Number Theory

Jacob Denson

November 10, 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 first few examples are

$$2, 3, 5, 7, 11$$

The numbers that are left over once we remove all prime numbers are called composite. It is of great importance that one may 'compose' prime numbers to form all the composite numbers.

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 $a \leqslant \sqrt{n}$ or $b \leqslant \sqrt{n}$. 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

$$2,3,4,\dots,M$$

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

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

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 any 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 is not divisible by any number less than the square root of n, it must be prime. The number of operations to perform this procedure is therefore proportional to the sum of reciprocol primes

$$\sum_{p \leqslant \sqrt{M}} \frac{M}{p}$$

which is $O(M\pi(\sqrt{M}))$, where $\pi(n)$ counts the number of primes less than or equal to n. We will eventually show that $\pi(n) \sim n/\log(n)$, so that our algorithm is $O(M^{3/2}/\log(M))$. A tighter analysis can show this algorithm actually runs in $\Theta(\sqrt{M}\log\log M)$ time.

A particular decomposition of a composite number is not necessarily unique, because we can just rearrange the prime numbers

$$2 \cdot 3 = 3 \cdot 2$$

But we shall soon know that this is the only problem we can have. We shall assume all future decompositions

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

are in standard for, with $p_1 < p_2 < \dots < p_m$. That there is only one decomposition of each number composes exactly what is commonly known as the fundamental theorem of arithmetic, but is a bit tricky to prove formally.

Before our endeavor, however, we answer a fundamental question about the primes. Are there infinitely many of them? It is entirely possible that we have some finite set of primes. The very first proof in all of number theory shows this is not the case.

Theorem 1.2 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Let $p_1,\dots,p_n$ be a finite collection of prime numbers, and consider the number

$$n = p_1 \dots p_n + 1$$

Then n is not divisible by p_1, $p_2,\dots,p_n$, because, dividing by the p_i leaves a remainder of 1. But n must be divisible by a prime, so there is some prime not among the p_i, and so no finite subset of the primes exhausts the set. □

This theorem also gives us bounds on how spread apart the prime numbers are. If $p_1,p_2,\dots,p_n$ are all primes from 1 to n, then there is a prime between p_n and $p_1 \dots p_n + 1$.

To start with, we essentially prove we can perform long division on $\mathbf{N}$.

Lemma 1.3. *If $n,m \in \mathbf{N}$, then we may write $m = ln + r$, where $r < n$.*

Proof. If $m < n$, the proof is trivial. Otherwise, write $m' = m - n$, apply induction, and write $m' = l'n + r$. Then $m = (l'+1)n + r$. □

Theorem 1.4. *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

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

Now $p_i \mid q_1^{k_1} \dots q_l^{k_l}$ 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

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

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

Chapter 2

Congruences

2.1 Systems of Linear Congruences

The general recurrence relation $ax \equiv b \pmod{n}$ is easily solved in the general theory. If $\gcd(a,n) \mid b$, then we can write $b = m(at + nu)$, and if we define $x = mt$, then $ax \equiv b$. There are $\gcd(a,n)$ different solutions to this equation modulo n, given by

$$x \qquad x + \frac{n}{\gcd(a,n)} \qquad x + 2\frac{n}{\gcd(a,n)} \qquad \dots \qquad x + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)}$$

The number of solutions is the same as the size of the kernel of the homomorphism from $\mathbf{Z}_n$ given by $x \mapsto ax$, and this contains $n/\gcd(a,n)$ elements, because this is just the order of a. In particular, if a and n are relatively prime, then the equation has a unique solution.

Now we consider the more general problem of solving a system of linear congruences. We want to find x such that

$$\begin{gathered} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \dots \\ a_m x \equiv b_m \pmod{n_m} \end{gathered}$$

Using the prior problem, the problem is unsolvable unless $\gcd(a_i, n_i) \mid b_i$. Then we can find separate x_i such that $a_i x_i \equiv b_i$. The problem then reduces to finding a set of c_i such that $c_i \equiv 1 \pmod{b_i}$ and $c_i \equiv 0 \pmod{b_j}$, for we can then let $x = c_1x_1 + c_2x_2 + \cdots + c_mx_m$. If the n_i are pairwise relatively prime (we say they are coprime), finding c_i is easy; if we set $N_i = \prod_{j \neq i} n_j$, then there is t and u such that $tn_i + uN_i = 1$. We can then set $c_i = uN_i$. Any other choice of c_i' differs by a multiple of $n_1 \dots n_m$, because we must then have $n_i \mid c_i - c_i'$ for each i, and by coprimality $n_1 \dots n_m \mid c_i - c_i'$.

Theorem 2.1. *If the n_i are coprime, then every system of linear equations has a solution, and this solution is unique modulo $n_1 \dots n_m$. In terms of ring theory, the projection map establishes an isomorphism*

$$\mathbf{Z}_{n_1 \dots n_m} \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \cdots \times \mathbf{Z}_{n_m}$$

If the n_i are not coprime, the problem becomes more complicated.