Geoffrey Parker - grp352
HW 8: 2.7-2.9, 2.10-2.14, 2.19-2.21
M328K
February 14th, 2012

2.7 Theorem (Fundamental Theorem of Arithmetic-Existence Part))**.** *Every natural number greater than* 1 *is either a prime number or it can be expressed as a finite product of prime numbers. That is, for every natural number* n *greater than* 1*, there exist distinct primes* $p_1, p_2, \dots, p_m$ *and natural numbers* $r_1, r_2, \dots, r_m$ *such that*

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

Proof. Let n be a natural number greater than 1. This will be a proof by induction. As a base case, take $n = 2$. In this case, $n = 2^1$, so our theorem holds. Our induction hypothesis will be that there exists some natural number N such that $N \geq 2$ and for all integers q where $2 \leq q \leq N$, q is either prime or a finite product of primes. Now, by theorem 2.1 there exists some prime p such that $p \mid N + 1$. By the definition of divides, there exists some integer k such that $N+1 = pk$. Since $N+1 > 0$ and $p > 0$, k must also be greater than 0. So we now have two cases:
Case 1: $k = 1$. In this case, $N + 1$ is prime, so we are done.

Case 2: $k > 1$: In this case, we know that p and k are both less than $N+1$. So by our induction hypothesis k a finite product of primes. Let us say that $k = a_1^{b_1} a_2^{b_2} \cdots a_m^{b_m}$ for distinct primes $a_1, a_2, \dots a_m$ and natural numbers $b_1, b_2, \dots, b_m$. Then if there exists some j such that $p = a_j$, $N + 1 = a_1^{b_1} a_2^{b_2} \cdots a_j^{b_j+1} \cdots a_m^{b_m}$ and so $N + 1$ is a finite product of primes. If such a j does not exists, then $N + 1 = pa_1^{b_1} a_2^{b_2} \cdots a_m^{b_m}$ and $N + 1$ is a finite product of primes. □

2.8 Lemma. *Let p and $q_1, q_2, \ldots, q_n$ all be primes and let k be a natural number such that $pk = q_1 q_2 \cdots q_n$. Then $p = q_i$ for some i.*

Proof. Let p and $q_1, q_2, \ldots, q_n$ all be primes and let k be a natural number such that $pk = q_1 q_2 \cdots q_n$. Since $pk = q_1 q_2 \cdots q_n$, then by the definition of divides $p \mid q_1 q_2 \cdots q_n$. Now, for any given q_i, let k be the product of all of the rest of the q's. So $p \mid q_i k$. Then since p and q_i are prime, $(p, q_i) = 1$ unless $p = q_i$. Therefore by theorem 1.41 this implies that $p \mid k$. We can see that there must be some $q_i = p$. However, since q_i is prime, the only numbers that divide it are 1 and itself. And since p is prime, p cannot be 1. Therefore $p = q_i$. □

2.9 Theorem (Fundamental Theorem of Arithmetic-Uniqueness part). *Let* n *be a natural number. Let* $\{p_1, p_2, \ldots, p_m\}$ *and* $\{q_1, q_2, \ldots, q_s\}$ *be sets of primes with* $p_i \neq p_j$ *if* $i \neq j$ *and* $q_i \neq q_j$ *if* $i \neq j$. *Let* $\{r_1, r_2, \ldots, r_m\}$ *and* $\{t_1, t_2, \ldots, t_s\}$ *be sets of natural numbers such that*

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}. \end{aligned}$$

Then $m = s$ *and* $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_s\}$. *That is, the sets of primes are equal but their elements are not necessarily listed in the same order; that is,* p_i *may or may not equal* q_i. *Moreover, if* $p_i = q_j$ *then* $r_i = t_j$. *In other words, if we express the same natural number as a product of powers of distinct primes, then the expressions are identical except for the ordering of the factors.*

Proof. Let n be a natural number. Let $\{p_1, p_2, \ldots, p_m\}$ and $\{q_1, q_2, \ldots, q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, \ldots, r_m\}$ and $\{t_1, t_2, \ldots, t_s\}$ be sets of natural numbers such that

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}. \end{aligned}$$

Let $P = \{p_1, p_2, \ldots, p_m\}$ and let $Q = \{q_1, q_2, \ldots, q_s\}$. Now, for any integer i where $1 \leq i \leq s$, we have $n = q_i \times q_1^{t_1} q_2^{t_2} \cdots q_i^{t_i - 1} \cdots q_s^{t_s}$. If we let $k = q_1^{t_1} q_2^{t_2} \cdots q_i^{t_i - 1} \cdots q_s^{t_s}$, then k is an integer. So $q_i k = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$. By lemma 2.8,this means that $q_i = p_j$ for some j. Therefore every q is an element of P. By equivalent logic, we can show that every p is an element of Q also. Therefore $P = Q$, which implies that $m = s$, since these are the respective cardinalities of equivalent sets. Now assume by way of contradiction that for any number of pairs natural numbers $\langle i \leq m, j \leq m \rangle$ we have $p_i = q_j$ and $r_i \neq t_i$. This means that for one specific pair $\langle i_0, j_0 \rangle$ it must be that $p_{i_0}^{|r_{i_0} - t_{j_0}|}$ is equal to the product of all the terms $p_i^{|r_i - t_j|}$ for all other $\langle i, j \rangle$. That is, the difference in exponents for any one prime is balanced by the differences in the exponents of the other primes. By the same logic that we used above to show that $P = Q$, we see that p_{i_0} must be in the set of other p_i's. But each prime is unique, so this is a contradiction. Therefore if $p_i = q_j$ then $r_i = t_j$. □

2.10 Exercise. *Express $n = 12!$ as a product of primes.*

Solution.

$$12! = 12 \times 11 \times \cdots \times 1$$
$$12! = 2^2 \cdot 3 \times 11 \times 2 \cdot 5 \times 3^2 \times 2^3 \times 7 \times 2 \cdot 3 \times 5 \times 2^2 \times 3 \times 2$$
$$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$$

□

2.11 Exercise. *Determine the number of zeroes at the end of* 25!.

Solution.

$$25! = 2^{22} \cdot 3^{10} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$$
$$25! = (2^6 \cdot 5^6)(2^{16} \cdot 3^{10} \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23)$$

There are 6 zeroes at the end of 25!. □

2.12 Theorem. *Let a and b be natural numbers greater than 1 and let $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the unique prime factorization of b. Then $a \mid b$ if and only if for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $r_i \leq t_j$.*

Proof. Let a and b be natural numbers greater than 1 and let $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the unique prime factorization of b.
Now assume that $a \mid b$. In this case, by the definition of divides there must exist some integer k such that $b = ak$. Let $x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$ be the unique prime factorization of k. Because $b = ak$, there cannot exist some integer $c \leq m$ and $d \leq n$ such that $p_c \neq x_d$. So for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$. And furthermore because $a \mid b$, $a \leq b$, so it must be that $r_i \leq t_j$ since these are exponents of unique factorizations of a and b.
Now assume that for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $r_i \leq t_j$. Let k be the product of all terms $q_j^{t_j - r_i}$ where $p_i = q_j$. So now k is an integer and $b = ak$. Therefore by the definition of divides, $a \mid b$. □

2.13 Theorem. *If a and b are natural numbers and $a^2 \mid b^2$ then $a \mid b$.*

Proof. Let a and b be natural numbers with $a^2 \mid b^2$. Let $p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ be the unique prime factorization of b. Then $p_1^{2r_1}p_2^{2r_2}\cdots p_m^{2r_m}$ will be the unique prime factorization of a^2 and $q_1^{2t_1}q_2^{2t_2}\cdots q_s^{2t_s}$ will be the unique prime factorization of b^2. So by theorem 2.12, for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $2r_i \leq 2t_j$. We can see that for all such i and j, it is also true that $r_i \leq t_j$. Therefore by theorem 2.12 $a \mid b$. □

2.14 Exercise. *Find* $(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3,\ 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$.

Solution. $11^4 \cdot 17$ □

2.19 Theorem. *There do not exist natural numbers m and n such that $7m^2 = n^2$.*

Proof. Assume by way of contradiction that there exist natural numbers m and n such that $7m^2 = n^2$. Let $p_1^{r_1}p_2^{r_2}\cdots p_a^{r_k}$ be the unique prime factorization of m and let $q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ be the unique prime factorization of n. Then $7m^2 = n^2$ may be expressed as $7 \times p_1^{2r_1}p_2^{2r_2}\cdots p_a^{2r_k} = q_1^{2t_1}q_2^{2t_2}\cdots q_s^{2t_s}$. Now assume that there exists some $p_a = 7$ in the factorization of m, with r_a possibly equal to 0. Let $q_b = p_a$. So our $7m^2 = n^2$ becomes $p_1^{2r_1}p_2^{2r_2}\cdots p_a^{2r_a+1}\cdots p_a^{2r_k} = q_1^{2t_1}q_2^{2t_2}\cdots q_b^{2t_b}q_s^{2t_s}$. Since $2r_a + 1$ is odd and $2t_b$ is even, they cannot be equal, and thus we have a contradiction. □

2.20 Theorem. *There do not exist natural numbers m and n such that $24m^3 = n^3$.*

Proof. Assume by way of contradiction that there exist natural numbers m and n such that $24m^3 = n^3$. Let $p_1^{r_1}p_2^{r_2}\cdots p_a^{r_k}$ be the unique prime factorization of m and let $q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ be the unique prime factorization of n. Then $24m^3 = n^3$ may be expressed as $2^3 3 \times p_1^{3r_1}p_2^{3r_2}\cdots p_a^{3r_k} = q_1^{3t_1}q_2^{3t_2}\cdots q_s^{3t_s}$. Now assume that there exists some $p_a = 3$ in the factorization of m, with r_a possibly equal to 0. Let $q_b = p_a$. So our $24m^3 = n^3$ becomes $p_1^{3r_1}p_3^{2r_2}\cdots p_a^{3r_a+1}\cdots p_a^{3r_k} = q_1^{3t_1}q_2^{3t_2}\cdots q_b^{3t_b}q_s^{3t_s}$. Since $3 \nmid r_a + 1$ and $3 \mid 3t_b$, they cannot be equal, and thus we have a contradiction. □

2.21 Exercise. *Show that $\sqrt{7}$ is irrational. That is, there do not exist natural numbers n and m such that $\sqrt{7} = \frac{n}{m}$.*

Solution. Assume by way of contradiction that there exist natural numbers n and m such that $\sqrt{7} = \frac{n}{m}$. Then $m\sqrt{7} = n$ and $(m\sqrt{7})^2 = n^2$, so $7m^2 = n^2$. However, this contradicts theorem 2.19, so $\sqrt{7}$ must be irrational. □