# Number Theory

Boston Bulis, Kyra Burke, and Lee Van Voorhis

Mentor: Sam Packman

April 2025

This paper offers a broad exploration of number theory, tracing its development from elementary concepts like divisibility and prime factorization to more advanced structures such as modular arithmetic and group theory. By examining key theorems, patterns, and proofs, we highlight the logical foundations and surprising complexity underlying the integers. While rooted in pure mathematics, number theory's applications—from cryptography to abstract algebra—demonstrate its enduring relevance. Our discussion emphasizes both the elegance of classical results and the power of modern algebraic approaches to reveal deeper insights into the structure of numbers

## 1 Introduction

Number theory is the study of integers and the patterns and structures that arise when we look closely at how they behave. It starts with familiar ideas like divisibility, remainders, prime numbers, but quickly builds into a deeper and more abstract understanding of how numbers relate to one another.

What makes number theory so interesting is how far you can go using just logic and basic arithmetic. Many of the results you will encounter do not rely on advanced techniques from calculus or algebra. Instead, you build up ideas step by step, often using clever reasoning and proof. Some of the most powerful results in mathematics come from simple questions. Which numbers can be written as the sum of two squares? How can you solve equations in integers? What happens when you reduce everything mod 7?

In this paper, we will explore topics like divisibility, congruences, primes, and theorems such as the Chinese Remainder Theorem. The goal is to build a clear and logical understanding of how numbers work and to show how deep ideas can come from simple questions.

## 2 Divisibility

At one of it's most fundamental levels, number theory is interested in the properties of divisibility.

- We say $a \mid b$ ("a divides b") if there is an integer a for which $b = ax$. For example, $5 \mid 30$ because $5 \mid 5 \cdot 6$
- We say a multiple can be defined if $a$ and $b$ be are integers with $b \neq 0$. We say that $a$ is a multiple of $b$ if there exists an integer $kZ$ such that $a = bk$

There are a couple fundemental proofs of divisibility we will go through, as they will lay the foundation for the rest of the proofs in this paper:

1. $a \mid b$ implies $a \mid bc$
   (a) proof: we can substitute $b = ax$ into $bc$, which implies $a \mid axc$. Since $a$ is found in the divisor and the dividend, it is implied that $a \mid bc$
2. $a \mid b$ and $b \mid c$ imply $a \mid c$
   (a) proof: let $b = ax$, $c = by$, and $c = az$, respectively. We will substitute $by = az$, and then substitute b: $(ax)y = az$. QED
3. $a \mid b$ and $a \mid c$ imply $a \mid (bx + cy)$ for any integers x and y
   (a) proof: $b = ai$, $c = aj$; moving back and substituting: $(aix + ajy)$ which can be simplified to $a \mid a(ix + jy)$
4. $a \mid b$ and $b \mid a$ implies $a = \pm b$
   (a) proof: $b = ax$, $a = by$; after substitution of $b$: $a = (ax)y$ which can be rewritten as $\frac{a}{a} = xy$ which can only be true if $x \cdot y = \pm 1$
5. $a \mid b$, $a > 0$, $b > 0$, imply $ab$
   (a) proof: $b = ax$, $b$ must be bigger than a, so $x1$.

## 3 Primes

Another important concept in number theory is prime numbers.

- A positive integer $p$ is considered prime if and only if there exists no integer $a$ other than 1 and $p$ (where $p \neq 1$) for which $a \mid p$
- A non-prime integer (that is not 0 or 1) is called a composite number
- 0 and 1 are not prime or composite.

Any number, prime or composite, can be written out uniquely as a product of powers of prime numbers.

For example, $480 = 5 \times 3 \times 2^4$. Ignoring order, this is the only way to write the prime factors of 480.

There is no largest prime number. To understand why this is true, imagine there is some largest prime number, which we will call $s$.

This means there is a finite number of prime numbers. If you multiply all of the primes up to $s$ together, the resulting number will be some integer $a$. $a+1$, then, is also an integer.

$a+1$ cannot be divisible by any of the numbers that $a$ was divisible by (other than 1,) as it is only 1 more, as if, for any integer $x$, if $x \mid a$, in order for $x \mid a+1$, it must also be true that $x \mid 1$, which is only true if $x = 1$.

Thus, $a$ and $a+1$ share no factors. This means that either $a+1$ is prime, meaning there is a prime larger than $s$ ($a$ is a multiple of $s$, so $a+1$ must be at least 1 bigger than $s$), or $a+1$ is composite and has prime factors that are larger than $s$ (as it has no prime factors smaller than $s$).

This means that there must be some prime larger than $s$, proving that there is no largest prime, as for each prime number there must be some prime larger than it.

Note that, although it is tempting to conclude that $a+1$ is prime, this is not true. A counter example is when $s = 13$. $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$ and is thus not prime.

## 4 Greatest Common Divisor and Least Common Multiple

- The greatest common divisor of two integers $a$ and $b$ is the largest integer that both $a$ and $b$ are divisible by. It's denoted by $\gcd(a, b)$.
- The least common multiple of two integers $c$ and $d$ is the smallest positive integer that is divisible by both $c$ and $d$. It's denoted by $\text{lcm}[c, d]$.

The least common multiple of two integers $a$ and $b$ is equivalent to $\frac{ab}{gcd(a,b)}$

The $\gcd(a, b)$ can be calculated by finding the prime factors of $a$ and $b$ and then finding the factors they have in common.

For example, we know if $a = 6$ and $b = 8$, then $\gcd(a, b) = 2$. This is because $6 = 2 \times 3$ and $8 = 2 \times 2 \times 2$. The only common factor there is 2, so the greatest common divisor is 2.

This works well for numbers that can be easily factored, but it gets more difficult with

larger numbers. For example, it's quite difficult to look at 719927 and know that its prime factorization is $13 \times 19 \times 701$.

One common way to find the greatest common divisor without fully factorizing the two integers is called Euclid's algorithm. It can be done by hand with some arithmetic or quite easily with a simple four-function calculator.

Euclid's algorithm works as follows. Take the two integers $a$ and $b$ and put them in the form $a - bx = r$, where $0 \leq r < b$. One such solution will exist for all $a$ and $b$, and an easy way to find $x$ is to divide $a$ by $b$ and then truncate any decimals, leaving you with an integer.

Once you have the form $a - bx = r$, check if $r = 0$. If it does, then the greatest common divisor is $b$. Otherwise, find an equation of the form $b - rx_2 = r_2$. Check if the remainder $r_2$ is zero, and if not, repeat the process until the remainder is 0.

Here is an example of Euclid's algorithm being used to find $\gcd(22113, 413712)$.

| a | b | x | r |
|---|---|---|---|
| 22113 | 413712 | 0 | 22113 |
| 413712 | 22113 | 18 | 15678 |
| 22113 | 15678 | 1 | 6435 |
| 15678 | 6435 | 2 | 2808 |
| 6435 | 2808 | 2 | 819 |
| 2808 | 819 | 2 | 351 |
| 819 | 351 | 2 | 117 |
| 351 | 117 | 3 | 0 |

Note that, as the smallest number was put first, the first step simply flips them. This is not a coincidence, this happens whenever the smaller number is put first. This is important, because it guarantees that $\gcd(a, b) = \gcd(b, a)$, which is true for all integer $a$ and $b$ As the final non-zero remainder is 117, the $\gcd(22113, 413712)$ is 117. Although the process of finding this number wasn't immediate, it's much faster than factoring the two numbers.

This is helpful because finding the greatest common divisor is useful in solving systems of congruences, and simplifying fractions to their lowest terms, among many other things.

If the greatest common divisor of two integers is 1, the two integers are referred to as **relatively prime**.

A set of multiple numbers can be relatively prime or pairwise relatively prime. If the set is relatively prime, there is no common divisor (other than 1) that divides all of the integers in the set. If it is pairwise relatively prime, then there are no two integers that have a non-1 common divisor.

An example of a set that is pairwise relatively prime is $\{1, 5, 21, 64\}$. An example of a set that is relatively prime but not pairwise relatively prime is $\{4, 8, 15, 16, 23, 42\}$.

## 5 Congruences

Congruences are a foundational concept in number theory. They offer a way to express relationships between integers based on the remainders they leave when divided by another integer. Instead of focusing on exact values, congruences group the numbers according to their remainders.

Let $a$, $b$, and $n$ be integers with $n > 0$. We say that $a \equiv b \pmod{n}$ (read as "a is congruent to b modulo n") if and only if $n \mid (a - b)$.

**Example**: $17 \equiv 5 \pmod{12}$ because $17 - 5 = 12$, and 12 is divisible by 12. Also, $23 \equiv 2 \pmod{7}$ because $23 \div 7 = 3$ remainder 2.

**Properties of Congruences**: if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then:

1. Addition: $a + c \equiv b + d \pmod{n}$
2. Subtraction: $a - c \equiv b - d \pmod{n}$
3. Multiplication: $ac \equiv bd \pmod{n}$
4. Power rule: $a^k \equiv b^k \pmod{n}$ for any integer $k$

These rules allow us to perform arithmetic modulo $n$ just like ordinary arithmetic, except we always reduce the result modulo $n$. For an example, let us compute $23 + 19 \pmod{7}$:

1. Reduce 23 and 19 modulo 7:
   - $23 \equiv 2 \pmod{7}$
   - $19 \equiv 5 \pmod{7}$
2. Now compute: $2 + 5 \equiv 7 \equiv 0 \pmod{7}$

Therefore, we can conclude that $23 + 19 \equiv 0 \pmod{7}$

**Linear Congruences**: A linear congruence is an equation of the form: $ax \equiv b \pmod{n}$ To solve this, we need to find all integers $x$ such that the equation is true.

The equation has a solution if and only if $\gcd(a, n)$ divides $b$. If the solution exists, there are exactly $\gcd(a, n)$ solutions modulo $n$. For example, here is how to find the solution for the equation $3x \equiv 6 \pmod 9$.

1. Find the $\gcd(3, 9)$, which is 3.

This means that there are 3 solutions to the congruence.

## 6 The Chinese Remainder Theorem

The Chinese Remainder Theorem is a critical tool in number theory and modular arithmetic. It allows us to solve systems of congruences by breaking up a complex problem into smaller, more simple ones.

The theorem states that if $n_1, n_2, ..., n_k$ are pairwise coprime integers, then for any integers $a_1, a_2, ..., a_k$, there exists a unique integer $x$ modulo $N$, where $N = n_1 n_2 ... n_k$, such that $x \equiv a_i \pmod{n_i}$ This means that $x$ satisfies all the given congruences simultaneously.
**Problem Example**: Solve the following system of congruences:

- $x \equiv 1 \pmod 3$
- $x \equiv 2 \pmod 5$

The moduli $n_1 = 3$ and $n_2 = 5$. Because these moduli are pairwise coprime, we can apply the CRT. Now, we must calculate $N$: $n_1 n_2 = 3 \times 5 = 15$. For $n_1 = 3$: $N_1 = \frac{15}{3} = 5$.

We now have to find $y_1$ such that $5y_1 \equiv 1 \pmod 3$. Because we know that $5 \equiv 2 \pmod 3$, we can simplify the congruence to $2y_1 \equiv 1 \pmod 3$.

$y_1$ cannot be 1 or 3, so by testing it at 2 we get $2 \times 2 = 4 \equiv 1 \pmod 3$, thus $y_1 = 2$. For $n_2 = 5$, $N_2 = \frac{15}{5} = 3$. We have to find $y_2$ such that $3y_2 \equiv 1 \pmod 5$.

By testing values, we arrive at $y_2 = 2$ because $3 \times 2 = 6 \equiv 1 \pmod 5$.

Now we can find the solution $x$ using the formula $x = a_1 N_1 y_1 + a_2 N_2 y_2$. By substituting the values we have, we get $10 + 12 = 22 = x$. Finally, we need to reduce $x$ modulo $N$: $x \equiv 22 \pmod{15}$.

# 7 Sets and Relations

Sets and relations are also important for number theory

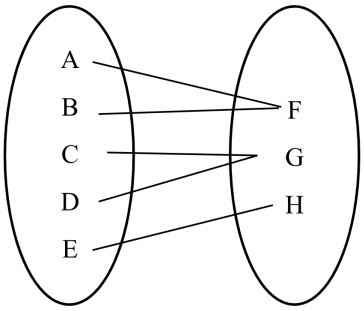
- A set is an unordered list of elements, denoted as $\{a, b, c\}$ where $a$, $b$ and $c$ are elements of the set. Each element can only be in a set once.
- A relation relates one set (the domain) to another set (the co-domain).

Sets can have anything in them, from numbers to letters to people to animals, but in this paper we will be talking about sets of numbers for the most part, whether that's integers, rational numbers, real numbers, or complex numbers.

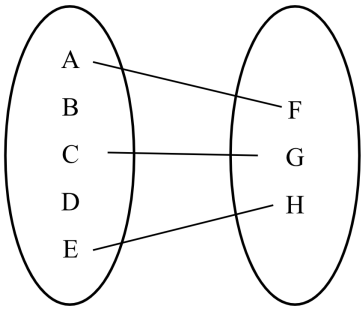
Sets also have **cardinality**, which is the number of elements in the set. If we let the set $A$ be $\{1, 3, 7, 9\}$, then the cardinality of $A$ (denoted by $|A|$) is 4, as there are 4 elements in the set.

There are many different kinds of relations, including functions, which map each element in the domain to exactly one element in the co-domain. We will be talking about three types of functions and relations here: **injective**, **surjective**, and **bijective**:

**Injective**: A relation $f$ is considered injective if and only if $f(a) = f(b)$ implies that $a = b$. In other words, there is no value in the codomain that has more than one value from the domain mapped to it.

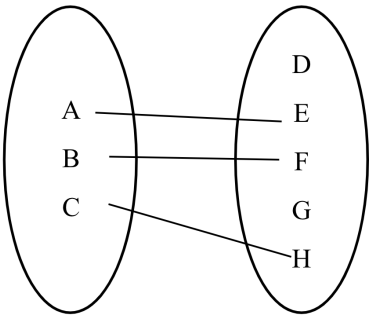



This isn't injective

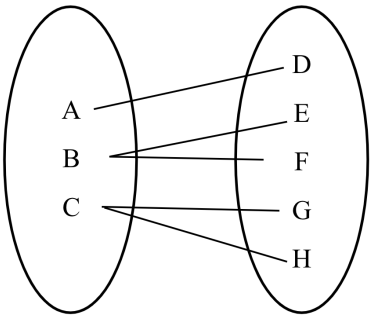



This is injective

**Surjective**: A relation $f$ is surjective if and only if every value in the co-domain has some corresponding value in the domain. In other words, the relation maps some value to every possible output value.

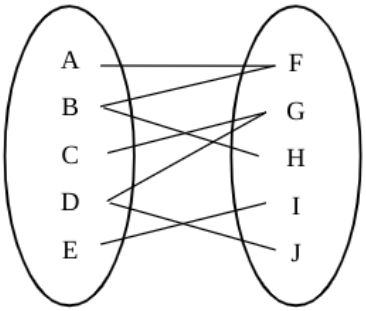



This isn't surjective

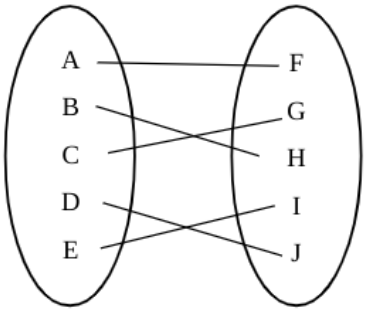



This is surjective

**Bijective**: A relation $f$ is bijective if and only if it is total, injective, and surjective. In other words, the relation maps each value in the domain to exactly one value in the co-domain.




This isn't bijective

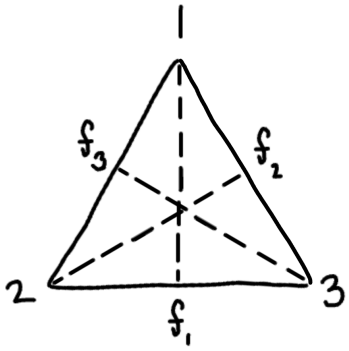



This is bijective

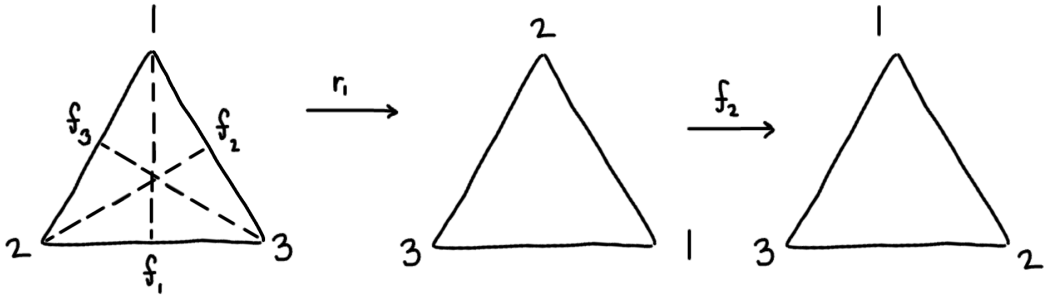
Bijections are quite important because if a bijection exists between two sets, the sets must have the same cardinality. This means if you can prove a bijection exists, the sets must be the same size. This is useful when talking about different sizes of infinity. Bijections are also utilized to prove isomorphisms, which are explained in the next section.

## 8 Group Symmetries

Imagine you've drawn a triangle and you're interested in understanding it's different symmetries. Assuming the triangle does not "change it's shape" on paper, we can rotate it 120, 240, or 360 degrees, or flip it along one of it's 3 axes. We will do as follows. $r_1 = 120°$, $r_2 = 240°$, and $r_3 = 360°$




To grow some intuition, say we're interested in creating a table to see what will happen when we rotate once, then flip/reflect along $f_2$.




As it turns out, this is the same as $f_1$.

In group theory, a **generator** is an element (or a set of elements) from which every other element in the group can be obtained by applying the group operation repeatedly, including inverses if necessary. For example, in the symmetry group of an equilateral triangle, denoted $D_3$, the group consists of six elements: the identity $e$, two rotations $r$ (by 120°) and $r^2$ (by 240°), and three reflections $f$, $rf$, and $r^2f$. The elements $r$ and $f$ are considered generators of $D_3$ because all six symmetries can be produced by combining these two elements in various ways.

To understand how these generators interact and to determine what symmetries they produce, we analyze compositions like $rf$ or $r^2f$. These compositions tell us how one symmetry (such as a reflection) transforms when combined with another (such as a rotation). For example, consider the expression:

$$(r^2f)(r) = r^2frr^{-1} = r^2(fr^2)r^{-1} = r^2rfr^{-1} = fr$$

This computation uses the property that reflections and rotations in $D_3$ satisfy relations like $fr = r^{-1}f$. Simplifying further, we find:

$$(r^2 f)(r) = fr = rf$$

This result tells us that certain compositions of the generators result in other known symmetries. By computing these compositions, we verify that every element of the group can be expressed in terms of $r$ and $f$, confirming that they generate the entire group. This can be expressed as

$$< r, f : r^3 = f^2 = e, fr^2 = rf >$$

## References

[1] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. 5th ed., John Wiley & Sons, 1991.