Geoffrey Parker
HW 7: 2.1-2.5, 2.7-2.9
M328K
February 9th, 2012

2.1 Theorem. *If n is a natural number greater than 1, then there exists a prime p such that $p|n$.*

Proof. Let n be a natural number greater than 1. We will show that there exists a prime p such that $p \mid n$. This will be a proof by induction. As our base case, take $n = 2$. Since n is prime, let $p = n$, and so p is prime and $p \mid n$. Our induction hypothesis is that there exists some natural number $N > 1$ such that for all q such that $1 < q <= N$, there exists a p such that p is prime and $p \mid q$. Now consider two cases:

Case 1: For all integers x, such that $1 < x \leq N$, $x \nmid N + 1$. In this case, because there are no integers other than 1 and itself that divide $N + 1$, $N + 1$ is prime. Simply let $p = N + 1$ and now $p \mid N + 1$ and p is prime.

Case 2: There exists some integer x such that $1 < x \leq N$ and $x \mid N + 1$. In this case, by the induction hypothesis there is some prime p such that $p \mid x$. Since $p \mid x$ and $x \mid N + 1$, then $p \mid N + 1$. □

2.2 Exercise. *Write down the primes less than 100 without the aid of a calculator or a table of primes and think about how you decide whether each number you select is prime or not.*

Solution. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.
Wrote down all the primes up to 41 simply by considering whether each odd number has a divisor other than 1 or itself. After 41, this got hard, so I did the Sieve of Eratosthenes on a piece of paper. □

2.3 Theorem. *A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.*

Proof. Consider a natural number $n > 1$. We will show that n is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n. Since this is an if and only if statement, this will be a two stage proof.

First, assume for all primes $p \leq \sqrt{n}$, p does not divide n. Assume by way of contradiction that n is composite. This means that there must be natural numbers i_0 and j_0 greater than 1 and less than n such that $n = i_0 j_0$ and there is no prime that divides either i_0 or j_0. Since $n = i_0 j_0$, either i_0 or j_0 must be less than or equal to $\sqrt{n}$. So assume without loss of generality that $i_0 \leq \sqrt{n}$. Now we can repeat this argument to find some integers i_1 and j_1 such that $i_0 = i_1 j_1$ and $1 < i_1 \leq \sqrt{i_0}$. We can see that this sequence of i's is approaching the minimal value, which is 2. However, this is a contradiction, because each i divides n and there is no prime that divides n and 2 is prime. Therefore n must be prime.

Now, assume that n is prime. Since n is prime, there are no numbers q such that $q \mid n$ unless q is 1 or n. Therefore for all primes $p \leq \sqrt{n}$, p does not divide n. □

2.4 Exercise. *Use the preceding theorem to verify that* 101 *is prime.*

Solution. First, $10 < \sqrt{101} < 11$. The primes less than 11 are: 2, 3, 5, 7. So we can see that for all p in $\{2, 3, 5, 7\}$, $p \nmid 101$. Therefore by theorem 2.3 101 is prime. □

2.5 Exercise (Sieve of Eratosthenes)**.** *Write down all the natural numbers from* 1 *to* 100*, perhaps on a* 10×10 *array. Circle the number* 2*, the smallest prime. Cross off all numbers divisible by* 2*. Circle* 3*, the next number that is not crossed out. Cross off all larger numbers that are divisible by* 3*. Continue to circle the smallest number that is not crossed out and cross out its multiples. Repeat. Why are the circled numbers all the primes less than* 100*?*

Solution.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Circled: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

The circled numbers are prime because all the numbers that are divided by primes less than 10 are crossed out. By theorem 2.3, this means that the crossed out numbers are not prime and the ones left are. □

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* $p_1, p_2, \ldots, p_m$ *and natural numbers* $r_1, r_2, \ldots, r_m$ *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 $a_1, a_2, \ldots a_m$ and natural numbers $b_1, b_2, \ldots, b_m$. 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 $N+1 = p a_1^{b_1} a_2^{b_2} \cdots a_m^{b_m}$ 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 $p \mid q_1 q_2 \cdots q_n$. This in turn implies that there exists some i such that $p \mid q_i$. 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 multiplicitve reduction of $p_i^{|r_i - t_j|}$ 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 $r_i = t_j$. □