Elementary Number Theory
Math 17500, Section 30
Autumn Quarter 2008

Primes

Definition 0.0.1 Fix $n \in \mathbb{Z}$. An integer a is called a *divisor* of n provided that $a|n$.

Definition 0.0.2 An integer $p > 1$ is called a *prime* provided that the only positive divisors of p are 1 and p itself. An integer $n > 1$ is called *composite* if it is not prime.

Theorem 0.0.3 Every integer $n > 1$ has at least one prime factor.

Theorem 0.0.4 Every integer $n > 1$ may be factored into a product of primes.

Theorem 0.0.5 Let p be prime. If $p|ab$, then $p|a$ or $p|b$.

Theorem 0.0.6 (Fundamental Theorem of Arithmetic)
Every integer $n > 1$ may be factored into a product of primes in a unique way up to the order of the factors. In other words, there exists a uniquely determined set of primes $\{p_1, \ldots, p_k\}$ and a uniquely determined set of corresponding positive integers $\{\alpha_1, \ldots, \alpha_k\}$ such that $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$.

Theorem 0.0.7 If $a^2|b^2$, then $a|b$.

Definition 0.0.8 A real number x is defined to be *rational* if there exist integers p and q such that $q \cdot x = p$ and *irrational* otherwise.

Exercise 0.0.9 Show that if n is a positive integer that is not a perfect square (that is, there is no $a \in \mathbb{Z}$ such that $a^2 = n$), then $\sqrt{n}$ is irrational. (You do not need to show that $\sqrt{n}$ is a real number, though this is a good exercise in analysis.)

Theorem 0.0.10 There are infinitely many primes.

Exercise 0.0.11 Show that there are infinitely many primes of the form $4n + 3$.

Exercise 0.0.12 Show that if $n > 0$ is composite, then there is some prime p dividing n such that $1 < p \leq \sqrt{n}$.

Exercise 0.0.13 Suppose $n > 0$ is composite and that p is the smallest prime dividing n.
Show that if $p > \sqrt[3]{n}$, then the integer n/p is also prime.

Theorem 0.0.14 There exist arbitrarily large gaps between consecutive primes.

Definition 0.0.15 A prime number of the form $p = 2^n - 1$ is called a *Mersenne prime*.

Exercise 0.0.16 Show that if $p = 2^n - 1$ is a Mersenne prime, then n itself it prime.

Exercise 0.0.17 Find the smallest prime n for which $p = 2^n - 1$ is not a Mersenne prime.

Definition 0.0.18 A prime number of the form $p = 2^n + 1$ is called a *Fermat prime*.

Exercise 0.0.19 Show that if $p = 2^n + 1$ is a Fermat prime, then n has no odd divisors besides 1. (And hence $n = 2^k$ for some $k \geq 0$.)

Exercise 0.0.20 Show that $p = 2^{2^k} + 1$ is a Fermat prime for $k = 0, 1, 2, 3, 4$ but not for $k = 5$.