Prime Numbers

DEFINITION: A **prime** is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

EXAMPLE: The numbers $2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47$ are prime.

DEFINITION: A positive integer which is not prime, and which is not equal to 1, is called **composite**.

EXAMPLE:

1. The number 1 is neither prime nor composite.
2. The integers

$$4 = 2 \cdot 2, \quad 8 = 4 \cdot 2, \quad 33 = 3 \cdot 11, \quad 111 = 3 \cdot 37, \quad 1001 = 7 \cdot 11 \cdot 13$$

are composite.

LEMMA: Every positive integer greater than 1 has a prime divisor.

Proof: We prove the lemma by contradiction; we assume that there is a positive integer > 1 having no prime divisors. Then, since the set of positive integers > 1 with no prime divisors is non-empty, the well-ordering property tells us that there is a least positive integer n greater than 1 with no prime divisors. Since n has no prime divisors and n divides n, we see that n is not prime. Hence, we can write $n = ab$ with $1 < a < n$ and $1 < b < n$. Because $a < n$, a must have a prime divisor. By Theorem 1 from Section 1.5, any divisor of a is also a divisor of n, so that n must have a prime divisor, contradicting the fact that n has no prime divisors. We can conclude that every positive integer has at least one prime divisor. ■

THEOREM 1: There are infinitely many primes.

Proof: Suppose that there are only finitely many prime numbers,

$$p_1,\ p_2, \ldots, p_n \tag{1}$$

where n is a positive integer. Consider the integer

$$Q_n = p_1 p_2 \ldots p_n + 1 \tag{2}$$

By the Lemma above, Q_n has at least one prime divisor, say, q. Since all the prime numbers are listed in (1), it follows that $q = p_j$ for some integer j with $1 \le j \le n$. Rewrite (2) as

$$Q_n - p_1 p_2 \ldots p_n = 1 \tag{3}$$

Since p_j divides Q_n and $p_1 p_2 \ldots p_n$, it divides $Q_n - p_1 p_2 \ldots p_n$ by Theorem 2 from Section 1.5. From this and (3) it follows that p_j divides 1. This is impossible, since no prime divides 1. This contradiction shows that there are infinitely many primes. ■

THEOREM 2: If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.

Proof: Since n is composite, we can write $n = ab$, where a and b are integers with

$$1 < a \leq b < n$$

We must have $a \leq \sqrt{n}$, since otherwise

$$b \geq a > \sqrt{n}$$

and

$$ab > \sqrt{n} \cdot \sqrt{n} = n$$

Now, by the Lemma above, a must have a prime divisor, which by Theorem 1 from Section 1.5 is also a divisor of n and which is clearly less than or equal to $\sqrt{n}$.