1.3 Primes and Unique Factorization

Definition. An integer $p > 1$ is *prime* if its only positive divisors are 1 and p. An integer $n > 1$ that is not prime is called *composite.*

Note. Our textbook does not require that primes be positive. Under the book's definition, if p is a prime, then $-p$ also counts as a prime. This is not the standard definition, so I will not be using it in this course.[1]

Example. The first few primes are $2, 3, 5, 7, 11, 13$. Note that 9 is composite, because 3 is a divisor of 9. Also, 91 is composite, because 7 is a divisor of 91.

Theorem. *Every integer $n > 1$ is divisible by a prime.*

Proof. Assume otherwise that there exists an integer greater than 1 that is not divisible by a prime. Let n be the smallest such integer. Since n is not divisible by a prime, n cannot be prime itself. Therefore it has a positive divisor a $a \neq 1, n$. Thus $a < n$, so the definition of n ensures that a has a prime divisor p. Since $p \mid a$ and $a \mid n$, it follows that $p \mid n$, which is a contradiction. □

How can we tell whether a given integer $n > 1$ is prime?[2] By definition, n is prime if it is not divisible by any of $2, 3, \ldots, n-1$. But we don't want to have to perform $n-2$ trial divisions; that will be extremely time-consuming if n is large. Fortunately, the following theorem shows that we don't need that many; the only divisors we need to test are primes less than $\sqrt{n}$.

Theorem. *Let n be an integer greater than 1. If n has no prime divisors $\leq \sqrt{n}$, then n is prime.*

Proof. We prove the contrapositive: if n is composite, then n has a prime divisor $\leq \sqrt{n}$. Since n is composite, $n = ab$ for some a, b with $1 < a \leq b < n$. Thus $a^2 \leq ab = n$, so $a \leq \sqrt{n}$. Let p be any prime divisor of a; then p is a prime divisor of n with $p \leq a \leq \sqrt{n}$, as desired. □

Example. Is 97 prime? By the theorem, we need only test the primes $\leq \sqrt{97} \approx 9.84$. These primes are 2, 3, 5, 7. It is easy to check that 97 is not divisible by any of these four numbers, so 97 is prime.

[1] The advantage of the book's definition is that it is consistent with how we will define primes in other rings later, whereas the standard definition is not. But in practice, this inconsistency causes no confusion.

[2] This is a very important and difficult question; the answer we will give here has the virtue of being straightforward, but is not remotely the fastest way to test whether n is prime when n is large.

Theorem. *There are infinitely many primes.*

Proof. Assume for the sake of contradiction that there were only finitely many primes $p_1, \dots, p_k$. Let $Q = p_1 p_2 \dots p_k + 1$. Then Q is not divisible by any p_i. (In fact, the remainder when Q is divided by p_i is 1.) This is a contradiction, since Q must be divisible by a prime. □

We now give an alternate definition of prime. The theorem is useful now, and will also be instructive when we get to ring theory.

Theorem. *An integer $p > 1$ is prime if and only if it has the following property:*

$$\textit{If } p \mid bc, \textit{ then } p \mid b \textit{ or } p \mid c.$$

Proof. First suppose p is prime. Suppose $b, c \in \mathbb{Z}$ such that $p \mid bc$. Since p is prime, (p, b) is either 1 or p. If $(p, b) = p$, then $p \mid b$ and we are done. If $(p, b) = 1$, then the fact that $p \mid bc$ implies $p \mid c$ (by a theorem from the previous section).

Now suppose p has the property. We know that p has a prime divisor q, so $p = qn$ for some integer n. Therefore $p \mid qn$, so $p \mid q$ or $p \mid n$. Note that $n = p/q < p$, so $p \nmid n$. Therefore $p \mid q$. The only divisor of q that is greater than 1 is q itself, so $p = q$, which proves p is prime. □

Corollary. *If p is prime and $p \mid a_1 a_2, \dots a_r$, then p divides at least one of the a_i.*

Proof. The proof is by induction on r. The case $r = 1$ is trivial, and the case $r = 2$ is the previous theorem. Now suppose $r \geq 3$, and assume the theorem holds for $r - 1$ factors. Since $p \mid (a_1 a_2 \dots a_{r-1}) a_r$, the previous theorem says that $p \mid a_1 a_2 \dots a_{r-1}$ or $p \mid a_r$. If $p \mid a_r$, we are done; if $p \mid a_1 a_2 \dots a_{r-1}$, then by induction p divides one of $a_1, \dots, a_{r-1}$, and we are again done. □

The Fundamental Theorem of Arithmetic

The following theorem is half of the Fundamental Theorem of Arithmetic.

Theorem. *Every positive integer can be written as a product of primes.*[3]

Proof. The proof is by induction; we assume the theorem is true for $1, 2, \dots, n - 1$ and prove it for n. If n is itself prime, we are done. Otherwise, $n = ab$ for some integers $1 < a, b < n$. By assumption, a and b are products of primes, so n is also. □

The other half of the Fundamental Theorem of Arithmetic is the observation that an integer essentially has only one prime factorization. For example, try factoring 60 multiple ways, such as $60 = 2 \cdot 2 \cdot 3 \cdot 5$ or $60 = 2 \cdot 3 \cdot 5 \cdot 2$. You'll find that the prime factors are always $2, 2, 3, 5$; the only difference is the order of the factors. The FTA says that this is always the case:

[3] We consider 1 to be an empty product of primes, i.e., a product of no primes.

Theorem. ***(Fundamental Theorem of Arithmetic)*** *Every positive integer n is a product of primes. This product is unique up to order.*

Proof. We have already seen that n is a product of primes. We prove uniqueness by induction on n; assume the theorem is true for all positive integers $< n$.

Suppose n has two prime factorizations:

$$n = p_1 \dots p_r \quad \text{and} \quad n = q_1 \dots q_s.$$

We want to prove that $p_1, \dots, p_r$ and $q_1, \dots, q_s$ are the same primes, possibly in a different order.

Since $p_1 \mid n = q_1 \dots q_s$, we know that p_1 divides one of the q_i. Rearranging the q_i, we may assume $p_1 \mid q_1$. Since p_1 and q_1 are both prime, it follows that $p_1 = q_1$. Therefore

$$\frac{n}{p_1} = p_2 \dots p_r = q_2 \dots q_s.$$

By the induction hypothesis, n/p_1 has a unique prime factorization, so $p_2, \dots, p_r$ and $q_2, \dots, q_s$ are the same primes in some order. This completes the proof. □