# 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:**

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