Number Theory

Jacob Denson

January 11, 2018

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 Submonoids of the Natural Numbers

Our results about the greatest common denominator immediately have applications to subsets of the natural numbers closed under addition, semigroups. Let X denote an arbitrary subset of the natural numbers closed under addition, and let d denote the greatest common denominator of X.

Theorem 2.1. *X contains all but finitely many of $d\mathbf{N}$*

Proof. Dividing every element of X by d, it suffices to show that if the greatest common denominator of X is one, then X contains all but finitely many natural numbers. If we take a finite subset $x_1, \dots, x_n \in X$ such that $\gcd(x_1, \dots, x_n) = 1$, then there are integers $a_1, \dots, a_n \in \mathbf{Z}$ such that $\sum a_i x_i = 1$. Consider $M = \sum |a_i| x_i$. We claim that X contains all numbers greater than or equal to M^2. Given $0 \leqslant N < M$, we can write

$$M^2 + KM + N = \sum [(M+K)|a_i| - Na_i] x_i$$

and $\sum (M+K)|a_i| - Na_i \geqslant (M+K-N)|a_i| \geqslant (M-N)|a_i| \geqslant 0$, so $M^2 + KM + N$ is a positive sum of elements of X, and therefore $M^2 + KM + N \in X$. □

Corollary 2.2. *Every submonoid of the natural numbers is finitely generated.*

Example. *The upper bound M^2 is essentially tight for the natural numbers. If we consider the set $x\mathbf{N} + (x+1)\mathbf{N}$, and if $n = ax + b(x+1) = (a+b)x + b$, where $n \equiv x - 1$ modulo x, then $b \equiv x - 1$ modulo x, and so $b \geqslant x - 1$, in which* *case we conclude $n \geqslant (x-1)(x+1)$. It follows that if N is any number chosen large enough that $N, N+1, \dots \in x\mathbf{N} + (x+1)\mathbf{N}$, then there is $0 \leqslant k < x$ with $N + k \equiv x - 1$ modulo x, and so*

$$N \geqslant (x-1)(x+1) - k \geqslant (x-1)(x+1) - x = x^2 - x - 1$$

But in this case we have $(x+1) - x = 1$, so $M = 2x+1$, and $M^2 = 4x^2 + 4x + 1$, and so the upper bound is tight up to a constant.

2.2 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 $x = c_1 x_1 + c_2 x_2 + \dots + c_m x_m$. 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 2.3. *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*

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

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

Chapter 3

Diophantine Approximation

The rational numbers **Q**, most closely connected to the integers, form a dense subset of the set **R** of all real numbers. The field of diophantine approximation deals with how well one can approximate **R** by particular rational numbers. Because the rational numbers with a fixed denominator q divide the interval into length $1/q$ segments, there exists a rational number p/q such that $|x - p/q| \leqslant 1/2q$. The first interesting result was of Dirichlet, which was also historically one of the first uses of the pidgeonhole principle.

Theorem 3.1 (Dirichlet's Approximation Theorem)**.** *If x is irrational, there exists infinitely many rational numbers p/q such that $|x - p/q| \leqslant 1/q^2$.*

Proof. Given a rational number a, define $\langle a \rangle = a - \lfloor a \rfloor$ to be the **fractional part** of a, which lies in the range $[0,1)$. Fix some large integer N, and consider the numbers $\langle x \rangle$,$\langle 2x \rangle$,$\dots \langle (N+1)x \rangle$. The interval $[0,1)$ divides itself into N parts

$$\left[0,\frac{1}{N}\right),\left[\frac{1}{N},\frac{2}{N}\right),\dots,\left[\frac{N-1}{N},1\right)$$

The pidgeonhole principle then guarantees that there are two values $\langle nx \rangle$ and $\langle mx \rangle$ lying in the same of these intervals, so that $|\langle nx \rangle - \langle mx \rangle| < 1/N$. This can be reexpressed as $|(n-m)x - (\lfloor nx \rfloor - \lfloor mx \rfloor)| \leqslant 1/N$, or

$$\left| x - \frac{\lfloor nx \rfloor - \lfloor mx \rfloor}{n-m} \right| \leqslant \frac{1}{N(n-m)} \leqslant \frac{1}{(n-m)^2}$$

Denote this first approximation of x by p_1/q_1, and write $|x-p_1/q_1| = \alpha_1$. If x is irrational, then $\alpha_1 > 0$, and if we choose $N > 1/\alpha_1$, we may find p_2/q_2 with $q_2 \leqslant N$ and

$$|x - p_2/q_2| \leqslant 1/Nq_2 \leqslant 1/q_2^2$$

because $1/Nq_2 < \alpha_1$, $p_2/q_2 \neq p_1/q_1$. We may continue this process to find distinct rational numbers $p_1/q_1, p_2/q_2, \dots$, proving the theorem. □

On the other hand, most irrational numbers cannot be approximated to a rational number p/q to a factor of $1/q^3$, which follows from this simple theorem, using the fact that the intervals covered by all the rational numbers form a very small cover of the real line. Call an irrational number x 3-approximatible if there are infinitely many rational numbers p/q with $|x - p/q| \leqslant 1/q^3$.

Theorem 3.2. *The family of 3 approximatible functions is a set of Lebesgue measure zero.*

Proof. Note that if we take a rational number p/q, whose numerator and denominator is simplified, then the bound for the 3 approximations loosens because the denominator decreases, so we can approximate x by p/q if and only if x is in the interval $I_{p/q} = [p/q - 1/q^3, p/q + 1/q^3]$, where we assume p and q are relatively prime. We prove that the 3 approximatible numbers in $[0,1]$ form a set of measure zero, for then, since $x > 1$ is approximatible if and only if $x - 1$ is approximatible, proves the general result.

If $p > q$, then $p/q - 1/q^3 \leqslant 1 + 1/q - 1/q^3 \geqslant 1$, so $I_{p/q} \cap [0,1] \subset \{1\}$, and if $p < 0$, then $p/q + 1/q^3 \leqslant 1/q^3 - 1/q \leqslant 0$, so $I_{p/q} \cap [0,1] \subset \{0\}$. Thus the only time when $I_{p/q} \cap [0,1]$ is a set of positive measure is if $0 \leqslant p \leqslant q$. But in this case then $|Ip/q| = 2/q^3$, and

$$\sum_{q=1}^{\infty} \sum_{\substack{p \leqslant q \\ \gcd(p,q)=1}} |I_{p/q}| = \sum_{q=1}^{\infty} \frac{2\varphi(q)}{q^3} \leqslant \sum_{q=1}^{\infty} \frac{2}{q^2} < \infty$$

and so the Borel-Cantelli lemma implies that the set $E = \limsup I_{p/q}$ is a set of measure zero, and this is precisely the set of 3-approximatible numbers. □