Patterns in primes

We will discuss a number of issues related to the pattern of the sequence of primes

- First we show there are infinitely many primes
- We then discuss the Prime Number Theorem, that gives us an estimate of the number of primes up to n.
- We then consider various sequences of numbers, and examine whether they contain infinitely many numbers or not.

Reading

Section 3.3

Practice Problems

3.3 1, 2, 5, 6, 12
Challenge 3.3 (optional) 8, 11, 15, 16
Fun 3.3 17 is an interesting and alternative proof that there are infinitely many numbers

Notes

Infinitude of Primes

The standard theorem was already known by the ancient greeks:

> There are infinitely many prime numbers

- This is a perfect example for a proof by contradiction. Assume that there were only finitely many prime numbers, let's call them $p_1, p_2, \ldots, p_k$
- Before we look at the more general logic, let's consider a simpler example.
  - Say there were only 3 prime numbers, 2, 3 and 5. Can we derive a contradiction?
  - All we need to do is find a number that is not divisible by any of these 3 numbers. That number must have some prime divisor, and since it cannot be one of those 3, there must more prime numbers. Hence the contradiction.
  - In this particular case it is easy to do, for instance 7 is not divisible by any of those 3 numbers. But we want an argument we would be able to carry out in general.
  - The trick is to note that for any $n > 1$, the numbers n and $n + 1$ cannot have any prime factors in common, something we discussed some time ago.

  - So if we find a number n that is divisible by the 3 primes, then $n+1$ cannot be divisible by any of them.
  - Their product $n = 2 * 3 * 5 = 30$, is such a number. That completes the proof.

- The general proof is similar. Take the product $n = p_1 p_2 \cdots p_k$.
- Consider $n+1$. There must be a prime dividing it. And that prime cannot be any of the $p_1, \ldots, p_k$. So there must be more primes than those!

The Prime Number Theorem

Knowing there are infinitely many primes is a nice start. But *how many* primes are there? Are they somewhat rare, or is every 5th number a prime number? The proof above does not give us any indication.

For instance, the way we figured out there are more primes than $2, 3, 5$ was to say that none of them can divide $30 + 1 = 31$, so there must be some prime factor dividing 31. In fact, 31 itself is prime. But in our search for that prime number, we missed 7, 13, 17 and so on.

In order to answer this question, mathematicians often start with a definition:

> Define the function $\pi(n)$ to be the number of primes that are less than or equal to n.

For example, $\pi(10) = 4$, $\pi(20) = 8$, $\pi(30) = 10$.

Our question now becomes: What can we say about how this function grows with n?

The result goes under the name of the **Prime Number Theorem**:

> For large n, the function $\pi(n)$ is approximately equal to $\frac{n}{\log n}$.

This doesn't tell us whether a number is prime or not, but it does tell us roughly how many primes to expect. This is a very difficult theorem to prove, and we will not do so here.

Formulas

There are some standard formulas that people have come up over the years in the hopes of generating prime numbers. Here are some of these topics.

Fermat's numbers Fermat looked at the formula $F(n) = 2^{2^n} + 1$, in the hopes it would always produce prime numbers. In fact the first couple are prime numbers:

n	F(n)
1	5

n	F(n)
2	17
3	257
4	65537
5	4294967297

Fermat was able to show the first 4 of those to be prime, but the sequence grows too fast after that. Later on it was shown that $F(5)$ is in fact NOT a prime number.

Here are some open questions about Fermat numbers:

- Is F_n composite for all $n > 4$?
- Are there infinitely many Fermat primes?
- Are there infinitely many composite Fermat numbers?
- Are there any Fermat numbers that are not square-free?

Fermat primes are related to constructible regular polygons.

> The only regular n-gons that can be constructed with compass and straightedge are those where $n = 2^k p_1 \dots p_t$ where all the p_i are Fermat primes. (Gauss)

Fermat primes also have applications to the generation of pseudo-random numbers.

Dirichlet's Theorem Dirichlet asked a different question. If we look at "arithmetic" progressions, namely the sequence $an+b$ with a, b fixed and n ranging over the natural numbers, can we figure out if such a sequence can or must have infinitely many prime numbers in it?

If a, b have factors in common then it is impossible to find any primes in the sequence, as any number in it is a linear combination of a and b, so they have as factor any common factor of a and b.

However, if a and b have no factors in common, then it makes sense to ask how many primes there are in the sequence $an + b$.

Dirichlet proved not only that there are infinitely many primes in any such sequence, but also that they are more or less uniformly distributed between the different arithmetic sequences, something that we might be able to state more precisely later.

For instance, the sequences $3n + 1$ and $3n + 2$ contain infinitely many prime numbers each, and in fact each contains roughly half of the prime numbers.

Mersenne Primes A very interesting sequence of primes is known as the Mersenne Primes[1], which are numbers of the form $M(p) = 2^p - 1$.

These numbers only have a chance of being prime if p is itself a prime, so let us list some of those:

[1] http://en.wikipedia.org/wiki/Mersenne_prime

p	M(p)
2	3
3	7
5	31
7	127
11	2047
13	8191

We already see that not all of these numbers are prime. For example, $2047 = 23 \times 89$. But they are considered as good candidates for large prime numbers.

Currently we know a total of 42 Mersenne Primes, the largest of them being $2^{57,885,161} - 1$, which has 17 million digits. It would take about 4600 pages to display this number on a standard word processor.

The Great Internet Mersenne Prime Search[2] project is a massive distributed computing project constantly searching for new Mersenne numbers.

[2] http://en.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search