Math 96:
Number Theory Techniques

October 13th, 2023

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 uniquely 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.

2008 A3: Start with a finite sequence $a_1, a_2, \ldots, a_n$ of positive integers. If possible, choose two indices $j < k$ such that a_j does not divide a_k and replace a_j and a_k by $mathrmgcd(a_j, a_k)$ and $\text{lcm}(a_j, a_k)$, respectively. Price that if this process is repeated, it must eventually stop and the final sequence does not depending on the choices made. (Note: gcd means the greatest common divisor and lcm means least common multiple.)

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.

1998 B6: Prove that, for any integers a, b, c there exists a positive integer n such that $\sqrt{n^3 + an^2 + bn + c}$ is not an integer.

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.

1983 A3: Let p be in the set $\{3, 5, 7, 11, \ldots\}$ of add primes and let

$$F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}.$$

Prove that if a and b are distinct integers in $\{0, 1, 2, \ldots, p-1\}$ then $F(a)$ and $F(b)$ are not congruent modulo p, that is, $F(a) - F(b)$ is not exactly divisible by p.

5 Solutions to Quadratic Equations

If you have a polynomial $p(x) = x^2 + ax + b$, it will always have two roots (counting multiplicities) which sum to $-a$. If a and b are both integers, and one of these roots is another integer n, then the other root must also be an integer $-a - n$. This means that if you have one integer root of this polynomial, you can find another as well. If this was applied to a polynomial in one variable, this might not be too useful, as it would merely give you one of two solutions from the other one. However, if you have a polynomial in *several* variables that is degree 2 in each of them, you can keep switching which variable you are applying this trick to often generating infinitely many solutions.

1978 B4: Prove that for every real number N, the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^4 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

has a olution for which x_1, x_2, x_3, x_4 are all integers larger than N.