Chapel Hill Math Circle:
Prime Numbers

1 Introduction

Last week we considered a few families of special numbers. In this worksheet, we consider what is possibly the most special family of numbers: the primes!

The second section collects some preliminary facts, as well as some "basic" facts regarding prime numbers. The third section explores the fact that there are infinitely many primes, including some facts regarding infinitely many primes of certain forms.

The next, and fourth, section introduces two families of primes named after famous mathematicians: the Mersenne and Sophie Germain primes. The final section touches on the prime number theorem, which gives an indication of the distribution of primes amongst the integers.

2 Basic Facts

Recall that an integer a divides another integer b, written $a|b$, if there exists some integer k such that $b = ka$.

Exercise 2.1 Prove that if $a|b$ and $b|a$, then either $a = b$ or $a = -b$.

A *prime number* is an integer that cannot be written as the product of 2 or more smaller integers ≥ 1. We can also express this by saying p is a prime if its only divisors are p and 1.

Exercise 2.2 Suppose p, q, r, and s are all distinct primes. Can $pq = rs$?

Exercise 2.3 Let p be prime, and a and k be positive integers. Prove that if p divides a^k, then p^k divides a^k.

Exercise 2.4 Prove that an integer n is prime if and only if n is not divisible by any prime p, with $1 < p \leq \sqrt{n}$.

A natural question is if there is a formula for the nth prime, i.e. a function $f(n)$ that is prime for every integer n. If we relax the condition to being $f(n)$ returns primes, along with some possibly non-primes, then $f(n) = n$ is certainly a valid (but not very helpful) function.

Exercise 2.5 Show that the polynomial $f(n) = n^2 - n + 41$ returns a prime for $n = 1, 2, 3$, and 4.

It turns out that $f(n)$ is a prime number for $n = 1, 2, ..., 40$.

Exercise 2.6 What happens at $n = 41$? I.e. is $f(41)$ prime?

Another example is the polynomial

$$g(n) = (n - 40)^2 + (n - 40) + 41,$$

which is prime for $n = 1, ..., 79$.

Exercise 2.7 Show that $g(80)$ is a composite number. Hint: find constants a and b such that $g(n) = n^2 + an + b$.

It is a theorem that no non-constant polynomial with integer coefficients can be prime for all n, so even though we may be able to get arbitrarily long strings of primes as outputs from a polynomial (like from f and g above), eventually we'll get composite numbers.

The discussion and exercises below work off the assumption that there are infinitely many primes; a priori this is not necessarily the case, but we will see a proof in the next section that it is indeed true.

Another route is to look for primes that take special forms. Mersenne primes are one example of these, which we'll consider in a later section, but here let's try for a particularly simple expression.

Exercise 2.8 How many primes can be written in the form $a^3 - 1$ for some integer a?

Two much harder questions are the following, which are still unsolved.

Exercise 2.9 ***** Show that there are infinitely many primes of the form $n^2 + 1$, where n is an integer.

Exercise 2.10 ***** Show that there are infinitely many twin primes, i.e. primes of the form p and $p + 2$.

If you manage to solve the above exercise, you'll have made a deep and important contribution to modern mathematics. In 2013 it was shown that there are infinitely many prime pairs of the form $(p, p+k)$, where k is an integer no bigger than $70,000,000$. As of 2014, the integer k from the last statement has been brought down to 216. Of course if it is shown that k can be 2, then the twin prime conjecture will be proven, but we're still a ways away.

Another interesting related question is that of prime triples, i.e. triples of the form $(p, p+k_1, p+k_2)$ for integers k_1, k_2 with p a prime.

Exercise 2.11 If $p > 2$ and $(p, p+k_1, p+k_2)$ is a prime triple, show that k_1 and k_2 must both be even. Why does this fail when $p \leq 2$?

Exercise 2.12 Show that there cannot exist prime triples of the form $(p, p+2, p+4)$. Hint: at least one of the three numbers must be divisible by a prime less than 10; why?

Two open problems in the same vein as the last exercise are the following:

Exercise 2.13 ***** Show that there are infinitely many prime triples of the form $(p, p+4, p+6)$.

Exercise 2.14 ***** Show that there are infinitely many prime triples of the form $(p, p+2, p+6)$.

Perhaps a surprising, but not too hard to prove, statement is that there are arbitrarily large gaps between primes. In the framework given above, if we have an odd integer k, then we can find a prime p such that p and $p+k$ are primes, and there are no primes between p and $p+k$.

Exercise 2.15 Prove this. Hint: consider the consecutive integers $(n+1)!+2, (n+1)!+3, (n+1)!+4, ..., (n+1)!+n, (n+1)!+(n+1)$.

3 The Infinitude of Primes

A fact known since the time of the Greeks is that there are infinitely many primes. Euclid's[1] proof proceeds roughly as follows: suppose to the contrary that there are finitely many primes, and list them $p_1, p_2, ..., p_N$. Consider the

[1]One of the great Greek mathematicians, he also wrote the most influential math text in history "Euclid's Elements."

product $P = p_1 p_2 \cdots p_N + 1$. Note that none of the p_i divide P, since none of the p_i divides 1, so P cannot be a composite of any of the p_i. This implies P is another prime number, and so P must be in our list $p_1, ..., p_n$. This is impossible though; $P > p_i$ for each of the finitely many p_i. Our assumption is therefore false, proving that there are infinitely many primes.

Exercise 3.1 * Prove that there are infinitely many primes of the form $4n+3$, where n is an integer. Hint: consider the number $P = 2^2 \cdot 3 \cdot \cdots p_N - 1$, i.e. 1 less than the product of the first N primes, which is of the form $4n + 3$. Show that it cannot be the product of a prime of the form $4n + 1$, etc.

Exercise 3.2 * Using similar ideas as in the last exercise, show that there are infinitely many primes of the form $6n + 5$.

An interesting theorem, well beyond the scope of this worksheet, is a theorem by Dirichlet: if a is positive and a and b are coprime, then there are infinitely many primes of the form $an + b$. The cases $b = 1$ and $b = -1$ are considerably easier, but still beyond this worksheet.

Exercise 3.3 * A key step in the proof of Dirichlet's theorem is showing that the series $\sum_n \frac{1}{q_n}$ diverges, where q_n are primes congruent to b modulo a. Show that if this series diverges, then there are infinitely many primes of the form $an + b$.

An interesting fact is that, letting p_n denote the nth prime, the series

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots = \infty.$$

The proof of this is not too difficult, but would take us a little astray. For those interested, the book "An Introduction to the Theory of Numbers" by Hardy and Wright is an excellent introduction to this beautiful area of mathematics, and is very readable.

4 Primes with Names

In this section, we'll look at two classes of primes named after famous mathematicians. These are the Mersenne primes, named after Marin Mersenne (1588-1648), and Sophie Germain primes, named after Sophie Germain (1776-1831).

Mersenne Primes

A special class of prime numbers are the *Mersenne primes*. These are primes of the form $M_n = 2^n - 1$ for some integer n.

Exercise 4.1 Verify that M_2, M_3, and M_5 are in fact prime, but M_4 is not.

Since January of this year there are 49 known Mersenne primes; the largest of these numbers is

$$M_{74,207,281} = 2^{74,207,281} - 1,$$

which has 22,338,618 digits. It is not known whether or not there are infinitely many Mersenne primes, even though there are infinitely many primes.

Exercise 4.2 ***** Prove that there are infinitely many Mersenne primes.

An exercise that is slightly easier is the following:

Exercise 4.3 Show that if $2^n - 1$ is to be a prime, then n must be a prime. Hint: write $n = ab$, a composite, and show that $2^n - 1$ must also be composite.

Sophie Germain Primes

A *Sophie Germain prime* is a prime number p such that both p and $2p + 1$ are prime.

Exercise 4.4 What are the first four Sophie Germain primes?

The largest known Sophie Germain prime pair is $(p, 2p + 1)$, where

$$p = 2,618,163,402,417 \cdot 2^{1,290,000} - 1,$$

discovered in early 2016.

The importance of this family prime numbers is by an early result related to Fermat's last theorem. Sophie Germain proved[2] that if p is a Sophie Germain prime, then there are no non-trivial integers x, y, and z, none a multiple of p, such that

$$x^p + y^p = z^p.$$

[2]In 1825, about 169 years before Fermat's last theorem was finally proved.

Many similar sub-cases of Fermat's last theorem were proven throughout the years, but a complete, general proof took many more years of developments, using tools not developed until the last 50 years.

Exercise 4.5 Show that if p is a Sophie Germain prime greater than 3, then p is congruent to 2 mod 3, i.e. $p - 2$ is divisible by 3.

5 The Prime Number Theorem

The prime number theorem (PNT) gives an asymptotic distribution of the primes. While there are a number of proofs of the PNT, some of the earliest proofs utilized the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

A well-known still-unsolved problem is the Riemann hypothesis, which is a conjecture about the non-trivial zeros of ζ as a function of complex numbers. In this section, we'll explore some more basic ideas related to the PNT.

Let $\pi(N)$ denote the number of primes less than or equal to N.

Exercise 5.1 What is $\pi(10)$? What about $\pi(100)$?

Exercise 5.2 We have $\pi(N+1) - \pi(N) = 0$ or $= 1$; why? What must be true of N and $N+1$ in each case?

The function $\pi(N)$ is often called the prime counting function. The PNT states that, for large N,

$$\pi(N) \sim \frac{N}{\log N},$$

where $\log N$ denotes the natural log of N. One can think of $\sim$ as meaning "approximately," but the more rigorous mathematical term is "asymptotic to." This means that

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

We can check this theorem numerically as well:

$$\begin{aligned}
\pi(10) = 4, &\quad \frac{10}{\ln(10)} = 4.343, \\
\pi(100) = 25, &\quad \frac{100}{\ln(100)} = 21.715, \\
\pi(1000) = 168, &\quad \frac{1000}{\ln(1000)} = 144.765, \\
\pi(10000) = 1229, &\quad \frac{10000}{\ln(10000)} = 1085.736, \\
\vdots &\quad \vdots \\
\pi(10^{10}) = 455,052,511, &\quad \frac{10^{10}}{\ln(10^{10})} = 434,294,481.903.
\end{aligned}$$

While the difference between the two columns tends to infinity, the ratio of the two numbers actually tends to one, albeit very slowly. For example, it has been numerically verified that

$$\frac{\pi(10^{25})}{10^{25}/\log(10^{25})} \approx 1.018.$$

Besides giving us a sense of the distribution of primes, the PNT can be used to get a probabilistic sense of where the primes are.

Exercise 5.3 Show that we can interpret the PNT as saying "the probability that a random integer between 1 and N is prime as approximately $\frac{1}{\log(N)}$."