

Number Theory

Jacob Denson

September 30, 2017

Table Of Contents

1	The Prime Numbers	2
2	Congruences	5
2.1	Submonoids of the Natural Numbers	5
2.2	Systems of Linear Congruences	6

Chapter 1

The Prime Numbers

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

$$1, 2, 3, \dots$$

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 $a = p_1 p_2 \dots p_n$, and $b = q_1 q_2 \dots q_m$, and then $n = p_1 \dots p_n q_1 \dots q_m$. \square

An interesting fact to notice is that if $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. 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 off 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 reciprocal primes

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

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 form, 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. \square

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 $m = (l' + 1)n + r$. \square

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

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

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 $m \leq l$. 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. \square

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, semi-groups. 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 $0 \leq N < M$, we can write

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

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

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

Example. *The lower bound M^2 is essentially tight for the natural numbers. If we consider two prime numbers $p < q$, and suppose that q contiguous numbers $x, x + 1, \dots, x + q - 1 \in p\mathbf{N} + q\mathbf{N}$. This is equivalent to all integers greater than*

or equal to x being in $p\mathbf{N} + q\mathbf{N}$, because we can add q to the equations to obtain all integers. Now if $x + k = a_k p + b_k q$, then modulo q , $x + k \equiv a_k p$. Since $x + k$ ranges over all q equivalence classes of \mathbf{Z}_q , the values a_0, \dots, a_{q-1} must all be distinct, and therefore there must be some m with $a_m \geq q - 1$, in which case

$$x + k = a_m p + b_m q \geq (q - 1)p$$

and thus

$$x \geq (q - 1)p - k \geq (q - 1)(p - 1)$$

So $x = \Omega(pq)$. If $q = 2p + 1$, then $q - 2p = 1$, and

$$(q + 2p)^2 \leq 2q(4p + 1) = 8pq + 2$$

So if there are infinitely many Sophie Germain primes (prime pairs of the form p and $2p + 1$), then the bound is tight up to a constant for arbitrarily large primes.

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

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

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

$$a_1 x \equiv b_1 \pmod{n_1}$$

$$a_2 x \equiv b_2 \pmod{n_2}$$

...

$$a_m x \equiv b_m \pmod{n_m}$$

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 $x = c_1 x_1 + c_2 x_2 + \cdots + c_m x_m$. 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*

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

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