Lecture 8 - Some Facts About Prime Numbers

Prime numbers occupy a very special place in number theory for two primary (yeah!) reasons:

1) They form the building blocks for all natural numbers, due to the fundamental theorem of arithmetic.
2) They are still very mysterious. Even though mathematicians have been studying prime numbers since antiquity, there are still very many things we don't yet know or understand.

In this lecture we'll discuss some of the important results about primes, as well as some of the big open questions which no one has yet been able to answer.

We begin with an old result attributed to the ancient Greek mathematician Euclid.

Theorem

There are infinitely-many prime numbers

Pf

We will do a proof by contradiction, supposing there are only finitely-many primes and showing this leads to a logical contradiction.

So suppose there were only finitely-many primes, say $p_1, p_2, \ldots, p_n$. Now consider the number q defined as follows:

$$q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

By the fundamental theorem of arithmetic, q can be written as a product of the primes $p_1, \ldots, p_n$. That is, q is a multiple of some collection of these primes. Can q be a multiple of p_1? No: the way we've constructed q, $q \equiv 1 \pmod{p_1}$. But all of the multiples of p_1 are congruent to zero modulo p_1. Similarly, $q \equiv 1 \pmod{p_2}$, $q \equiv 1 \pmod{p_3}$, $\ldots$, $q \equiv 1 \pmod{p_n}$. Thus q is not a multiple of the primes $p_1, \ldots, p_n$.

Since every natural number has a (unique) prime factorization, the list of primes $p_1, \ldots, p_n$ must be incomplete.

We could repeat this argument for any finite collection of primes, and so we must conclude that every finite list of primes is incomplete, and hence there must be infinitely-many primes. □

Notice that the number q in the proof need not be prime!

Exercise

Find a finite list of primes, $p_1, p_2, \ldots, p_n$, with $n > 2$ such that $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ is not prime.

The natural numbers split into two categories: even and odd. With the exception of 2, all prime numbers are odd. It turns out, however, that we can still split the primes (other than 2) into two halves.

Even-ness and odd-ness really mean congruence classes modulo 2 with even numbers congruent to 0 (mod 2), and odd numbers congruent to 1 (mod 2).

For the primes greater than 2 we will consider congruence classes modulo 4. Every odd prime is congruent to either 1 or 3 (mod 4) — being congruent to 0 or 2 would make the number even.

Primes congruent to 1 modulo 4

5, 13, 17, 29, 37, 41, 53, 61, 73, ...

Primes congruent to 3 modulo 4

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, ...

The most obvious question to ask about these lists of primes is whether they are infinite or not. Before answering this, let's make an observation about arithmetic modulo 4.

Lemma

Let $a, b \in \mathbb{Z}$.

- If $a \equiv 1 \pmod 4$ and $b \equiv 1 \pmod 4$, then $ab \equiv 1 \pmod 4$.
- If $a \equiv 1 \pmod 4$ and $b \equiv 3 \pmod 4$, then $ab \equiv 3 \pmod 4$
- If $a \equiv 3 \pmod 4$ and $b \equiv 3 \pmod 4$, then $ab \equiv 1 \pmod 4$

Pf

This is easily verified if we recall that multiplication of congruence classes is well-defined. □

Theorem

There are infinitely-many primes congruent to 3 modulo 4.

Pf

Suppose there were only finitely-many primes congruent to 3 modulo 4 — say $p_1, p_2, \dots, p_n$. Now consider the number

$$q = 4p_1p_2\cdots p_n + 3$$

Consider the prime factorization of q — say

$$q = \pi_1 \pi_2 \cdots \pi_m$$

where each π_j is prime.

Notice at least one of $\pi_1, \dots, \pi_m$ must be congruent to 3 modulo 4. Otherwise they would all be congruent to 1 modulo 4 (Quick exercise: Why can q not be even?), but the product of numbers congruent to 1 modulo 4 gives a number which is congruent to 1 modulo 4. Thus one of the π_j is congruent to 3 modulo — say it's π_i.

Observe that π_i can not be on the original list $p_1, \dots, p_n$ because $\pi_i \mid q$, but none of $p_1, \dots, p_n$ do. □

Notice that the above proof does <u>not</u> carry over for showing there are infinitely-many primes congruent to 1 modulo 4. We can come up with a list of primes congruent to 1 modulo 4 and then consider the number $4p_1 \cdots p_n + 1$ and its factorization, but we have no guarantee this factorization must contain a prime congruent to 1 modulo 4, as we could multiply an even number of primes congruent to 3 modulo 4 and get a number congruent to 1 modulo 4.