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 contradiction 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.

Implicit in this result is an algorithm for writing N as a product of primes. Given N, start with 2 and try dividing N by 2. Do this until it's not divisible by 2 any more. Then do that by 3, and 4, and so on.

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.

% Math 2710 % Sep 23-27

Base b arithmetic

Theorem: Let $N > 0$ be an integer and let $b > 0$ be another integer. Then there exists an integer n and exactly one set of integers $r_0, \ldots, r_n$, with $r_n \neq 0$ and all $0 \leq r_i < b$, so that

$$N = r_n b^n + r_{n-1} b^{n-1} + \ldots + r_0.$$

Proof part I

Proof: One proof of this is given on pages 42-43 of the text. Here is a slightly different one. First we prove that, for every positive integer, there is at least one set $r_0, \ldots, r_n$ such that

$$N = r_n b^n + r_{n-1} b^{n-1} + \ldots + r_0.$$

Then we will show that there is only one such set. Let S be the set of positive integers for which there DO NOT exist an integer n and at least one sequence $r_0, \ldots, r_n$ as in the theorem. We will show S is empty by contradiction. So if S is not empty, by well-ordering it has a smallest element. Call that element M. By the division algorithm, we can write $M = Ab + r$ with $0 \leq r < b$. Since $A < M$, and M is the first number not of the desired form, we can write

$$A = r_m b^m + \cdots + r_0$$

But then

$$M = Ab + r = r_m b^{m+1} + \cdots + r_0 b + r$$

which *IS* of the desired form. This contradicts the assertion that S is non-empty so S must be empty.

Proof part II

To show that there is only one sequence that works, suppose we have two such sequences so that

$$N = r_n b^n + r_{n-1} b^{n-1} + \ldots + r_0.$$

and also

$$N = s_n b^n + s_{n-1} b^{n-1} + \ldots + s_0.$$

If the two representations are different, there must be a smallest integer j such that $r_j \neq s_j$. Subtracting the two representations, all of the terms involving b^i for $i < j$ would cancel out, so we would have

$$N - N = 0 = b^j (Ab + (r_j - s_j))$$

and so $Ab + (r_j - s_j) = 0$. Since b divides Ab, we must have b divides $r_j - s_j$, and since both are between 0 and b , this means $r_j - s_j = 0$. This contradicts the assumption that there was a j where r_j and s_j were different so they must all be the same

Prime numbers

Proposition: If p is prime, and p divides a product ab, then $p|a$ or $p|b$.

Proof: We know that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. In the second case, $p|a$. In the first, case, we can apply Proposition 2.28 to see that $p|b$.

Theorem: Let $N > 0$ be a positive integer. Then there is one and only one way to write N as a product of primes written in non-decreasing order.

Proof: Assume the result is false and Let N be the smallest integer that has two such representations

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_k.$$

Then $p_1 | q_1 q_2 \cdots q_k$. If $p_1 = q_1$, we could cancel p_1 from the two representations and get a smaller integer N/p_1 with two representations, so we must have $p_1 \neq q_1$. Therefore $p_1 | q_2 \cdots q_k$. By the same argument, $p_1 \neq q_2$ so $p_1 | q_3 \cdots q_k$. Continuing in this way we eventually get $p_1 | q_k$. Since $p_1 \neq 1$, we have $p_1 = q_k$. This means we can cancel $p_1 = q_k$ from the two representations to get a smaller integer with two representations; that's a contradiction since N was the smallest such. Therefore the representation is unique.

Prime factorizations, divisors, gcd, lcm

Definition: Let $\mathrm{ord}_p(n)$ be the power of p that occurs in the prime factorization of n.

Proposition: If m and n are two integers and $\mathrm{ord}_p(n) = \mathrm{ord}_p(m)$ for all primes p, then $n = \pm m$.

Proposition: If d and n are two integers, then $d|n$ if and only if $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(n)$ for all primes p.

Proposition:

- $\text{ord}_p(\gcd(a,b)) = \min(\text{ord}_p(a), \text{ord}_p(b))$ for all primes p.
- $\text{ord}_p(\gcd(a,b)) = \max(\text{ord}_p(a), \text{ord}_p(b))$ for all primes p.