4.3 Primes

Definition 1. *A prime is an integer greater than 1 that is divisible by no positive integers other than 1 and itself. An integer greater than 1 that is not prime is called composite.*

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.*

Theorem 2. *If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.*

Proof. If n is composite, by the definition of a composite integer, we know that n has a factor a with $1 < a < n$. Hence, by the definition of a composite integer, we have $n = ab$, where b is an integer greater than 1. We will show that $a \leqslant \sqrt{n}$ or $b \leqslant \sqrt{n}$. If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. Consequently, $a \leqslant \sqrt{n}$ or $b \leqslant \sqrt{n}$. Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$. □

Example 1. *To check whether* 91 *is prime, we need only check the divisibility of* 91 *by primes less than or equal to* $\sqrt{91}$*. Since* $\sqrt{91} < \sqrt{100} = 10$*, we just check the divisibility of* 91 *by the primes* $2, 3, 5$*, and* 7*.* 91 *is odd, so* 91 *is not divisible by* 2*. Since the sum of digits of* 91 *(*$= 9 + 1 = 10$*) is not a multiple of* 3*,* 91 *is not divisible by* 3*. Since* 91 *does not have a units digit of* 0 *or* 5*,* 91 *is not divisible by* 5*. However,* $91 = 7 \cdot 13$*. Thus* 91 *is composite. Similarly, we can establish that* 97 *is prime.*

Theorem 3. *There are infinitely many primes.*

The following proof is one of the most beautiful proofs in mathematics.

Proof. We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, namely $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 p_2 \cdots p_n + 1.$$

By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes. However, none of the primes p_j divides Q, for if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1$. Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes. □

Definition 2. *Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by* $\gcd(a, b)$.

Definition 3. *The integers a and b are relatively prime if their greatest common divisor is* 1.

Definition 4. *The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if* $\gcd(a_i, a_j) = 1$ *whenever* $1 \leqslant i < j \leqslant n$.

Definition 5. *The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by* $\operatorname{lcm}(a, b)$.

Remark 1. *One way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers a and b are*

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\gcd(a,b)$ *is given by*

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

where $\min(x,y)$ *represents the minimum of the two numbers x and y. Similarly, the least common multiple of a and b is given by*

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

where $\max(x,y)$ *represents the maximum of the two numbers x and y.*

Theorem 4. *If $a, b \in \mathbb{Z}^+$, then*

$$ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

Lemma 1. *Let $a = bq + r$, where a, b, q, and r are integers. Then* $\gcd(a,b) = \gcd(b,r)$.

Proof. If we can show that the common divisors of a and b are the same as the common divisors of b and r, we will have shown that $\gcd(a,b) = gcd(b,r)$, because both pairs must have the same greatest common divisor. So suppose that d divides both a and b. Then it follows that d also divides $a - bq = r$ (from Theorem 1 of Section 4.1). Hence, any common divisor of a and b is also a common divisor of b and r. Likewise, suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r is also a common divisor of a and b. Consequently, $\gcd(a,b) = \gcd(b,r)$. □

The Euclidean Algorithm Using the above lemma, we successively divide and record the remainder, then divide the previous divisor by the previous remainder, until we reach a remainder of zero. The last nonzero remainder is the greatest common divisor.

Example 2. *Find the greatest common divisor of* 312 *and* 84 *using the Euclidean algorithm.*

Solution. Successive uses of the division algorithm give:

$$\begin{aligned} 312 &= 3 \cdot 84 + 60 \\ 84 &= 1 \cdot 60 + 24 \\ 60 &= 2 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0 \end{aligned}$$

Hence, $\gcd(312, 84) = 12$, because 12 is the last nonzero remainder. □

Theorem 5 (Bézout's Theorem)**.** *If a and b are positive integers, then there exist integers s and t such that* $\gcd(a,b) = sa + tb$.

Remark 2. *We may find numbers s and t by tracing back the steps in the Euclidean algorithm.*

Example 3. *In the previous example, we found that* $\gcd(312, 84) = 12$. *We may write* 12 *as a linear combination of* 312 *and* 84*, starting from the next to last step in the Euclidean algorithm, and going back,*

as follows:

$$\begin{aligned}
60 &= 2 \cdot 24 + 12 \\
\therefore 60 - 2 \cdot 24 &= 12 \\
84 &= 1 \cdot 60 + 24 \\
\therefore 84 - 1 \cdot 60 &= 24 \\
\therefore 60 - 2 \cdot (84 - 1 \cdot 60) &= 12 \\
\therefore 60 - 2 \cdot 84 + 2 \cdot 60 &= 12 \\
\therefore 3 \cdot 60 - 2 \cdot 84 &= 12 \\
312 &= 3 \cdot 84 + 60 \\
\therefore 312 - 3 \cdot 84 &= 60 \\
\therefore 3 \cdot (312 - 3 \cdot 84) - 2 \cdot 84 &= 12 \\
\therefore 3 \cdot 312 - 9 \cdot 84 - 2 \cdot 84 &= 12 \\
\therefore 3 \cdot 312 - 11 \cdot 84 &= 12
\end{aligned}$$

Lemma 2. *If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

Proof. Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that

$$sa + tb = 1.$$

Multiplying both sides of this equation by c, we obtain

$$sac + tbc = c.$$

We can now use Theorem 1 of Section 4.1 to show that $a \mid c$. By part (ii) of that theorem, since $a \mid bc$ (given in this lemma), $a \mid tbc$. Because $a \mid sac$ and $a \mid tbc$, by part (i) of that theorem, we conclude that a divides $sac + tbc$. Because $sac + tbc = c$, we conclude that $a \mid c$, completing the proof. □

Corollary. *If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.*

We can now show that a factorization of an integer into primes is unique. That is, we will show that every integer can be written as the product of primes in nondecreasing order in at most one way. This is part of the fundamental theorem of arithmetic. We will prove the other part, that every integer has a factorization into primes, in Section 5.2.

Proof (of the uniqueness of the prime factorization of a positive integer): We will use a proof by contradiction. Suppose that the positive integer n can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, each p_i and q_j are primes such that $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_s$ and $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_t$. When we remove all common primes from the two factorizations, we have

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v},$$

where no prime occurs on both sides of this equation and u and v are positive integers. By the above Corollary, it follows that p_{i_1} divides q_{j_k} for some k. Because no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of n into primes in nondecreasing order. □

We have seen (Theorem 5 in §4.1) that we can multiply both sides of a congruence by the same integer. However, dividing both sides of a congruence by an integer does not always produce a valid congruence, as the following example shows.

Example 4. *We observe that $14 \equiv 8 \pmod 6$. However, if we divide both sides of this congruence by 2, we end up with an incorrect congruence: $7 \not\equiv 4 \pmod 6$.*

Although we cannot divide both sides of a congruence by any integer to produce a valid congruence, we can if this integer is relatively prime to the modulus.

Theorem 6. *Let m be a positive integer and let a, b, and c be integers.*
If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof. Because $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$. By Lemma 2, because $\gcd(c, m) = 1$, it follows that $m \mid a - b$. We conclude that $a \equiv b \pmod{m}$. □