Lecture 4 (29 May 2009)

Close Encounters with the Prime Numbers

The infinitude of primes. Have you ever played the game 'who could name the largest number"? It must have been a long time ago, since most kids discover very fast that there is no such thing as the possible largest number. You could always add one. But what about primes? What is the largest prime number? Perhaps a bit surprising, this question has two answers. There is a largest *known* prime, and currently (as of May, 2009) it is the 12,978,189 digit Mersenne prime $2^{43112609} - 1$ found in August 2008. 'Known' and 'as of now' are the key words here, because, as with natural number in general, there is no largest prime number.

The first proof of this fact, attributed to Euclid, and undeniably one of the most beautiful proofs ever, goes like this. Imagine there are only finitely many primes, say $p_1, p_2, p_3, \ldots, p_n$. Multiply them together, then add one! You get the number

$$P = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

It can't be prime, since it is definitely larger than the last existing prime, under our assumptions that's p_n. So it has to be a composite number. But every composite number has a prime factor. Indeed, consider the smallest non-trivial factor of a composite number. It is a prime number. So P has a prime factor, let's call it q. But q certainly can't be one the primes $p_1, \ldots p_n$, since P gives a remainder of 1 when divided by any of these primes, and therefore is not a multiple of any of these primes. So q must be a new prime, in contradiction with the assumption that the only primes were $p_1, p_2 \ldots, p_n$. So the assumption is wrong. There are infinitely many primes. Quod Erat Demonstrandum.

Theorems about primes. There are other statements about sequences containing infinitely many primes. For examples, there are infinitely many primes of the form $4k + 1$ and also of the form $4k + 3$. The proof of one these statements is within our reach, one only needs a slight modification of Euclid's proof. The proof of the other will be available after we learn about quadratic residues. Could you say which is which?

The number 4 is in way special here, one has the following very general result: *Dirichlet's Arithmetic Progressions Theorem:* A necessary and sufficient conditions for the sequence $a, a + d, a + 2d, \ldots, a + nd, \ldots$ to contain infinitely many primes is a and d to be relatively prime.

The primes are distributed among all natural number seemingly without any pattern, but there are results describing the statistical behaviour of primes. The most important one says that the probability that a given, randomly chosen number n is prime is proportional to its number of digits, or the logarithm of n. This statement, known as the Prime Number Theorem has been conjectured by Gauss (in a slightly different form) and proved at the end of the 19th

century independently by Hadamard (1896) and de la Valle'e Poussin (1896). Later, also independently, Erdös and Selberg give another proof, which didn't rely one anything beyond a standard course of calculus (and a lot of imagination, of course.) Riemann's hypothesis, one of the most famous and still unproven conjectures (dating from 1859) among its many consequences also implies a very precise bounds of the error terms in the Prime Number Theorem.

Conjectures about primes. Primes are essentially related to multiplication, and one could easily make observations about there behavior with respect to addition that are very difficult to prove or disprove. Two of the simplest and longstanding conjectures bear the names
The twin primes problem - are there infinitely many pairs of prime, such that the primes in each pair differ by two? ...and
Goldbach Conjecture - Every even integer greater than 2 is a sum of two primes.