Elementary Number Theory

Zac Zerafa

December 16, 2025

Contents

Part I

Fundamentals

Chapter 1

Numbers

1.1 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.

1.1.1 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).

1.1.2 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 $\mathbb{Z}$.

1.1.3 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 $\mathbb{Q}$.

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

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.

1.2 Divisibility

1.2.1 Divisibility

We define divisibility as the following relation on the integers.

Definition 1.4. Given two integers a, b, *a divides b* iff a can be multiplied by some integer to obtain b. We denote this relation as $a|b$.

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

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

A basic way of classing integers is by their *parity*; whether they're odd or even. This is directly related to a number's divisibility by 2.

An *even number* is a number divisible by 2

$$n \text{ is even} \iff 2|n$$

An *odd number* is a number that is not even.

$$n \text{ is odd} \iff 2|(n-1)$$

The concept of divisibility is familiar from arithmetic, but a rigorous treatment of our arithmetic intuitions is vital to proving higher theorems. *Euclid's division lemma* will be our first step in this vain.

1.2.2 Euclid's division lemma

We can decompose any number with respect to another number in the following way.

Lemma 1.1 (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.

$$n = dq + r$$

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

Although basic, it is a strong tool that proves useful in much of elementary and algebraic number theory.

1.2.3 Multiples and factors

Definition 1.5. A *multiple* of a is some integer that a divides; an integer that equals a multiplied by some integer.

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

Given an integer n, there are an infinite amount of multiples of n since one can just multiply n by anything to construct a new multiple. This means n goes into infinitely many numbers, the smallest of which (ignoring negative multiples) is n itself.

n may have infinite multiples, but what can we say about the nnumbers that n is a multiple *of*? This leads us to a new concept of *divisors*.

Definition 1.6. A *factor* or *divisor* of a is some integer that divides a; an integer that can 'go into' a with no remainder.

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

Unlike multiples, a number n has a finite amount of divisors; the largest being n itself and the smallest being 1.

1.2.4 Lowest common multiple

Definition 1.7. The *lowest common multiple* $\text{lcm} : \mathbb{Z}^2 \to \mathbb{N}$ is a function of two elements a, b that returns the smallest number that both a and b divide.

$$\text{lcm}(a, b) = \min\{n \in \mathbb{N} : a|n \wedge b|n\}$$

The idea of an LCM is useful in problems where one wants to see where two methods of incrementing first reach an identical point. For example, if store A sells strawberries in lots of 6 and store B sells strawberries in lots of 8, what is the minimum amount of strawberries that one can obtain by going to either store?

1.2.5 Greatest common factor

Definition 1.8. The *greatest common factor (GCF)* or *greatest common divisor (GCD)* $\gcd : \mathbb{Z}^2 \to \mathbb{N}$ is a function of two elements a, b that returns the largest number that divides both a and b.

$$\gcd(a, b) = \max\{n \in \mathbb{N} : n|a \wedge n|b\}$$

Proposition 1.1.

$$\gcd(a,b)\mathrm{lcm}(a,b) = ab$$

Proposition 1.2.

$$\gcd(a,\mathrm{lcm}(b,c)) = \mathrm{lcm}(\gcd(a,b),\gcd(a,c))$$

Note that if you extend this function to contain more than 2 values this proposition does not hold. This is because if you consider a, b, c, there may be factors that b, c have in common that aren't shared with a, excluding it from the GCD.

1.2.6 Euclidean algorithm

We first develop the theory that Euclid had in mind.

Proposition 1.3.

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

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

1.2.7 Bézout's lemma

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

Lemma 1.2 (Bézout's lemma)**.**

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

There are 3 main approaches to proving Bézout's lemma

- *Constructive approach*; Performing extended Euclidean algorithm
- *Formalistic approach*; Proving that the smallest RHS divides any other RHS, and that the RHS divides and is divided $\gcd(a, b)$
- *Ring theoretic approach*; Prove that $J = \{d : ax + by = d, x, y \in \mathbb{Z}\}$ is a nontrivial integral ideal of $\mathbb{Z}$, then similarly show that all elements of this ideal divides and is divided $\gcd(a, b)$

That third approach uses the machinery of ring theory to do the exact same thing as that second approach, and the second approach operates on the same basis (Euclidean algorithm) of the first approach.

1.3 Primality

1.3.1 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 1.9. 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.

1.3.2 Euclid's theorem

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

Definition 1.10. The *primorial* is a function returning the product of the first n prime numbers.

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

Theorem 1.2 (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.

1.3.3 Pair of coprime numbers

Definition 1.11. A *pair of coprime numbers* are a pair of integers a, b such that ther GFC is 1.

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

In other words, a pair of coprime numbers (a, b) share no factor in common. This weakens the property of being prime; where all pairs (p, a) where $a < p$ share no common factor. There is much that can be said about this relationship between numbers, and it will be particularly prevalent in our study of arithmetic functions.

By the Euclidean algorithm, if n, q are coprime, then so are $n, n - q$. This simple fact was used by me to prove a lemma for a girl I liked.

Lemma 1.3 (Sofia's lemma)**.**

$$S(n) = \{q \in \mathbb{N} \cap [1, n - 1] : \gcd(n, q) = 1\}$$

$$\forall n \in \mathbb{N} \setminus \{0, 1, 2\}[n| \sum_{s \in S(n)} s]$$

1.3.4 Euclid's lemma

Lemma 1.4 (Euclid's lemma)**.**

$$p \text{ is prime } \wedge p|ab \implies [p|b \vee p|a]$$

One can extend this notion to a numbers coprime to one factor rather than just prime numbers.

Lemma 1.5 (Generalized Euclid's lemma)**.**

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

Proposition 1.4.

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

1.3.5 Naive factorization algorithm

Proposition 1.5 (Sieve of Eratosthenes)**.**

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

$D \leftarrow \{n\}$
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

1.3.6 Fundamental theorem of arithmetic

Now that suficient theory on prime numbers and their basic properties have been established, it is time to introduce perhaps the most powerful tool in number theory. It is perhaps an intuitive fact, but nonetheless central in understanding the nature of numbers.

Theorem 1.3 (Fundamental theorem of arithmetic)**.** For any natural number greater than 1, there exists a unique representation of that number n as a product of prime powers.

$$\forall n \in \mathbb{N} \setminus \{0,1\}(\exists!(n_i)_{i=1}^{k}[n = \prod_{i=1}^{k} p_i^{e_i}])$$

This theorem is named as such because arithmetic was the old name for number theory; Gauss preferred the word 'higher arithmetic' for number theory.

Many corollaries follow

Proposition 1.6.

$$a|c \wedge b|c \implies ab|c$$

Pairing the FTA with some basic combinatorics gives us a way to count the amount of factors a number has.

Proposition 1.7. Let $n = \prod_{i=1}^{k} p_i^{e_i}$, then n has $\prod_{i=1}^{k}(e_i + 1)$ factors.

1.3.7 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.

-

- Fermat prime - Mersenne prime

Chapter 2

Modular arithmetic

2.1 Introduction to modular arithmetic

Numbers with the same remainder when divided by n form an equivalence class; Modular arithmetic is basically a convenient notation for arithmetic on these n equivalence classes.

Definition 2.1 (Congruence)**.**

$$a \equiv b \mod n \iff n|a-b$$

The number n is called the *modulus*; multiples of n are congruent to 0.

2.1.1 Basic laws

Equivalence relation

$$a \equiv a \mod m$$

$$a \equiv b \mod m \implies b \equiv a \mod m$$

$$a \equiv b \mod m \wedge b \equiv c \mod m \implies a \equiv c \mod m$$

Since congruences form equivalence relations, one can write residues by means of the set containing all numbers with the same residue $\mod n$. This is a neat notational shortcut.

$$[a]_n = \{a + kn : k \in \mathbb{Z}\}$$

$$a \equiv b \mod n \iff [a]_n = [b]_n$$

$$\mathbb{Z} = \cup_{i=0}^{n} [i]_n$$

$$j \notin [i]_n \iff [i]_n \cap [j]_n = \emptyset$$

Essentially, these equivalence classes partition $\mathbb{Z}$ (equivalence classes don't overlap, and every integer must belong to some equivalence class).

We'll describe the set of all these equivalence classes by writing $\mathbb{Z}/n\mathbb{Z}$. This will represent all the elements in our new 'modular algebrae'; addition and multiplication of mod n equivalence classes.

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n : a \in \mathbb{Z}\}$$

We now check that addition and multiplication are well defined on this equivalence relation (consider equivalence classes $[a]_n, [b]_n$, there exists a $[c]_n$ such that any $x \in [a]_n, y \in [b]_n$ obeys $x + y \in [c]_n$).

$$a \equiv b \mod n \wedge x \equiv y \mod n \implies a + x \equiv b + y \mod n$$

$$a \equiv b \mod n \wedge x \equiv y \mod n \implies ax \equiv by \mod n$$

Here are some obvious corollaries that follow, however they are included to accustomize the reader's intuition to the behaviour of modular arithmetic.

$$\forall k \in \mathbb{Z}[a \equiv b \mod n \implies a + k \equiv b + k \mod n]$$

$$\forall k \in \mathbb{Z}[a \equiv b \mod n \implies ak \equiv bk \mod n]$$

$$\forall k \in \mathbb{N} \setminus \{0\}[a \equiv b \mod n \implies a^k \equiv b^k \mod n]$$

Cancellation laws

$$\forall n \in \mathbb{N} \setminus \{0\}[an \equiv bn \mod nm \implies a \equiv b \mod m]$$

$$\forall n \in \mathbb{N}[\gcd(n, m) = 1 \wedge an \equiv bn \mod m \implies a \equiv b \mod m]$$

$$\gcd(a, n) = 1 \wedge ax \equiv ay \mod n \implies x \equiv y \mod n$$

$$p \text{is prime} \implies ax \equiv l$$

2.2 Divisibility tests

A nice use for conguence is an efficient notation for understanding and proving divisibility tests.

-digital sum -digital root

Definition 2.2.

$$n = \sum_{i=0}^{k} 10^i d_i$$

$$\mathrm{ds}(n) = \sum_{i=0}^{k} d_i$$

$$\begin{aligned} 2|n &\iff 2|(n \mod 10) \\ 5|n &\iff 5|(n \mod 10) \\ 10|n &\iff n \equiv 0 \mod 10) \end{aligned}$$

$$\begin{aligned} 4|n &\iff 4|(n \mod 100) \\ 2^k|n &\iff 2^k|(n \mod 10^k) \\ 5^k|n &\iff 5^k|(n \mod 10^k) \end{aligned}$$

$$\begin{aligned} 3|n &\iff 3|\mathrm{dr}(n) \\ 9|n &\iff 9|\mathrm{dr}(n) \end{aligned}$$

11 7 13

-binary squaring

2.2.1 Modular multiplicative inverse

2.3 Euler's theorem

One may recall that our definitions for our 'modular algebrae' allows for addition and multiplication of equivalence classes to be well defined, but exponentiation definitely isn't; we can't reduce exponents to theie equivalence class in these algebrae.

That said, exponentiation inerpreted as repeated multiplication rather than its own operator allows us to talk about it in a limited setting (we've already proved one proposition relating to 'exponentiation'). There's also some group theory that can be used to give a deeper understanding of what is occuring, but we'll take an apporach that is accessible to those uninitiated in the wizardry of group theory.

Perhaps the most interesting phenomenon of repeated multiplication om modular algebrae are Fermat's little theorem and its generalization Euler's theorem.

2.3.1 Fermat's little theorem

Theorem 2.1 (Fermat's little theorem)**.**

$$p \text{ is prime } \implies a^{p-1} \equiv 1 \mod p$$

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

2.3.2 Euler's totient function

Definition 2.3. *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 note one proposition that will be required to compare Fermat's version to Euler's.

Proposition 2.1.

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

2.3.3 Euler's theorem

Theorem 2.2 (Euler's theorem)**.**

$$\gcd(a, n) = 1 \implies a^{\varphi(n)} \equiv 1 \mod n$$

Notice that Euler's theorem reduces to Fermat's little theorem when n is prime. The underlying 'reason' for why Euler's theorem holds is not necessarily a numeric reason, but rather an algebraic one; studying group theory provides the tools to make this theorem almost trivial!

2.3.4 Primitive roots

Exponentiating an integer a coprime to the modulus by $\varphi(n)$ is a sure way to obtain an integer congruent to 1, however is t

Definition 2.4. A *primitive root modulo* n is an integer a with $\gcd(a, n) = 1$ such that $\varphi(n)$ is the smallest exponent such that $a^{\varphi(n) \equiv 1 \mod n}$ holds.

Proposition 2.2. a with $\gcd(a, n) = 1$ is a primitive root modulo n iff for any prime p dividing $\varphi(n)$, $a^{\frac{\varphi(n)}{p}} 1 \mod n$.

Honestly, a group theoretic approach is ideal for this study, however we can easily emulate the same ideas in an elementary setting.

We have an observation which allows us to enumerate the amount of primitive roots without even knowing them

Proposition 2.3. If there exists a primitive root modulo m, there are $\varphi(\varphi(n))$ of them.

The idea is that if r is a primitive root, then any r^k where k doesn't divide $\varphi(n)$ is a primitive root; this gives us a way of constructing $\varphi(\varphi(n))$ primitive roots. (From the group theoretic point of view, this is really asking for the amount of generators of $(\mathbb{Z}/n\mathbb{Z})^*$).

Proposition 2.4. There exists a primitive root modulo n iff n is 1,2,4 or a prime power p^k.

(Again with group theory, this is really asking when $(\mathbb{Z}/n\mathbb{Z})^*$ is a cyclic group).

2.3.5 Discrete logarithms

The theory of primitive roots, Fermat's little theorem and Euler's theorem proves powerful in studying discrete logarithms.

Definition 2.5. The *discrete logarithm* $\log_b(a)$ *modulo* m is any integer k solving the following.

$$a^k \equiv b \mod n$$

If a modulus admits a primitive root and we can find this primitive root, discrete logarithms become linear congruences! Let r be a primitive root, then we have $r^i \in [b]_n, r^j \in [a]_n$ our problem is as follows.

$$r^{jk} \equiv r^i \mod n$$

Since, we want to find the k satifying the following.

$$jk \equiv i \mod \varphi(n)$$

2.4 Chinese remainder theorem

Theorem 2.3 (Chinese remainder theorem)**.** Consider the following set of k simultaneous equations where the n_i are pairwise coprime with eachother.

$$\begin{cases} a_1 x \equiv r_1 \mod n_1 \\ \vdots \\ a_k x \equiv r_k \mod n_k \end{cases}$$

There exists a unique solution for x in $\mathbb{Z}/N\mathbb{Z}$, where $N = \prod_{i=1}^{k} n_i$.

By FTA, one can therefore break any modulo n problem into a sequence of modulo $p_i^{k_i}$ problems

The true power of the CRT is realizing that the problem of k congruences of coprime moduli is equivalent to some problem modulo $\prod_{i=1}^{k} n_i$. CRT asserts the uniqueness and existence of such a solution, however we can indeed form a constructive method to swap between the two.

Let $N = \prod_{i=1}^{k} n_i$, then if for k congruences $f(x) \equiv s_i \mod n_i$ (where the n_i are pairwise coprime)

$$f(x) \equiv \sum_{i=1}^{k} \frac{N}{n_i} r_i \mod N$$

Theorem 2.4. Consider the following set of k simultaneous equations where the n_i are pairwise coprime with eachother.

$$\begin{cases} f(x) \equiv 0 \mod n_1 \\ \vdots \\ f(x) \equiv 0 \mod n_k \end{cases}$$

If equation i has S_i solutions, then $f(x) \equiv 0 \mod N$ has $\prod_{i=1}^{k} S_i$ solutions for x in $\mathbb{Z}/N\mathbb{Z}$, where $N = \prod_{i=1}^{k} n_i$.

2.5 Quadratic residues

2.5.1 Modular quadratics

- quadratic residue

Definition 2.6 (Quadratic residue)**.** q is called a *quadratic residue modulo* n iff it is congruent to a square number mod n.

$$q \text{ is a quadratic residue modulo } n \iff \exists x \in \mathbb{Z}/n\mathbb{Z}[x^2 \equiv q \mod n]$$

It is useful to play around with quadratics mod n and wee what basic properties hold.

$$x^2 \equiv (n-x)^2 \mod n$$

The study of quadratic residues is simplified greatly when we considering the case where we have a prime modulus. When considering prime moduli, we use the Legendre symbol.

Definition 2.7 (Legendre symbol)**.** Let p be an odd prime, then the *legendre symbol* $\left(\frac{a}{p}\right)$ is defined as such.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue modulo p} \\ -1 & a \text{ is a quadratic nonresidue modulo p} \\ 0 & a \equiv 0 \mod p \end{cases}$$

We note some properties.

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

$$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$$

$$\left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right)$$

A crucial property of quadratic residues is the following.

Theorem 2.5. Let p be prime, then there are exactly $\frac{p-1}{2}$ unique quadratic residues in $\mathbb{Z}/p\mathbb{Z}$.

Here's fancy way to say the same thing with our new notation.

Corollary 2.1.

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$$

To prove this we require Lagrange's theorem.

2.5.2 Lagrange's theorem

There is a theorem due to Lagrange which proves extremely useful whenever we consider polynomials modulo some prime. Recall the idea that when p is prime $ax \equiv b \mod p$ has a unique solution in $\mathbb{Z}/p\mathbb{Z}$; Lagrange's theorem generalizes this proposition from linear functions topolynomials of any degree on $\mathbb{Z}/p\mathbb{Z}$.

Theorem 2.6 (Lagrange's theorem)**.** Let p be prime and $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. Either every coefficient is divisible by p, or the following conguence has $\deg(f)$ solutions in $\mathbb{Z}/p\mathbb{Z}$.

$$f(x) \equiv 0 \mod p$$

Imagine now that we have $\mathbb{Z}/m\mathbb{Z}$, where m is a product of distinct primes. We can make use of the Chinese remainder theorem to break the problem into multiple prime congruences and then apply Lagrange's theorem.

Corollary 2.2. Let $n = \prod_{i=1}^{k} p_i$ be a product of distinct prime and $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. Either every coefficient is divisible by p, or the following conguence has $k\deg(f)$ solutions in $\mathbb{Z}/n\mathbb{Z}$.

$$f(x) \equiv 0 \mod p$$

Lagrange's theorem also demonstrates great power in simplifying proofs; One remarkable theorem that can be proven by Lagrange's theorem is Wilson's theorem.

Theorem 2.7 (Wilson's theorem)**.**

$$p \text{ is prime} \iff (p-1)! \equiv -1 \mod p$$

With a prime modulus, every integer n has a unique inverse such that $n^{-1}n \equiv 1$. So when considering $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$, when an integer isn't its own inverse we can use commutativity to match each n in the product with its respective n^{-1} to get 1. We need to find which integers are their own inverse since they cannot match with anything in the product. This means we are to solve $x^2 \equiv 1 mod p$ which occurs only when x is 1 or -1 according to Lagrange's theorem. Therefore every other number is 'pairable' with its inverse to make 1, so we have the following.

$$(p-1)! \equiv \prod_{k=1}^{p-1} k \equiv \prod_{k=1}^{p-3} 1 \cdot 1 \cdot -1 \equiv -1 \mod p$$

Corollary 2.3.

$$p \text{ is prime } \implies [(\frac{p-1}{2})!]^2(-1)^{\frac{p-1}{2}} \equiv -1 \mod p$$

Furthermore, this corollary or Euler's criterion (to be covered) can be used to prove the following

Proposition 2.5.

$$\left(\frac{p-1}{p}\right) = 1 \iff p \equiv 1 \mod 4$$

Euler's criterion gives the Legendre symbol a more tangible form to work with. It can be proven using Fermat's little theorem and Lagrange's theorem (yet to be introduced) together, however there exists an even more elementary approach.

Theorem 2.8 (Euler's criterion)**.**

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$$

For the case where a is a quadratic residue, $a \equiv x^2 \mod p \implies a^{\frac{p-1}{2}} x^{p-1} \equiv 1 \mod p$ When a is a quadratic nonresidue, $x^2 \equiv 1 \mod p \implies x \equiv \pm 1 \mod p$, so therefore it must equal -1

2.5.3 Law of quadratic reciprocity

Lemma 2.1 (Gauss' lemma)**.**

$$a\mathbb{Z}/(\frac{p-1}{2})\mathbb{Z} = \{a, 2a, 3a, \ldots, (\frac{p-1}{2})a\}$$

$$n = |\{k \in a\mathbb{Z}/(\frac{p-1}{2}\mathbb{Z} : k > \frac{p-1}{2}\}|$$

$$\left(\frac{a}{p}\right) = (-1)^n$$

The proof works based on our favourite little fact that for prime moduli, for a fixed a, each ax is distinct for incongruent x.

$$(\frac{p-1}{2})! \equiv a^{\frac{p-1}{2}}(\frac{p-1}{2})!(-1)^n$$

$$1 \equiv a^{\frac{p-1}{2}}(-1)^n$$

$$a^{\frac{p-1}{2}} \equiv a^{p-1}(-1)^n$$

$$a^{\frac{p-1}{2}} \equiv (-1)^n$$

$$\left(\frac{a}{p}\right) \equiv (-1)^n$$

Theorem 2.9 (Law of quadratic reciprocity)**.**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

2.6 Ring theoretic formulation

After having learned the rudiments of modular arithmetic, we can analyze our work through the perspective of the algebraist.

2.6.1 Additive group of integers modulo n

2.6.2 Multiplicative group of integers modulo n

Since we know modular multiplicative inverses exist for numbers coprime to the modulus, we make $(\mathbb{Z}/n\mathbb{Z})^*$) only contain integers of $\mathbb{Z}/n\mathbb{Z}$ coprime to n since groups must have all elements invertible.

The fact that any ax has a unique solution mod p is actually analogous to the fact that $f(h) = gh$ is a bijection for any group. To compromise between group theory and number theory, we could say that $\mathbb{Z}/p\mathbb{Z}$ $f(n) = an$ is bijective.

When the modulus is prime, many desirable properties can be shown since evey element of the additive group (save 0) is still in the multiplicative group! This means that every element (except 0) is inveritible for multiplicative groups of prime moduli; this is why we can prove Fermat's little theorem, Lagrange's theorem, Wilson's theorem, and many more results. When our modulus isn't prime, we can establish the same results, however they'll only hold for the integers coprime to the modulus.

Even Euler's theorem that $a^{\varphi(n)} \equiv 1 \mod n$ is a trivial consequence of the group theoretic result that$g^{|G|} = 1_G$

A group of order n has $\varphi(n)$ generators, $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\varphi(n)$, and hence has $\varphi(\varphi(n))$ generators (i.e primitive roots).

2.6.3 Commutative ring of integers modulo n

Say we want to combine $(\mathbb{Z}/n\mathbb{Z})^+$ and $(\mathbb{Z}/n\mathbb{Z})^*$ into one algebraic structure. If we have $(\mathbb{Z}/n\mathbb{Z})^+$ as the base set, all the elements will be in our algebraic structure, but it is possible that for multiplication there will be elements without inverses (meaning that this structure will connect a group and a 'monoid'). On the other hand, if we have $(\mathbb{Z}/n\mathbb{Z})^*$ as the base set, we're missing the identity element for addition (0), and the set would never be closed under addition (my counter example is $(n-1)+1 = 0 \notin (\mathbb{Z}/n\mathbb{Z})^*$).

Though it sucks to lose invertibility, the former is definitely the better of the 2 cases, since having an ill-defined operation is just unacceptable. This additive group and multiplicative monoid combination is called a *ring*, and we also define the distributive law of multiplication with respect to addition.

Proposition 2.6. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring of two abelian groups.

When the modulus is prime, many desirable properties can be shown;

When studying quadratic residues, we often confined ourselves to prime moduli. The reason for this is because prime modular rings are fields; rings that can claim their invertibility back!

Proposition 2.7. Let p be prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

This is the necessary condition for Lagrange's theorem to hold; so the field properties have been implicitly working their magic whenever we employed Lagrange's theorem. This is the primary reason why the theorem is powerful to begin with!

Aurifeuillan factorization

Chapter 3

Integer sequences

3.1 Introduction to numeric sequences

We've studied some general concepts about $\mathbb{Z}$ like primality, divisibility, however perhaps we want to form a set of all integers that satisfy some certain property (for example, the set of all even integers, or the set of all prime numbers).

If there is some natural way to order these numbers satisfying our property, one could define an *integer sequence* for them; ordered tuples of integers.

This part will consider both integer properties and integer sequences, since the former can often be transformed into the latter.

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 is often used as notation to describe such numbers since integers are countable and well ordered.

Let's consider integer properties restricted to $\mathbb{N}$. If I is the set of nonnegative integers with a certain property, the well ordering principle states that we can order them into some integer sequence (not that we can't do this for $\mathbb{Z}$ since WOP doesn't hold).

Sometimes

Integer sequences such as these have arisen from curiosity about the integers, however many integer sequences have their origins in enumerative combinatorics; a field of math that studies counting problems. Some 'combinatorial' sequences are studied in a number theory setting, and some 'num-

ber theory' sequences are borrowed by combinatorics to calculate a quantity; number theory and combinatorics are quite intimately related.

Some 'integer sequences' are best interpreted rather as 'arithmetic functions' due to certain behaviours they exhibit when forming arithmetic on them. An entire chapter will be delegated to the study of the integer sequences of number theory (or at least integer sequences that I feel are historically number theoretic) as well as arithmetic functions. Though integer sequences studied in and of themselves find themselves in that chapter, integer sequences will be scattered throughout this book with the concepts they arise from.

Above all, there is one integer sequence 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.

3.2 Parity

An *even number* is a number divisible by 2

$$2n, n \in \mathbb{Z}$$

An *odd number* is a number that is not even.

$$2n + 1, n \in \mathbb{Z}$$

3.3 Arithmetic progression

-Closed form

3.4 Geometric progression

-Closed form

Therefore this part will also discuss properties of nonnegative integers.

3.5 n-gonal numbers

Definition 3.1 (Square number)**.** A *square number* is a number whose square root is an integer.

$$a \text{ is square} \iff \exists n \in \mathbb{N}[a = n^2]$$

One can prove that a square number n^2 is actually the sum of the first n odd numbers.

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

$$\forall n \in \mathbb{Z}[n^2 \equiv 1 \mod 4]$$

Definition 3.2 (Triangular number)**.** A *triangular number* is a number...

$$a \text{ is triangular} \iff \exists n \in \mathbb{N}[a = \sum_{k=1}^{n} k]$$

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

I can't go 2 seconds at a university without hearing the legend of Gauss rederiving this formula in his childhood, so I'll save myself the trouble and let your next 99 professors recount the story instead.

3.6 Recursive sequences

3.6.1 Fibonacci sequence

- Golden ratio; number such that it is equal to the ratio of one larger than it to itself.

$$\varphi = \frac{\varphi + 1}{\varphi}$$

$$\varphi = \frac{1 + \sqrt{5}}{2}$$

- binet's formula The Fibonacci recurrence relation is a second orer homogeneous difference equation.

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

$$\lim_{n\to\infty} \frac{F_n}{F_{n+1}} = \varphi$$

3.6.2 Lucas sequence

3.6.3 Pell sequence

Chapter 4

Rational sequences

4.1 Bernoulli numbers

4.1.1 Sums of powers

-Closed form

$$S_m(n) = \sum_{k=1}^{n} k^m$$

These sums have found use outside the realm of number theory; many engineering and physics problems since antiquity have had crossroads with sums of powers. Notably, these sums occur when calculating the Riemann integral of a polynomial. In this case, an alternative expression that avoids the use of summation would be useful in turning the series into a sequence; which is much easier to analyze for convergence.

Indeed one can show by induction that all sums of powers are representable by polynomials.

$$S_0(n) = n$$

$$S_1(n) = \frac{n(n+1)}{2}$$

$$S_2(n) = \frac{n(n+1)(2n+1)}{6}$$

$$S_3(n) = \frac{n^2(n+1)^2}{4}$$

4.1.2 Bernoulli numbers

Johann Bernoulli and Seki Takakazu were a Swiss and Japanese mathematicians who had both noticed patterns regarding the coefficients of the polynomial representations of the sums of powers. Johann calculated the polynomials for the first 10 sums of powers, and through some algebra heuristically noted the following.

Proposition 4.1 (Faulhaber's formula)**.**

$$\sum_{k=1}^{n-1} k^m = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m-k+1}$$

B_n was some mystery sequence unknown at the time, however today we have come to call them the *Bernoulli numbers*. Note that if we take $n = 1$ and multiply both sides by $(m + 1)$, we have a cleaner way in which we can formally define the Bernoulli numbers.

Definition 4.1. The *Bernoulli numbers* are the numbers fored by the sequence B_n such that the following is satisfied.

$$\sum_{k=0}^{m} \binom{m+1}{k} B_k = 0$$

I'm not going to lie, this definition isn't very elegant. The fact that we haven't got B_n on its own side of the equation is a little strange; this sequence is rather difficult to work with. We will progressively find nicer ways to define the Bernoulli numbers, the next best definition that we can derive is from the *exponential generation function* of the Bernoulli numbers; this is yet another result from daddy Euler.

For a sequence, its generating function is the function that sequence generates when they are used as coefficients for terms of a series. Why consider generating functions at all? Many number sequences are difficult to deal with, but if one can find a generating function with a closed form, it provides at least some edge to proving facts about said sequence; in combinatorics this is an extremely common technique. Since Bernoulli numbers are a bit of a tricky beast, a generating function is relatively useful in their study.

Proposition 4.2.

$$\sum_{n=1}^{\infty} B_n \frac{z^n}{n!} = \frac{z}{e^z - 1}$$

Many resources that I have studied use this as their definition of Bernoulli numbers. Although it is definitely better than 'our' definition, I believe it feels a bit arbitrary present this generating sequence without any elaboration. Euler had to leverage the original definition of Bernoulli numbers to obtain this result; so we too shouldn't put the cart before the horse.

4.1.3 Properties of Bernoulli numbers

$$\forall n \in \mathbb{N}(B_n \in \mathbb{Q})$$

$$\forall n \in \mathbb{N} \setminus \{0\}(B_{2n+1} = 0)$$

4.1.4 Applications of Bernoulli numbers

As well as their inclusion within the sums of powers formulae, Bernoulli numbers are frequently used in mathematical analysis as coefficients within taylor series

4.2 Harmonic numbers

Definition 4.2 (Harmonic number)**.** The *nth harmonic number* is defined in the following manner.

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

Generating function

$$\sum_{n=1}^{\infty} H_n z^n = \frac{-\ln(1-z)}{1-z}$$

Inductive form

$$H_n = H_{n-1} + \frac{1}{n}$$

Partial sum of consecutive harmonic numbers

$$\sum_{k=1}^{n} H_k = (n+1)H_n - n$$

Chapter 5

Elementary approach to Diophantine equations

5.1 Linear Diophantine equations

Definition 5.1. A *Diophantine equation* is an algebraic equation where solutions are restricted to integers.

Typically, x, y, z, w are reserved as variables for Diophantine equations, while other symbols represent constants; this book follows this convention.

Perhaps the most famous Diophantine equation is the following.

$$x^n + y^n = z^n, x, y, z \in \mathbb{Z}, n \in \mathbb{N}$$

Theorem 5.1 (Fermat's last theorem)**.**

$$\forall n \in \mathbb{N} \setminus \{0, 1, 2\}[\nexists a, b, c \in \mathbb{Z}[a^n + b^n = c^n]]$$

Though it was stated by Fermat at around 1637, the first proof was only published in 1995 by Andrew Wiles, making this an open problem for 358 years! It was though the machinery of algebraic geometry (specifically Iwasawa theory) that this conjecture was proven.

Methods from algebraic geometry prove extremely potent in the study of Diophantine equations due to the fact that these are algebraic equations that define geometric curves.

5.1.1 Linear Diophantine equation

Definition 5.2. A *linear Diophantine equation* is a Diophantine equation of the following form.

$$ax + by = c, a, b, c \in \mathbb{Z}$$

Proposition 5.1. Solutions (x, y) exist iff c is a multiple of $\gcd(a, b)$

One may note that linear Diophantine equations are strikingly similar to the equation featured in Bezout's identity.

One can generate an ordered pair by applying the extended Euclidean algorithm, however using this ordered pair one can generate an infinite amount of answers. The trick relies on adding and subtracting the LCM of a, b (the smallest integer that both ax' and bx' can create).

Proposition 5.2. Let the ordered pair (x, y) solve $ax + by = c$, then there exists solutions (x', y') defined as such is a solution for any $n \in \mathbb{Z}$.

$$x' = x + \frac{b}{\gcd(a, b)}n$$

$$y' = y - \frac{a}{\gcd(a, b)}n$$

Furthermore, this class represents all solutions to the linear Diophantine equation

5.1.2 Geometric analysis

$$y = \frac{a}{b}x + \frac{c}{b}$$

One may ask how many solutions have only positive integers? A geometric argument can admit a useful approximation; since solutions have constant length apart, we consider the positive length of the Diophantine line and the length between adjacent solutions.

$$n = \lfloor \frac{c}{ab} \rfloor$$

5.2 Homogeneous Diophantine equations

$$x^2 + y^2 = a, a \in \mathbb{Z}$$
$$\nexists a : x^2 + y^2 = a \iff a \equiv 3 \mod 4$$

All even numbers squared reduce to 0 modulo 4 since $(2n)^2 = 4n^2 \equiv 0 \mod 4$ and odd numbers 1 modulo 4 since $(2n-1)^2 = 4n^2-4n+1 = 4(n^2-n)+1 \equiv 1 \mod 4$. Therefore $x^2 + y^2$ can never reduce to 3 modulo 4 since the possible combinations are $0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 2$, excluding 3 from the possibilities. Therefore $a \equiv 3 \mod 4$ shows a disparity between the capabilities of the sum of two squares and a, proving the unsatisfiability of this diophantine equation.

Definition 5.3 (Pell's equation)**.**

$$x^2 - ny^2 = 1$$

5.2.1 Pythagorean triples

We will now study integer solutions to $x^2 + y^2 = z^2$.

x and y have the opposite sign

Theorem 5.2 (Euclid's formula)**.**

$$x = m^2 + n^2$$
$$y = 2nm$$
$$z = m^2 - n^2$$

5.2.2 Sum of two squares

Let's study integer solutions to $a^2+b^2 = n$. Our knwoledge of modular arithmetic, paired with the Brahmagupta-Fibonacci identity will prove essential here. Some geometric reasoning will also be beneficial to us.

By our study on squares modulo 4, we can deduce the following.

Theorem 5.3.

$$n3 \mod 4$$

This is a good start, but can we find a necessary and sufficient condition for n to be expressible as the sum of 2 squares?

Theorem 5.4. For an odd number n expressible in two distinct ways as sums of 2 squares, then n is composite and its factors are sums of 2 squares.

This can be proved by equating the distinct sum of 2 squares, constructing coprime factors, and then applying the Brahmagupta-Fibonacci identity.

Theorem 5.5 (Sum of two squares theorem)**.** n is a sum of 2 squares iff for each prime power factor p^k, $p^k 3 \mod 4$ when k is odd.

Chapter 6

Elementary arithmetic functions

6.1 Arithmetic function

6.1.1 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.

As we will see, arithmetic functions are also extremely useful for studying integer sequences (as we will see with *perfect numbers* and *Carmichael numbers*), and can even constitute as interesting integer sequences themselves!

6.1.2 Additivity and multiplicativity

Definition 6.1. 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.

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

Definition 6.2. 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.

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

6.1.3 Examples of familiar arithmetic functions

$! : \mathbb{N} \to \mathbb{N}$

$\varphi : \mathbb{N} \to \mathbb{N}$

6.2 Divisor functions

6.2.1 Divisor functions

$$\sigma_z(n) = \sum_{d|n} d^z$$

6.2.2 Tau function

The specific function $\sigma_0 = \tau$ simply counts divisors.

$$\sigma_0 \text{ is multiplicative}$$

$$\sigma_0(p) = 2$$

$$\sigma_0(p^n) = n + 1$$

$$\sigma_0(n\#) = 2^n$$

6.2.3 Higher order divisor function

The function $\sigma_1 = \sigma$ is the sum of divisors.

$$\sigma_1(p) = p + 1$$

$$\sigma_1 \text{ is multiplicative}$$

- pentagonal number theorem

6.2.4 Perfect numbers

σ_1 is intimately related to the inteeger sequence of *perfect numbers*.

First, we clarify the term proper divisor.

Definition 6.3. A *proper divisor of* n is a divisor n that isn't n.

Definition 6.4. A *perfect number* is an integer that equals the sum of its proper divisors.

$$n \text{ is perfect } \iff n = \sigma_1(n) - n$$

The multiplicative nature of σ_1 admits an elegant prood of the following.

Theorem 6.1 (Euclid-Euler theorem)**.**

$$n \text{ is perfect } \iff n = 2^{p-1}(2^p - 1) \wedge 2^p - 1 \text{ is prime}$$

6.3 Totient functions

The totient of a number is the count of numbers less than and coprime to that number. There have been many arithmetic functions related to this notion, however none as fundamental as Euler's.

6.3.1 Euler's totient function

-multiplicative -prime powers

$$\varphi(p^n) = p^n - p^{n-1}$$

$$\varphi(n^k) = n^{k-1}\varphi(n)$$

- euler product form - number equals sum of euler phis for each divisor (see Group Theory)

$$n = \sum_{d \in \mathbb{N} : d | n} \varphi(d)$$

- non coprime multiples in argument

6.3.2 Jordan's totient function

- Clash with Bessel function notation

6.3.3 Carmichael function

Ferma's little theorem is a curious result, and Euler's theorem is a powerful generalization. One may be tempted to ask however if $\varphi(n)$ is truly the smallest exponent such that $a^{\varphi(n)} \equiv 1 \mod n$ for any a where a, n are coprime.

We define an arithmetic function to characterize this.

Definition 6.5. 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 $1 \mod n$.

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

One can use basic group theory relating to cyclic groups to prove the following.

Proposition 6.1.

$$\lambda(n) = \begin{cases} \varphi(n) & n \in \{p^k : p \text{ is an odd prime } \wedge k \in \mathbb{N}\} \cup \{1, 2, 4\} \\ \frac{\varphi(n)}{2} & n = 2^r, r \geq 3 \\ \operatorname{lcm}(\lambda(n_1), \ldots, \lambda(n_k)) & n = \prod_{i=1}^{k} n_i, n_i \text{ are distinct prime powers} \end{cases}$$

Note that this first case of the Carmichael function is essentially when we have a primitive root!

Why should one care about the smallest exponent? Any exponent m with $a^m \equiv 1 \mod n$ (a, n coprime) divides $\lambda(n)$; this result doesn't necessarily hold for $\varphi(n)$.

It finds use in the study of Carmichael numbers and Korselt's theorem.

Definition 6.6. A *Carmichael number* is a composite number that satisfies the following, where $\gcd(a, n) = 1$.

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

n is a Carmichael number $\iff$ n is composite $\wedge \forall a \in \mathbb{N}[\gcd(a, n) = 1, a^{n-1} \equiv 1 \mod n$

Definition 6.7. A number is square-free iff each prime divisor has a multiplicity of 1.

$$n \text{ is square-free} \iff n = \prod_{i=1}^{k} p_i \wedge p_i \text{are distinct primes}$$

The following theorem gives an alternative characterization of Carmichael numbers, which relies on the minimal exponent given by the Carmichael function.

Theorem 6.2 (Korselt's theorem)**.** n is a Carmichael number iff it is square-free, and for each prime divisor of n (denoted p), $p - 1$ divides $n - 1$

$$n \text{ is a Carmichael number} \iff n = \prod_{i=1}^{k} p_i \wedge p_i \text{are distinct primes} \wedge p_i - 1 | n - 1$$

Carmichael numbers with a factor p^k have a factor p, so $a^{p-1} \equiv 1 \mod p$ as well as $a^{n-1} \equiv 1 \mod p$. Since $p - 1$ is the smallest value with such a property, $p - 1 | n - 1$. Carmichael numbers with factor p^k need to obey $a^{\lambda(p^k)} \equiv a^{p^{k-1}(p-1)} \equiv 1 \mod p^k$ as well as $a^{n-1} \equiv 1 \mod p^k$. $p^{k-1}(p-1) | n-1$. Since p^{k-1} can't divide $n-1$ since p^{k-1} divides n, $k = 1$ so n must be square free.

6.4 Multiplicative function

6.4.1 Möbius function

μ - Möbius inversion formula

6.4.2 Liouville function

λ - Clash with Carmichael function notation

6.4.3 Partition function

p

6.4.4 Von Mangoldt function

Λ

Part II

Advanced

Chapter 7

p-adic numbers

It's often useful to consider Diophantine equations on $\mathbb{Z}/p\mathbb{Z}$ to aid in its study on $\mathbb{Z}$. One caveat is that $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}$ is not injective; integers of the same equivalence class are indistinguishable under this analysis.

Our problem is that $\mathbb{Z}/p\mathbb{Z}$ is a finite algebraic structure (finite field), but $\mathbb{Z}$ is infinite; there is a loss of information in the process. One solution is to consider $\times_{k=1}^{\infty}\mathbb{Z}/p^k\mathbb{Z}$. $\mathbb{Z}/p^k\mathbb{Z}$

Lemma 7.1 (Hensel's lemma)**.** Let $f(x_k) \equiv 0 \mod p^k$, if $\gcd(p, f'(x_k)) = 1$, then there exists a $x_{k+1} = p^{k+1}m + a$ such that $f(x_{k+1}) \equiv 0 \mod p^{k+1}$ and $\frac{f(x_k)}{p^k} + mf'(x_k) \equiv 0 \mod p$.

Definition 7.1 (p-adic integers)**.** Let p be a prime number, $\mathbb{Z}_p$

Definition 7.2 (p-adic numbers)**.** Let p be a prime number, $\mathbb{Q}_p$