Math 96:
Number Theory Techniques

October 10th, 2025

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.

Van Vleck Talent Search 2024-2025 competition part II number 4: Let $n = 2^{2024} \cdot 3^{2025}$. How many positive divisors does n^2 have that are less than n, but do not divide n?

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.

1940 A1: Prove that if $f(x)$ is a polynomial with integral coefficients, and there exists an integer k such that none of the integers $f(1), f(2), \ldots, f(k)$ is divisible by k, then $f(x)$ has no integral root.

4 The Chinese Remainder Theorem

When considering which modulus m to consider, it usually suffices to consider m a power of a prime. This is because a result known as the Chinese Remainder Theorem says that all of the information modulo m can be uniquely reconstructed by knowing what happens mod powers of primes dividing m.

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. This also generalizes to any number of moduli $m_1, m_2, \ldots, m_k$ so long as they are *pairwise relatively prime* (i.e. $\gcd(m_i, m_j) = 1$ for all $i \neq j$). In particular:

- $a \equiv b \pmod{\prod m + i}$ if and only if $a \equiv b \pmod{m_i}$ for all i.
- For any integers y_i there is an x so that $x \equiv y \pmod{m_i}$ for all i.

Note that if m is any number, we can always write $m = \prod m_i$ where each m_i is a power of a prime and the m_i's are pairwise relatively prime.

The Chinese Remainder Theorem allows one to break down arithmetic modulo a complicated modulus m to working modulo its prime power factors (which is often easier). It also allows one to construct numbers with important congruential properties by piecing together information mod different factors.

1955 B4: Do there exist $1,000,000$ consecutive integers each of which contains a repeated prime factor?

5 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.

Modulo more complicated m, one can use Euler's generalization which states that if x is relatively prime to m that $x^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is the number of classes mod m relatively prime to m, which is given by $m \prod_{p|m} \frac{p-1}{p}$.

1985 A4: Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_i?

6 Valuations

One sometimes useful quantity to consider is the number of times that a particular prime of interest divides various numbers. In particular, one can define the *p-adic valuation* of a non-zero integer n as $v_p(n)$ is the number of times p occurs in the prime factorization of n. You can even extend this valuation to non-zero rational numbers by letting $v_p(n/m) = v_p(n) - v_p(m)$. This valuation has several useful properties:

- $v_p(nm) = v_p(n) + v_p(m)$
- $v_p(n^k) = kv_p(n)$
- $v_p(n+m) \geq \min(v_p(n), v_p(m))$ with equality if $v_p(n) \neq v_p(m)$

1955 A6: Find a necessary and sufficient condition on the positive integer n that the equation

$$x^n + (2+x)^n + (2-x)^n = 0$$

have a rational root.