Lecture 27, Oct. 31

Note. There exist arbitrary large gaps between prime numbers.

27.1 Theorem (Bertrand's postulate)**.** *For every $n \in \mathbb{Z}^+$ there is a prime p with $n < p \leq 2n$*

27.2 Theorem (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *Let $a, b \in \mathbb{Z}^+$ with $gcd(a, b) = 1$. Then there exists infinitely many primes p of the form $p = a + tb$ for some $t \in \mathbb{Z}$. In other words, there exist infinitely many primes in the sequence*

$$a, a + b, a + 2b, a + 3b, \cdots$$

27.3 Theorem (The Prime Number Theorem)**.** *For $x \in \mathbb{R}$ let $\pi(x)$ denote the number of primes p with $p \leq x$. Then*

$$\pi(x) \ \frac{x}{lnx}$$

which means that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/lnx} = 1$$

27.4 Conjecture (n^2 Conjecture)**.** For all $n \in \mathbb{Z}^+$ there exists a prime p with $n^2 < p < (n+1)^2$

27.5 Conjecture ($n^2 + 1$ Conjecture)**.** There are infinitely many primes of the form $p = n^2 + 1$ for some $n \in \mathbb{Z}$

27.6 Conjecture (Mersenne Primes Conjecture)**.** There exist infinitely many primes of the form $p = 2^n - 1$ for some $n \in \mathbb{Z}^+$ (such primes are called Mersenne Primes).

27.7 Exercise. If $2^n - 1$ is prime, then n is prime.

27.8 Conjecture (Fermat Primes Conjecture)**.** There are only finitely many primes of the form $p = 2^n + 1$ with $n \in \mathbb{Z}^+$ (such primes are called Fermat primes).

27.9 Exercise. If $2^n + 1$ is prime then $n = 2^k$ for some $k \in \mathbb{N}$

27.10 Conjecture (Twin Primes Conjecture)**.** There exist infinitely many primes p such that $p+2$ is also prime. Such primes p and $p + 2$ are called twin primes.

27.11 Conjecture (Goldbach's Conjecture)**.** Every even number $n \geq 2$ is a sum of two primes.

27.12 Theorem (Unique Prime Factorization)**.** *Every integer $n \geq 2$ can be expressed uniquely in the form*

$$n = \prod_{i=1}^{l} p_i = p_1 p_2 \cdots p_l$$

for some $l \in \mathbb{Z}^+$ and some primes $p_1, p_2, \cdots, p_l$ with $p_1 \leq p_2 \leq \cdots \leq p_l$.

Proof. First we show existence. Let $n \geq 2$. Suppose, inductively, that every integer k with $2 \leq k < n$ can be written (uniquely) in the required form. If n is prime then $n = p_1$ with $p_1 = n$.

Suppose n is composite, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Since $2 \leq a < n$ and $2 \leq n < n$ we can write

$$a = \prod_{i=1}^{l} p_i$$

and

$$b = \prod_{j=1}^{m} q_j$$

with $l, m \in \mathbb{Z}$ and the q_j, p_i are primes.

Thus

$$\begin{aligned} n =& ab \\ =& p_1 p_2 \cdots p_l q_1 q_2 \cdots q_m \\ =& r_1 r_2 \cdots r_{l+m} \end{aligned}$$

where the $(l+m)-$tuple $(r_1, r_2, \cdots, r_{l+m})$ is obtained by rearranging the entries of the

(l+m)-tuple $(p_1, p_2, \cdots, p_l, q_1, q_2, \cdots, q_m)$

into non-decreasing order.

Next we prove uniqueness. We need to show that if $n = p_1 p_2 \cdots p_l$ and $n = q_1 q_2 \cdots q_m$ where $l, m \in \mathbb{Z}^+$ and the p_i and q_j are primes with $p_1 \leq p_2 \leq \cdots \leq p_l$ and $q_1 \leq q_2 \leq \cdots q_m$, then $l = m$ and $p_i = q_i$ for all i.

Suppose $n = p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_m$ as above. Since $n = p_1 p_2 \cdots p_l$ we have $p_1 \mid n$. Since $n = q_1 q_2 \cdots q_m$ we have $p_1 \mid q_1 q_2 \cdots q_m$. It follows that $p_1 \mid q_k$ for some k with $1 \leq k \leq m$. Say $p_1 \mid q_k$. Since q_k is prime, its only positive divisors are 1 and q_k. Since $p_1 \neq 1$, so $p_1 = q_k$. Similarly, $q_1 = p_j$ for some j with $1 \leq j \leq l$. Since $p_1 = q_k \geq q_1 = p_j \geq p_1$, so we must have $p_1 = p_j = q_1$. $\square$