3.1 THE FUNDAMENTAL THEOREM OF ARITHMETIC

Essential to everything discussed herein—in fact, essential to every aspect of number theory—is the notion of a prime number. We have previously observed that any integer $a > 1$ is divisible by ± 1 and $\pm a$; if these exhaust the divisors of a, then it is said to be a prime number. Put somewhat differently:

DEFINITION 3-1. An integer $p > 1$ is called a *prime number*, or simply a *prime*, if its only positive divisors are 1 and p. An integer greater than 1 which is not a prime is termed *composite*.

Among the first ten positive integers 2, 3, 5, 7 are all primes, while 4, 6, 8, 9, 10 are composite numbers. Note that the integer 2 is the only even prime, and according to our definition the integer 1 plays a special role, being neither prime nor composite.

For the rest of the book, the letters p and q will be reserved, so far as is possible, for primes.

Proposition 14 of Book IX of Euclid's *Elements* embodies the result which later became known as the Fundamental Theorem of Arithmetic, namely, that every integer greater than 1 can, except for the order of the factors, be represented as a product of primes in one and only one way. To quote the proposition itself: "If a number be the least that is measured by prime numbers, it will not be measured by any other prime except those originally measuring it." Since every number is either a prime or, by the Fundamental Theorem, can be broken down into unique prime factors and no further, the primes serve as the "building blocks" from which all other integers can be made. Accordingly, the prime numbers have intrigued mathematicians through the ages, and while a number of remarkable theorems relating to their distribution in the sequence of positive integers have been proved, even more remarkable is what remains unproved. The open questions can be counted among the outstanding unsolved problems of all mathematics.

To begin on a simpler note, we observe that the prime 3 divides the integer 36, where 36 may be written as any one of the products

$$6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2.$$

In each instance, 3 divides at least one of the factors involved in the product. This is typical of the general situation, the precise result being:

THEOREM 3-1. *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof: If $p \mid a$, then we need go no further, so let us assume that $p \nmid a$. Since the only positive divisors of p are 1 and p itself, this implies that $\gcd(p, a) = 1$. (In general $\gcd(p, a) = p$ or $\gcd(p, a) = 1$ according as $p \mid a$ or $p \nmid a$.) Hence, citing Euclid's Lemma, we get $p \mid b$.

This theorem easily extends to products of more than two terms.

COROLLARY 1. *If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k, where $1 \leq k \leq n$.*

Proof: We proceed by induction on n, the number of factors. When $n = 1$, the stated conclusion obviously holds, while for $n = 2$ the result is the content of Theorem 3-1. Suppose, as the induction hypothesis, that $n > 2$ and that whenever p divides a product of less than n factors, then it divides at least one of the factors. Now, let $p \mid a_1 a_2 \cdots a_n$. By Theorem 3-1, either $p \mid a_n$ or else $p \mid a_1 a_2 \cdots a_{n-1}$. If $p \mid a_n$, then we are through. As regards the case $p \mid a_1 a_2 \cdots a_{n-1}$, the induction hypothesis ensures that $p \mid a_k$ for some choice of k, with $1 \leq k \leq n - 1$. In any event, p divides one of the integers $a_1, a_2, \ldots, a_n$.

COROLLARY 2. *If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.*

Proof: By virtue of Corollary 1, we know that $p \mid q_k$ for some k, with $1 \leq k \leq n$. Being a prime, q_k is not divisible by any positive integer other than 1 or q_k itself. Since $p > 1$, we are forced to conclude that $p = q_k$.

With this preparation out of the way, we arrive at one of the cornerstones of our development, the Fundamental Theorem of Arithmetic. As indicated earlier, this theorem asserts that every integer

greater than 1 can be factored into primes in essentially one way; the linguistic ambiguity "essentially" means that $2 \cdot 3 \cdot 2$ is not considered as being a different factorization of 12 from $2 \cdot 2 \cdot 3$. Stated precisely:

THEOREM 3-2 (Fundamental Theorem of Arithmetic). *Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.*

Proof: Either n is a prime or it is composite; in the former case, there is nothing more to prove. If n is composite, then there exists an integer d satisfying $d \mid n$ and $1 < d < n$. Among all such integers d choose p_1 to be the smallest (this is possible by the Well-Ordering Principle). Then p_1 must be a prime number. Otherwise, it too would have a divisor q with $1 < q < p_1$; but then $q \mid p_1$ and $p_1 \mid n$ imply that $q \mid n$, which contradicts the choice of p_1 as the smallest divisor, not equal to 1, of n.

We may therefore write $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2 n_2$; that is,

$$n = p_1 p_2 n_2, \qquad 1 < n_2 < n_1.$$

If n_2 is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3 n_3$, with p_3 a prime:

$$n = p_1 p_2 p_3 n_3, \qquad 1 < n_3 < n_2.$$

The decreasing sequence

$$n > n_1 > n_2 > \cdots > 1$$

cannot continue indefinitely, so that after a finite number of steps n_{k-1} is a prime, say p_k. This leads to the prime factorization

$$n = p_1 p_2 \cdots p_k.$$

To establish the second part of the proof—the uniqueness of the prime factorization—let us suppose that the integer n can be represented as a product of primes in two ways; say

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s, \qquad r \leq s$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \leq p_2 \leq \cdots \leq p_r, \; q_1 \leq q_2 \leq \cdots \leq q_s.$$

Since $p_1 \mid q_1 q_2 \cdots q_s$, Corollary 2 of Theorem 3-1 tells us that $p_1 = q_k$ for some k; but then $p_1 \geq q_1$. Similar reasoning gives $q_1 \geq p_1$, whence $p_1 = q_1$. We may cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Now repeat the process to get $p_2 = q_2$ and, in its turn,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

Continue in this fashion. If the inequality $r < s$ held, we would eventually arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

which is absurd, since each $q_i > 1$. Hence $r = s$ and

$$p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r,$$

making the two factorizations of n identical. The proof is now complete.

Of course, several of the primes which appear in the factorization of a given positive integer may be repeated as is the case with $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. By collecting like primes and replacing them by a single factor, we could rephrase Theorem 3-2 as

COROLLARY. *Any positive integer $n > 1$ can be written uniquely in a* canonical form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where, for $i = 1, 2, \ldots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.

To illustrate: the canonical form of the integer 360 is $360 = 2^3 \cdot 3^2 \cdot 5$. As further examples we cite

$$4725 = 3^3 \cdot 5^2 \cdot 7, \quad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2.$$

Theorem 3-2 should not be taken lightly, for there do exist number systems in which the factorization into "primes" is not unique. Perhaps the most elemental example is the set E of all positive even integers. Let us agree to call an even integer an e-prime if it is not the product of two other even integers. Thus, 2, 6, 10, 14, ... are all e-primes