**3 .1 .1 Divisibility**

Number theory is concerned with the properties of the integers. One of the most important is divisibility.

**Definition .** Let a and b be integers with . We say that a divides b, if there is an integer k such that b = ak. This is denoted by a|b. Another way to express this is that b is a multiple of a.

**Examples.** 3|15, —15|60, 7 f 18 (does not divide).

The following properties of divisibility are useful.

Proposition . Let a,b,c represent integers.

1. For every , and . Also, 1|b for every b.
2. If and , then .
3. I f and , then for all integers s and t;

Proof. Since ,we may take in the definition to obtain .

Since , we take to prove . Since , we have . This proves (1). In(2), there exist and such that and Therefore, , so . For (3), write and . Then , so .

For example, take in part (2). Then simply means that b is even. The statem ent in the proposition says that c, which is a multiple of the even number b, must also be even (that is, a multiple of ).

**3 .1 .2 Prime Numbers**

A number that is divisible only by 1 and itself is called a **prime number**. The first few primes are 2,3,5,7,11,13,17,. An integer that is not prime is called **composite**, which means that n must expressible as a product of integers with , . A fact, known already to Euclid, is that there are infinitely many prime numbers. A more precise statement is the following, proved in 1896.

**Prime Number Theorem** . Let be the number of primes less tha x. Then

In the sense that ratio

We won't prove this here; its proof would lead us too far away from our cryptographic goals. In various applications, we'll need large primes, say of around 100 digits. We can estimate the number of 100-digit primes as follows:

So there are certainly enough such primes. Later, we’ll discuss how to find them.

Prime numbers are the building blocks of the integers. Every positive integer has a unique representation as a product of prime numbers raised to different powers. For example, 504 and 1125 have the following factorizations

504 = 23327, 1125 = 3253.

Moreover, these factorizations are unique, except for reordering the factors. For example, if we factor 504 into primes, then we will always obtain- three factors of 2, two factors of 3, and one factor of 7. Anyone who obtains the prime 41 as a factor has made a mistake.

**Theorem** . Every positive integer is a product of primes. This factorization into primes is unique, up to reordering the factors.

*Proof*. There ia a small technicality that must be dealt with before we begin. When dealing with products, it is convenient to make the convention that an empty product equals 1. This is similar to the convention that . Therefore, the positive integer 1 is a product of primes, namely the empty product. Also, each prime is regarded as a one factor product of primes.

Suppose there exist positive integers that are not products of primes. Let n be the smallest such integer. Then n cannot be 1 (= the empty product), or a prime {= a one factor product), so n must be composite. Therefore, with ,. Since n is the smallest positive integer that is not a product of primes, both a and b are products of primes. But a product of primes times a product of primes is a product of primes, so is a product of primes. This contradiction shows that the set of integers that are not products of primes must be the empty set. Therefore, every positive integer is a product of primes.

The uniqueness of the factorization is more difficult to prove. We need the following very important property of primes.

**Lemma** . If p is a prime and p divides a product of integers ab, then either or . More generally, if a prime p divides a product ab z, then p must divide one of the factors a ,b ,... ,z.

For example, when , this says that if a product of two integers is even then one of the two integers must be even. The proof of the lemma will be given at the end of this section, after we discuss the Euclidean algorithm.

Continuing with the proof of the theorem, suppose th at an integer n can be written as a product of primes in two different ways;

n = pa1Y 21 ---Ps’ = < 7 ^

where p i, . . . , ps and qi, . , . , qt are primes, and the exponents a,- and bj are nonzero. If a prime occurs in both factorizations, divide both sides by it to obtain a shorter relation. Continuing in this way, vve may assume that none of the primes p i, . .. ,ps Occur among the qj's. Take a prime that occurs on the left side, say p \. Since p t divides n, which equals , the lemma says that p1 must divide one of the factors qj. Since qj is prime, . This contradicts the assumption that pi does not occur among the qj’s. Therefore, an integer cannot have two distinct factorizations, as claimed.