course, this may not be the first occurrence of such a gap. In fact, 90, 91, 92, 93, 94, 95, and 96 are all composite. Another current hot topic in prime number theory (utilizing the computer in no small amount) is looking for the first occurrence of a gap for each possible size. The largest effectively calculated gap has length 1355 and it occurs *first* after the prime 401,429,925,999,153,707.

Exercise 1.3.9 Find 10 consecutive composite integers.

This leads us to Goldbach's Conjecture. In a letter to Euler in 1742, Christian Goldbach guessed that every even integer greater than 4 is the sum of two primes. This has been verified for many numbers, but a proof remains unrealized.

Exercise 1.3.10 Assuming Goldbach's conjecture is true, prove that there exists a way to write every integer greater than 1 as the sum of at most three primes.

Do they all have the same structure?

Certainly not. In fact, primes come in a surprisingly wide variety of structures. Throughout history, primes of certain types have been studied for one reason or another. They are often named for the primary mathematician who studied them. There are Fermat primes (prime of the form $2^{2^n}+1$ studied by Pierre Fermat), Germain primes ($\frac{p-1}{2}$ studied by Sophie Germain), and Mersenne primes (2^p-1 studied by Marin Mersenne). In the first formula, n is a natural number; in the second two p is a prime. In some cases there are infinitely many primes (Germain) while in others there are only finitely many (there are currently 47 known Mersenne primes and 5 known Fermat primes). We will look into some of these in more detail later.

Exercise 1.3.11 Find the first 5 Fermat primes, Germain primes, and Mersenne primes.

Exercise 1.3.12 Show that if $a^n - 1$ is prime, then $a = 2$ and n must be prime.
[Hint: $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$]

Are there formulas that yield the primes?

Yes, but not very handy ones. Aside from the limited formulas given above by $f_p(n) = n^2 + n + p$, there are a few formulas that produce primes. Most of these formulas are very un-utilitarian however. In one (see Exercise 1.3.13 below), in order to find, say the 10^{th} prime, you must count the number of primes less than or equal to 2^{10}. There are 172 primes less than or equal to 2^{10}, but in counting this, we've gone right past the one we wanted to find.

There is an even more amazing, yet useless formula for primes. In 1957, American mathematician William Mills proved that there exists a positive real number r such that $f(n) = [r^{3^n}]$ is prime for any natural number n (where the symbol [ ] denotes the greatest integer function). However, no one, including Mills, knows what that real number r is. This is a perfect example of an existence theorem.

Finally, there is also an amazing polynomial that produces every prime number. It is a 25^{th} degree polynomial in 26 unknowns, and when evaluated at positive integers, if a positive integer is achieved, it's prime.

Exercise 1.3.13 In 1964, Williams devised the following formula:

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\sqrt[n]{\frac{n}{1+\pi(m)}} \right].$$

Again, [ ] denotes the greatest integer function, and $\pi(m)$ is of course Euler's function. Use this formula to find the 5^{th} prime.