Elementary Number Theory

Zac Zerafa

September 29, 2025

Contents

Part I

Numbers

Chapter 1

Types of numbers

Number theory studies integers, integer functions, and numbers with close relations to integers such as the rational numbers. More specific areas of number theory may look at algebraic numbers and transcendental numbers (algebraic and transcendental number theory), however elementary number theory tends to focus on just integers, possibly rational numbers on occasion.

Though readers are quite familiar with numbers, we define them for completeness.

1.1 Natural numbers

Definition 1.1. The *natural numbers* are numbers where each number has a successor. The set of natural numbers is denoted $\mathbb{N}$.

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$$

$$\mathbb{N} = \{n + 1 : n \in \mathbb{N}\} \cup \{0, 1\}$$

The natural numbers are simple enough, yet much can be said about them and there are many unanswered questions related to them. A few neat properties can be seen by breaking the number up into a sum of its ones, tens, hundreds, etc. This is generalized by the *basis representation theorem.*

Theorem 1.1 (Basis representation theorem)**.** For any natural numbers n, b, there is a unique sequence $(d_i)_{i=0}^{k}$ with $d_i < b$that can represent n in the following way.

$$n = \sum_{i=0}^{k} d_i b^i$$

This theorem is responsible for the machinery behind the basic addition algorithm learnt at school; the basis representation theorem with $b = 10$ provides the justification to add multidigit numbers by adding ones digits together, tens digits together ans so forth, and borrowing is the necessary remedy when the $d_i \geq b$.

One caveat with natural numbers is that subtraction isn't always well defined even though addition is. For example $4 - 5 \notin \mathbb{N}$. This is because although every number has a successor, not every number has a predecessor (0 ruins the fun for us).

1.2 Integers

Definition 1.2. The *integers* are an extension of the natural numbers such that each number also has a predecessor. The set of integers is denoted $\mathbb{Z}$.

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

$$\mathbb{Z} = \{b - a : a, b \in \mathbb{N}\}$$

Working with integers, the mathematician can be sure that addition, subtraction, and multiplication are closed in $\mathbb{Z}$.

1.3 Rational numbers

Both the natural numbers and integers are closed under multiplication, but we require the rational numbers ensure closure under division.

Definition 1.3. The *rational numbers* are an extension of the integers such that the quotient of two integers is always well defined. The set of rational numbers is denoted $\mathbb{Q}$.

$$\mathbb{Z} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$$

As readers might know, there are also *irrational numbers*; numbers that can be approximated as close as desired by rational numbers, alas they cannot be represented as a fraction of two integers. Examples of these are $\sqrt{2}$ and π; this is described more in Transcendental Number Theory and Real Analysis.

Chapter 2

Basic classes of integers

Just like the natural numbers, integers have a straightforward definition but have extremely deep properties. Sometimes we can identify that a certain group of numbers have some special 'pattern' or 'property', while other numbers don't. A sequence or set might be used as notation to describe such numbers.

The nth *even number* is every second number starting from 0

$$(2n)_{n\in\mathbb{N}}$$

$$(0, 2, 4, 6, 8, 10, ...)$$

The nth *odd number* is every second number starting from 1. The idea is that it captures the numbers that are not even.

$$(2n + 1)_{n\in\mathbb{N}}$$

$$(1, 3, 5, 7, 9, 11, ...)$$

The kth *multiple of* n is the result of $k \times n$

$$(kn)_{k\in\mathbb{N}}$$

The kth *power of* n is the result of n^k

$$(n^k)_{k\in\mathbb{N}}$$

The nth *square number* is the result of squaring n

$$(n^2)_{n\in\mathbb{N}}$$

$$(0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, ...)$$

Proposition 2.1. The sum of the first $n-1$ odd numbers is the nth square number

$$n^2 = \sum_{k=0}^{n-1}(2k+1)$$

The nth *triangle number* is a number obtained by adding up the first n numbers.

$$S_n = \sum_{k=0}^{n} k$$

$$(0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, ...)$$

Triangle numbers have a closed form expression that makes them easier to computer and

Proposition 2.2.

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

There are also some notable integer sequences that come from the field of enumerative combinatorics; number theory is indeed used to study these sequences. The Fibonacci and Catalan numbers are perhaps the most famous examples. Indeed, number theory and combinatorics are quite intimately related.

Above all, there is one class of a number that has perpetually fascinated and eluded mathematicians for millennia, and they are perhaps the most elegant and enigmatic class of integers in mathematics entirely. They are no other than the *prime numbers*; though we'll have to develop some theory on divisibility before we can discuss them.

Chapter 3

Divisibility

3.1 Divisibility

We define divisibility as the following relation on the integers.

Definition 3.1. Given two integers a, b, a *divides* b iff a can be multiplied by some integer to obtain b. We denote this relation as $a|b$.

$$a, b \in \mathbb{Z}$$

$$a|b \iff \exists k \in \mathbb{Z}(ak = b)$$

3.2 Euclid's division lemma

Lemma 3.1 (Euclid's division lemma)**.** Every natural number n can be represented with a unique d and a unique r less than d in the following manner.

$$n = dq + r$$

$$\forall n \in \mathbb{N}(\exists! d \in \mathbb{Z}, r \in \mathbb{N} \cap [0, d)[n = qd + r])$$

3.3 Multiples and factors

Definition 3.2. A *multiple* of a is some integer that a divides; an integer that equals a multiplied by some integer.

$$m \text{ is a multiple of } a \iff a|m$$

Definition 3.3. A *factor* or *divisor* of a is some integer that divides a; an integer that can 'go into' a with no remainder.

$$d \text{ is a factor of } a \iff d|a$$

3.4 Lowest common multiple

3.5 Greatest common factor

3.6 Euclidean algorithm

We first develop the theory that Euclid had in mind.

Proposition 3.1.

$$m, n \in \mathbb{Z} \implies \gcd(m, 0) = m \wedge \forall q \in \mathbb{Z}[\gcd(m, n) = \gcd(m - qn, n)]$$

$m \leftarrow \max(a, b)$
$n \leftarrow \min(a, b)$
while $m\%n > 0$ **do**
  $v \leftarrow m$
  $m \leftarrow n$
  $n \leftarrow v\%n$
end while
$d \leftarrow n$

3.7 Bézout's lemma

This identity follows from the extended Euclidean algorithm and will prove vital in our analysis coprimality. It is also important in abstract algebra, where they classify algebraic structures on whether this identity holds.

Lemma 3.2 (Bézout's lemma)**.**

$$\exists x, y \in \mathbb{Z}[ax + by = \gcd(a, b)]$$

- perfect number

Chapter 4

Primality

4.1 Prime numbers

Prime numbers lie not just in the heard of number theory, but in the heart of a mathematician. This book will provide only an elementary insight into their properties, however resorting to the likes of modern algebra and complex analysis allows for some seriously gourmet proofs.

Definition 4.1. A natural number greater than 1 is a *prime number* iff it is divisible only by 1 and itself.

$$n \in \mathbb{N} \setminus \{0, 1\} \text{ is prime } \iff \{d \in \mathbb{N} : d|n\} = \{1, n\}$$

A natural number greater than 1 is a *composite number* iff it is not prime.

Here we have yet another definition that is easy to understand, but bears consequences beyond even the richest of imaginations. This chapter will analyze prime numbers using elementary algebra and the results on integers and divisibility established earlier, however as we progress into modular arithmetic, we will draw upon some deeper reasoning (basic group theory sugar coated by elementary methods) to get a hold of some more interesting results.

Though riveting stuff awaits when we add a bit of 'algebraic magic', studying prime numbers in an elementary setting is by no means boring. We shall demonstrate the original proof of Euclid's theorem; often hailed as one of the most elegant proofs in mathematics.

4.2 Euclid's theorem

We introduce a nice notation that goes particularly well with the theorem that we are about to prove.

Definition 4.2. The *primorial* is a function returning the product of the first n prime numbers.

$$n\# = \prod_{i=1}^{n} p_i$$

Theorem 4.1 (Euclid's theorem)**.** There are an infinite amount of prime numbers; for any prime number, there is a larger prime number.

$$p \text{ is prime } \implies \exists q(q \text{ is prime } \land q > p)$$

Assume p is the nth prime number and consider $n\# + 1$. $n\# + 1$ is not divisible by any of the first n primes. If $n\# + 1$ is either prime itself, we are done. If it is not prime, them it must be divisible by a prime number larger than p.

4.3 Pair of coprime numbers

Definition 4.3. A *pair of coprime numbers* are a pair of integers a, b such that ther GFC is 1.

$$(a, b) \text{ are coprime } \iff \gcd(a, b) = 1$$

4.4 Euclid's lemma

Lemma 4.1 (Euclid's lemma)**.**

$$p \text{ is prime } \land p|ab \land \neg(p|a) \implies p|b$$

Lemma 4.2 (Generalized Euclid's lemma)**.**

$$c|ab \land \gcd(c, a) = 1 \implies c|b$$

Proposition 4.1.

$$a|a$$
$$a|b \wedge b|c \implies a|c$$
$$a|b \implies an|bn$$
$$an|bn \wedge a \neq 0 \implies a|b$$
$$a, b > \wedge a|b \implies a \leq b$$

4.5 Naive factorization algorithm

Proposition 4.2.

$$n \text{ is composite} \implies \exists p[p \text{ is prime} \wedge p \leq \sqrt{n}]$$

- algo here

$D \leftarrow \{n\}$
while $\exists d \in D(d \text{ is composite})$ **do**
  for $a \in \mathbb{N} \cap [2, \sqrt{d}]$ **do**
    if $a|d$ **then**
      $D \leftarrow D \setminus \{d\}$
      $D \leftarrow D \sqcup \{a, \frac{d}{a}\}$
      break
    end if
  end for
end while

4.6 Fundamental theorem of arithmetic

4.7 Types of prime numbers

Some mathematicians have restricted their study to prime numbers of a certain forms. The reason for this is because mathematicians seek to understand how primality interacts with other mathematical properties, in hopes of finding interesting results. For instance, numbers of the form $2^n - 1$ have some

properties that permit relatively efficient algorithms for checking their primalities.

-

- sieve of Eratosthenes - Fermat prime - Mersenne prime

4.8 Relationship with Riemann Zeta function

Daddy Euler had a strong penchant for infinite products and, like all mathematicians, for prime numbers. This is definitely reflected in his proposition on the Riemann Zeta function factorization.

Part II

Modular arithmetic

Chapter 5

Modular arithmetic

Chapter 6

Euler's theorem

6.1 Fermat's little theorem

Theorem 6.1 (Fermat's little theorem)**.**

$$a^{p-1} \equiv 1 \mod p$$

However there is a stronger version of the theorem. It requires the understanding of a *totient function.*

6.2 Euler's totient function

Definition 6.1. *Euler's totient function* $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$

$$\varphi(n) = |\{m \in \mathbb{Z} \cap [1, n)[\gcd(n, m) = 1]\}|$$

Much can be said about Euler's totient function; the bulk of these results will be left for a chapter on *arithmetic functions.* We will however ist one proposition that will be required to compare Fermat's version to Euler's.

Proposition 6.1.

$$\varphi(p) = p - 1$$

6.3 Euler's totient function

Theorem 6.2 (Euler's theorem)**.**

$$a^{\varphi(n)} \equiv 1 \mod n$$

Chapter 7

Chinese remainder theorem

Theorem 7.1 (Chinese remainder theorem)**.**

- Lagrange's theorem

Chapter 8

Quadratic residues

- quadratic residue - Euler's criterion - Gauss' lemma - law of quadratic reciprocity - Wilson's theorem - uniqueness mod (p-1)/2 of quadratic residues

Part III

Elementary arithmetic functions

Chapter 9

Arithmetic function

9.1 Arithmetic function

We have been implicitly using functions to aid our analysis of the integers, notably the GCD, LCM, and Euler's totient function. These are called *arithmetic functions*, and are used to characterize and relate integers in various contexts and through various means. It's often a way that inherently algebraic or combinatoric concepts are manifested in the realm of elementary probability theory.

An *arithmetic function* is a function $f : \mathbb{N} \setminus \{0\} \to \mathbb{C}$ with a domain of the positive integers and its image being a subset of the complex numbers.

9.2 Additivity and multiplicativity

An *additive function* is an arithmetic function where multiplication of coprime domain elements corresponds to addition of image elements.

$$f \text{ is additive} \iff [\gcd(a, b) = 1 \implies f(ab) = f(a) + f(b)]$$

A *totally additive function* drops the requirement for coprimality.

$$f \text{ is completely additive} \iff f(ab) = f(a) + f(b)$$

A *multiplicative function* is an arithmetic function where multiplication of coprime domain elements corresponds to multiplication of image elements.

$$f \text{ is multiplicative} \iff [\gcd(a, b) = 1 \implies f(ab) = f(a)f(b)]$$

A *totally multiplicative function* drops the requirement for coprimality.

$$f \text{ is totally multiplicative } \iff f(ab) = f(a)f(b)$$

9.3 Examples of familiar arithmetic functions

Chapter 10

Tau and Sigma function

10.1 Tau function

10.2 Sigma function

Chapter 11

Totient functions

- what does totient mean

11.1 Euler's totient function

11.2 Jordan's totient function

- Clash with Bessel function notation

11.3 Carmichael function

Definition 11.1. The *Carmichael function* $\lambda : \mathbb{N} \to \mathbb{N}$ is the totient function returning the smallest power that all integers coprime to n are congruent to $1 \mod n$.

$$\lambda(n) = \min\{m : \forall a \in \{a : \gcd(a, n) = 1\}[a^m \equiv 1 \mod n]\}$$

- Carmichael numbers

Chapter 12

Multiplicative function

12.1 Möbius function

- Möbius inversion formula

12.2 Liouville function

λ - Clash with Carmichael function notation

12.3 Partition function

p

12.4 Von Mangoldt function

Λ

Part IV

p-adic numbers