Math 2710

Sep 23-27

Prime Numbers

Definition: An integer $p > 1$ is called *prime* if its only positive divisors are 1 and p. Otherwise it is called *composite.*

Proposition: Every integer greater than 1 can be written as a product of prime numbers (including the case where the integer is a product of just one prime number.)

Lemma: Let $N > 1$ be an integer. Let $d > 1$ be the smallest divisor of N greater than 1. Then d is prime.

Proof: By contradiction. If d is not prime, it has a divisor r greater than 1 and smaller than d. Since $r|d$, and $d|N$, r is a divisor of N. (Proposition 2.1 (i)). This contradicts the fact that d is the smallest divisor of N greater than 1. Therefore d is prime.

Proof of the Proposition: Let S be the set of integers greater than one that are not a product of prime numbers. If S is not empty, it has a smallest element, Call that element N. Let d be the smallest divisor of N greater than 1. If $d = N$, then N is prime by the Lemma, so it is a product of prime numbers, which is a contraction of $N \in S$. If $d < N$, then d is a prime number by the lemma, and $N/d < N$. Since $N/d < N$\$, $N/d \notin S$, so N/d is a product of prime numbers. But then $N = d(N/d)$ so N is also a product of prime numbers. Therefore S must be empty, and every integer is a product of primes.

There are infinitely many primes

Theorem: There are infinitely many primes.

Proof: We will show that, given any prime number P, there is a prime number Q that is greater than P. Given P, let M be the product of all the prime numbers less than or equal to P, and let $H = M + 1$. Notice that if $L \leq P$ is a prime number, then $L|M$, so $L \not| H$ (Proposition 2.1(ii)). Let Q be the smallest divisor of H that is greater than 1. By the lemma, H is prime. By the preceeding remark, Q cannot be less than or equal to P. Therefore Q is a prime number greater than P, as desired.