Math 96:
Number Theory Techniques

October 4th, 2024

1 Introduction

Number theory broadly speaking is the study of the integers and their arithmetic. This deals with a number of topics including looking for integer solutions to polynomial equations and primes and factorization. In this lecture we will introduce some of the most basic concepts in number theory along with the most important results.

2 Primes and Factorization

Perhaps the most basic concept in number theory are primes and factorization. These can be used to understand what the multiplicative structure of the integers looks like. A *prime number* is a natural number larger than 1 that cannot be written as a product of two strictly smaller numbers. The *Fundamental Theorem of Arithmetic* says that any natural number can be written as a product of prime numbers and that furthermore, this representation is unique up to reordering of the factors. The fundamental theorem of arithmetic is very useful when thinking about multiplying numbers together. Essentially you can think of a natural number as a bag of primes that are being multiplied together. Multiplying two numbers together amounts to simply combining their bags.

This way of looking at things is also useful for thinking about other multiplicative properties of these numbers. For example, we say that a number n *divides* another number m if there is a third integer k so that $n \cdot k = m$. This will be possible if and only if there is some collection of primes that you can add to n's bag in order to reproduce m's. This will be possible if and only if every prime that appears in n's bad also appears in m's at least as many times.

Two other concepts that show up frequently are those of the *greatest common divisor* (gcd) of two numbers or the *least common multiple* (lcm). The gcd of n and m is the largest number k that divides both n and m. Using the Fundamental Theorem of Arithmetic, we can see that the number of copies of any prime p in the factorization of k is at most the minimum of the number of copies in the factorization of n and the number of copies of m. If you let

k be the number for which this holds for every prime p, you will get the gcd. Furthermore, it is not hard to see that *any* common divisor of n and m is a divisor of the greatest common divisor. Similarly, the least common multiple of n and m is the smallest number that is both a multiple of n and a multiple of m. You can get this by for each prime p taking the maximum of the number of copies of p in the factorization of n and in the factorization of m. Furthermore any common multiple of n and m will be a multiple of their lcm.

1999 B6: Let S be a finite set of integers, each greater than 1. Suppose that for each integer n there is some $s \in S$ such that $\gcd(s, n) = 1$ or $\gcd(s, n) = s$. Show that there exist $s, t \in S$ such that $\gcd(s, t)$ is prime.

3 Modular Arithmetic

If you add or multiply two numbers, you can determine the last digit of the result only knowing the last digit of the initial numbers. This observation allows you to define a 'last digit arithmetic' for numbers that can be useful. The generalization of this is what is known as modular arithmetic, which is a quite useful tool in number theory.

Given integers a, b, and m we say that a is congruent to b modulo m (written $a \equiv b \pmod{m}$) if m divides $a - b$. This has a bunch of important properties:

- Congruence modulo m is an equivalence relation, namely:
  - $a \equiv a \pmod{m}$
  - If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$
  - If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
- Each number is equivalent to its remainder upon dividing by m. In particular, for every pair of integers a, m there is a unique $r \in \{0, 1, 2, \ldots, m-1\}$ so that $a \equiv r \pmod{m}$.
- Arithmetic modulo m is well defined, namely if $a' \equiv a \pmod{m}$ and $b' \equiv b \pmod{m}$ then:
  - $a' + b' \equiv a + b \pmod{m}$
  - $a' \cdot b' \equiv a \cdot b \pmod{m}$.

This last point means that arithmetic of numbers modulo m is well defined. You can do algebra on mod m numbers in more or less the same way that you could with normal integers (though division is now a bit more complicated), but things are often simplified because there are now only finitely many possible numbers to consider (0 through $m - 1$), and because m is now equivalent to 0 (which can often be used to simplify things considerably). This is often a useful tool for gaining information about solutions to integer equations by considering them modulo m for some carefully chosen m. It should be noted that it is usually best to take m a power of a prime as the Chinese Remainder Theorem says that

information about what happens modulo more general m can be pieced together from this.

In particular, the Chinese Remainder Theorem says that if m and m' are relatively prime (i.e. $\gcd(m, m') = 1$), then:

- $a \equiv b \pmod{mm'}$ if and only if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{m'}$.
- For any integers y, y' there is an x so that $x \equiv y \pmod{m}$ and $x \equiv y' \pmod{m'}$.

Together these mean that doing arithmetic modulo mm' is essentially the same as doing arithmetic mod m and mod m' at the same time.

2019 B6: Let $\mathbb{Z}^n$ be the integer lattice in $\mathbb{R}^n$. Two points in $\mathbb{Z}^n$ are called *neighbors* if they differ by exactly 1 in one coordinate and are equal in all other coordinates. For which integers $n \geq 1$ does there exist a set of points $S \in \mathbb{Z}^n$ satisfying the following two conditions?

1. If p is in S, then none of the neighbors of p is in S.
2. If $p \in \mathbb{Z}^n$ is not in S, then exactly one of the neighbors of p is in S.

4 Multiplicative Structure Modulo p

Another important set of results involves what happens when you multiply numbers modulo a prime p. Clearly, multiplying anything by 0 gives 0, but if you take any other number a not divisible by p and keep multiplying by a, you will eventually get 1 modulo p. In particular, *Fermat's Little Theorem* states that if p is a prime and a is not a multiple of p then $a^{p-1} \equiv 1 \pmod{p}$. This is a quite useful fact to know if you are interested in taking powers of a number modulo p. Furthermore, for every prime p there is always at least one *primitive generator* g so that every number mod p except for 0 can be written as a power of g. In particular, this gives you a new way to think about the non-zero numbers modulo p as just the different powers of g, which is particularly useful if you want to understand how they multiply.

1994 B6: For any integer n, set

$$n_a = 101a - 100 \cdot 2^a.$$

Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

5 Multiplicative Functions

A function on the natural numbers $\mathbb{N}$ is called *multiplicative* if for every pair of relatively prime integers n and m that $f(nm) = f(n)f(m)$. In particular, this means that if n factors as $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ then $f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k})$. Therefore,

all the values of f are determined by their values on products of primes. There are a bunch of well known examples of multiplicative functions including:

- The identity function - $Id(n) = n$. $Id(p^n) = p^n$.
- The divisor function - $d(n)$ is the number of integers that divide n. $d(p^a) = a + 1$.
- The sigma function - $\sigma(n)$ is the sum of all positive divisors of n. $\sigma(p^a) = 1 + p + p^2 + \ldots + p^a = (p^{a+1} - 1)/(p - 1)$.
- The totient function - $phi(n)$ is the number of integers modulo n that are relatively prime to n. $\phi(p^a) = (p - 1)p^{a-1}$.

There are some nice ways of combining multiplicative functions. For example, if f and g are multiplicative then so is:

- Their product - $(f \cdot g)(n) = f(n)g(n)$.
- Their convolution - $(f \star g)(n) = \sum_{m|n} f(m)g(n/m)$.

1964 B5: Let u_n $(n = 1, 2, 3, \ldots)$ denote the least common multiple of the first n terms of a strictly increasing sequence of positive integers (for example the sequence $1, 2, 3, 4, 5, 6, 10, 12, \ldots$). Prove that the series

$$\sum_{n=1}^{\infty} 1/u_n$$

is convergent.