Number Theory

Jacob Denson

July 17, 2016

Table Of Contents

Chapter 1

The Prime Numbers

Number theory is the study of the positive integers, those numbers you know as

$$1, 2, 3, \ldots$$

The most basic relation between these numbers is that of divisibility. An integer a is divisible by b, denoted $b \mid a$, if there is a number n for which $nb = a$. Any number n has divisors 1 and itself. Of particular interest are the primes, integers greater than 1, whose divisors consist of only itself and one. The composite numbers are those that are not prime. It is of great importance that one may 'compose' prime numbers to form composites.

Theorem 1.1. *Every integer can be written as a product of prime numbers.*

Proof. If n is a prime number, then it can obviously be written as a prime. Otherwise, we may write $n = ab$, for $1 < a, b < n$. Continuing this expansion process, we may continue to expand a and b as a product of smaller numbers. Eventually these smaller numbers must be prime, for otherwise we would have an infinite decreasing chain of positive integers, of which we know the impossibility. Thus we have prime decompositions $a = p_1 p_2 \ldots p_n$, and $b = q_1 q_2 \ldots q_m$, and then $n = p_1 \ldots p_n q_1 \ldots q_m$. □

An interesting fact to notice is that if $n = ab$, then either $a < \sqrt{n}$ or $b < \sqrt{n}$. Thus every composite number is divisible by a prime number smaller than the composite's square root. This leads to a simple procedure for finding all primes up to a certain number M. We first write down the integers

$$2, 3, 4, \ldots$$

and cross off all numbers divisible by 2 (all even numbers). We end up with the list

$$3, 5, 7, 9, 11, \ldots$$

Now we cross off all numbers divisible by 3. Any number which eventually ends up at the beginning of the queue must be prime, for it is not divisible by a prime smaller than it. If we continue to cross of numbers divisible by the first primes, we will find all primes. We may stop once we reach an integer bigger than $\sqrt{M}$, for if a number has not been crossed off at this point, it must be prime. The number of operations to perform this procedure is propotional to $O(M\pi(\sqrt{M}))$, where $\pi(n)$ counts the number of primes less than or equal to n. We will eventually show that $\pi(n)$ converges to $n/\log(n)$, so that our algorithm is $O(M^{3/2}/\log(M))$

The primes in an expansion are not necessarily distinct, nor in a particular order. We say a decomposition

$$p_1^{n_1} \ldots p_m^{n_m}$$

is in standard form if $p_1 < p_2 < \cdots < p_m$. A simple question is whether a decomposition in standard form is unique? This composes exactly what is commonly known as the fundamental theorem of arithmetic.

Theorem 1.2. *Every integer has a unique decomposition in standard form.*

Proof. We shall rely on a useful property, to be proved later. If p is prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$. Now suppose that

$$p_1^{n_1} \ldots p_m^{n_m} = q_1^{k_1} \ldots p_l^{k_l}$$

Now $p_i \mid q_1^{k_1} \ldots q_l^{k_l}$ for each i, so $p_i \mid q_j$ for some j, hence $p_i = q_j$. Since the p_i are distinct, the q_j must also be distinct, so $m \leqslant l$. By symmetry (for we may perform the same technique with the q_i), $m = l$. For each i, we must have $n_i = k_i$, for if $n_i < k_i$, we may write

$$p_1^{n_1} \ldots p_i^0 \ldots p_m^{n_m} = p_1^{k_1} \ldots p_i^{k_i - n_i} \ldots p_m^{k_m}$$

and p_i divides the right hand side, but not the left hand side, a contradiction. □

s