Number Theory
Fall 2022 Lecture Notes

Elisa Bellah

Contents

Preface

Broadly, number theory studies the additive and multiplicative properties of the integers. In this course, we will explore this subject from elementary, analytic, and algebraic perspectives. Our goal will be to cover basic topics and main results from a variety of areas. Topics include: the fundamental theorem of arithmetic, arithmetic functions, prime numbers and primitive roots (including applications in cryptography), Diophantine analysis, quadratic reciprocity, algebraic number theory, and the geometry of numbers.

These lectures notes will be updated each week as we progress through the course. I will be pulling from a variety of resources, all of which will be referenced in the bibliography. Some resources you may use a supplements include:

- Rosen's book on Elementary Number Theory ([**Ros00**])
- Pete Clark's notes from a similar course ([**Cla18**])
- Apostol's text on Analytic Number Theory ([**Apo76**]),
- Stewart and Tall's text on Algebraic Number Theory ([**ST16**]), and
- Keith Conrad's expository papers.

The following list will be updated as new notation appears in the notes.

List of Notation

$\mathbb{Z}$ - the set of integers

$S^{\times}$ - the set of nonzero elements of a set S

Chapter 1

The Fundamental Theorem of Arithmetic

1.1. Introduction

Our goal in this course is to survey some techniques used to study the additive and multiplicative properties of the integers. If we consider the integers under either of these operations individually, we know quite a bit about their structure. The integers under addition form a cyclic group, generated by the integer 1. The following theorem tells us that the prime numbers are the "building blocks" of the integers under multiplication. (Recall that a prime number p is an integer whose only positive divisors are 1 and p.) More formally, the primes generate the multiplicative group of $\mathbb{Q}^\times$ (noting that $\mathbb{Z}$ does not form a group under multiplication, so we must extend to a larger set).

Theorem 1.1 (The Fundamental Theorem of Arithmetic)**.** *Let n be any positive integer. Then, there exist prime numbers $p_1, p_2, \ldots, p_t$ and positive integers $k_1, k_2, \ldots, k_t$ so that*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}.$$

Furthermore, if we order our primes so that $p_1 < p_2 < \cdots < p_t$ then this representation is unique. We call this representation the prime factorization of n.

Example 1.2. We have the following prime factorizations

(1) $108 = 2^2 \cdot 3^3$

(2) $1485 = 3^3 \cdot 5 \cdot 11$

(3) $7663 = 79 \cdot 97$

In this chapter, we will prove Theorem 1.1 and look at some of its consequences. In future chapters, we'll explore some of the properties (and mysteries) of the prime numbers, as well as problems that arise when we "mix" our two operations.

1.2. Proof of the Fundamental Theorem

We need the following lemmas.

Lemma 1.3. *For a prime p and integers a, b, if $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Note that if p does not divide a, then $\gcd(p, a) = 1$. By the Euclidean algorithm, there exists integers x, y with

$$px + ay = 1.$$

Multiplying the above equation by b, we have

$$pxb + ayb = b. \tag{1.1}$$

Since we've assumed $p \mid ab$ we can write $ab = kp$ for some integer k. Substituting this into equation (1.1) we get $p(xb + yk) = b$, and so $p \mid b$. □

The proofs of the following two lemmas will be left as exercises.

Lemma 1.4. *For a prime p and integers $a_1, a_2, \ldots, a_n$, if $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_i$ for some $i \in \{1, \ldots, n\}$.*

Lemma 1.5. *Every positive integer is either a prime number or a product of prime numbers.*

We are now prepared to prove Theorem 1.1.

Proof of the Fundamental Theorem of Arithmetic. Let $n \in \mathbb{Z}_{>0}$. By Lemma 1.5, we know that n has a prime factorization. We need to show that this factorization is unique. Suppose that we can write n as

$$n = p_1 \cdots p_t = q_1 \cdots q_s,$$

where $p_1 \leq \cdots \leq p_t$ and $q_1 \leq \cdots \leq q_s$ are prime. *(Note here that we've allowed primes to be repeated, so that we do not need to keep track of powers. We need to show that $t = s$ and $p_i = q_i$ for all $i = 1, \ldots, t$).* We have $p_1 \mid q_1 \cdots q_s$, so by Lemma 1.4 we must have $p_1 \mid q_j$ for some $j \in \{1, \ldots, s\}$. Since p_1 and q_j are prime, this implies that $p_1 = q_j$ for some $j \in \{1, \ldots, s\}$. Relabelling our q_j so that $q_j = p_1$ gives

$$p_2 \cdots p_t = q_2 \cdots q_s.$$

Repeating this process gives

$$1 = q_{t+1} \cdots q_s,$$

and so we must have $s = t$ and $p_i = q_i$ for all $i = 1, \ldots, s$. □

1.3. Some Consequences of the Fundamental Theorem

The fundamental theorem is named for a good reason. If you want to study the multiplicative properties of the integers, this theorem is often going to be needed. In this section, we give some examples for how this theorem might be applied. Our goal here is to get comfortable with this theorem, since it will come up frequently throughout the course.

1.3.1. Greatest Common Divisors and Least Common Multiples. Recall for integers a and b, the *greatest common divisor* of a and b is the largest integer d so that $d \mid a$ and $d \mid b$, and is denoted $d = \gcd(a,b)$. The *least common multiple* of a and b is the smallest integer m so that $m = ak$ and $n = b\ell$, for some $k, \ell \in \mathbb{Z}$, and is denoted $m = \operatorname{lcm}(a,b)$. The Euclidean Algorithm gives us an efficient method to find the greatest common divisor of two integers. The following results give an alternate method to finding the greatest common divisor when the prime factorization is known, and two methods to find the least common multiple of two integers. We will first need the following lemma, whose proof is left as an exercise.

Lemma 1.6. *Suppose that a positive integer n has prime factorization $n = p_1^{k_1} \cdots p_t^{k_t}$. Then, the divisors of n are given by $n = p_1^{\ell_1} \cdots p_t^{\ell_t}$ where $0 \leq \ell_i \leq k_i$ for all $i = 1, \ldots, t$.*

Note that we have the following alternate representation for the prime factorization of an integer. Let $p_1, p_2, p_3, \ldots$ denote the set of prime numbers ordered so that

$$p_1 < p_2 < p_3 < \cdots$$

Then, for any integer n, we can write

$$n = \prod_{i=1}^{\infty} p_i^{k_i}$$

where $k_i \geq 0$. Observe that this representation is also unique. This notation will more easily allow us to compare prime factorizations.

Lemma 1.7. *Let a and b be positive integers with prime factorization*

$$a = \prod_{i=1}^{\infty} p_i^{k_i} \text{ and } b = \prod_{i=1}^{\infty} p_i^{r_i}.$$

Then, $\gcd(a,b) = \prod_{i=1}^{\infty} p_i^{min\{k_i, r_i\}}$ *and* $\operatorname{lcm}(a,b) = \prod_{i=1}^{\infty} p_i^{max\{k_i, r_i\}}$.

Proof. Let

$$d = \prod_{i=1}^{\infty} p_i^{\min\{k_i, r_i\}}.$$

Since $\min\{k_i, r_i\} \leq k_i$, then $d \mid a$. Similarly, since $\min\{k_i, r_i\} \leq r_i$, then $d \mid b$. So, d is a common divisor of a and b. Now, let

$$e = \prod_{i=1}^{\infty} p_i^{c_i}$$

be any common divisor of a and b. By Lemma 1.6, we must have $c_i \leq k_i$ and $c_i \leq r_i$. So, $c_i \leq \min\{k_i, r_i\}$ which gives that $e \leq d$. We leave the proof of the formula for the least common multiple as an exercise. □

Lemma 1.8. *Let a and b be positive integers. Then,*

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}.$$

Proof. Suppose that a and b have prime factorization

$$a = \prod_{i=1}^{\infty} p_i^{k_i} \text{ and } b = \prod_{i=1}^{\infty} p_i^{r_i}.$$

By Lemma 1.7 we know that

$$\gcd(a,b) = \prod_{i=1}^{\infty} p_i^{\min\{k_i,r_i\}}.$$

So,

$$\frac{ab}{\gcd(a,b)} = \prod_{i=1}^{\infty} p_i^{c_i},$$

where $c_i = k_i + r_i - \min\{k_i, r_i\}$. The result will then follow by Exercise 6 □

Example 1.9. We now have a few methods to compute greatest common divisors and least common multiples. For example,

(1) $\gcd(4,10) = 2$, $\operatorname{lcm}(4,10) = 20$

(2) $\gcd(74,383) = 1$, $\operatorname{lcm}(74,383) = 28342$

(3) $\gcd(160,192) = 32$, $\operatorname{lcm}(32,192) = 960$

1.3.2. Some Irrational Numbers.

We first recall the following proof, which you may have seen in an introduction to proofs course.

Theorem 1.10. *$\sqrt{2}$ is irrational.*

Proof. Suppose for a contradiction that $\sqrt{2}$ is rational. Then, there are coprime integers m, n so that

$$\sqrt{2} = \frac{m}{n}.$$

This gives

$$2n^2 = m^2, \tag{1.2}$$

and so $2 \mid m^2$. Since 2 is prime, then by Lemma 1.3 we have that $2 \mid m$. So we can write $m = 2\ell$ for some integer ℓ which gives $m^2 = 4\ell$. Substituting this into equation (1.2) gives

$$2n^2 = 4\ell \Rightarrow n^2 = 2\ell.$$

So, $2 \mid n^2$ which again implies that $2 \mid n$. But this contradicts our assumption that m and n are coprime. □

The Fundamental Theorem of Arithmetic will allow us to generalize this proof in order to characterize all irrational roots.

Theorem 1.11. *For a positive integer a, $\sqrt[k]{a}$ is rational if and only if $a = \ell^k$ for some integer ℓ.*

Proof. The backward direction is straightforward, since if $a = \ell^k$ then $\sqrt[k]{a} = \ell$ is rational. So suppose that $\sqrt[k]{a}$ is rational. Then, there exist coprime integers m, n so that

$$\sqrt[k]{a} = \frac{m}{n}.$$

This gives

$$a = \frac{m^k}{n^k}. \tag{1.3}$$

We claim that m^k and n^k are also coprime. To see this, suppose that m and n have prime factorizations

$$m = \prod_{i=1}^{\infty} p_i^{r_i} \text{ and } n = \prod_{i=1}^{\infty} p_i^{s_i}.$$

This gives the following prime factorizations of m^k and n^k

$$m^k = \prod_{i=1}^{\infty} p_i^{kr_i} \text{ and } n^k = \prod_{i=1}^{\infty} p_i^{ks_i}.$$

Since $\gcd(m,n) = 1$, then by Lemma 1.7 we have $\min\{r_i, s_i\} = 0$ for all $i = 1, \ldots, t$. For any i this gives

$$\min\{kr_i, ks_i\} = k \min\{r_i, s_i\} = 0,$$

and so $\gcd(m^k, n^k) = 1$. By equation (1.3) we know that $n^k \mid m^k$ and so it must be the case that n^k, which implies that $n = 1$, since we've assumed that a is positive. So, $a = m^k$ is a perfect kth power. □

1.3.3. Primes modulo 4. In future chapters, we'll look at a few different proofs of the infinitude of primes. Interestingly, it is also the case that there are infinitely many primes congruent to 1 and 3 modulo 4. Note that integers congruent to 0 and 2 modulo 4 are even, and there is only one even prime number. We use the Fundamental Theorem of Arithmetic to prove one of these cases, and leave the other as an exercise.

Theorem 1.12. *There are infinitely many prime numbers p with $p \equiv 3 \pmod 4$.*

Proof. Suppose for a contradiction that there are only finitely many primes congruent to 3 modulo 4, say $q_1 = 3, q_2, q_3, \ldots, q_r$. Let

$$Q = 4q_2q_3 \cdots q_r + 3. \tag{1.4}$$

Let Q has prime factorization

$$Q = p_1^{k_1} \cdots p_t^{k_t}.$$

If $p_i \equiv 1 \pmod 3$ for every $i = 1, \ldots, t$ then we would have $Q \equiv 1 \pmod 4$, but this contradicts equation (3.3). So, it must be the case that $p_i \equiv 3 \pmod 4$ for some $i \in \{1, \ldots, t\}$. But then $p_i = q_j$ for some $j \in \{1, \ldots, r\}$, which would mean that $q_j \mid Q$. This contradicts equation (3.3). □

Theorem 1.12 and Exercise 8 are special cases of the theorem below.

Theorem 1.13 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *If* $\gcd(a, m) = 1$*, then there are infinitely many primes p with $p \equiv a \pmod m$.*

This is a celebrated theorem in analytic number theory, which takes a bit more machinery from analytic number theory than we'll have time for in this course. If you are interested, you may look into Chapter 7 of [**Apo76**]. Further special cases are also covered in the expository paper of Keith Conrad referenced in [**Cond**].

1.3.4. Series of Reciprocals of Primes. This section will follow [**Cone**]. Recall that the harmonic series $\sum_{n=1}^{\infty} 1/n$ diverges. The following theorem tells us that the smaller sum of reciprocals of primes diverges as well.

Theorem 1.14. *Let $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$ be the set of all prime numbers. Then*

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

diverges.

Proof. Suppose that $\{p \in \mathbb{P} \mid p \leq n\} = \{p_1, p_2, \dots, p_\ell\}$ We have

$$\begin{aligned} \prod_{i=1}^{\ell} \frac{1}{1-\frac{1}{p}} &= \prod_{i=1}^{\ell} \sum_{k=0}^{\infty} \frac{1}{p^k}, \text{ by geometric series} \\ &= \sum_{k_i \in \mathbb{Z}_{\geq 0}} \frac{1}{p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}} \\ &> \sum_{k=1}^{n} \frac{1}{k}. \end{aligned}$$

The final equality can be seen by noting that that for any integer $0 < k \leq n$, if a prime p divides k, then we must have $p \leq n$. So, it must be the case that every integer smaller than n only has prime factors from the list $\{p_1, p_2, \dots, p_\ell\}$. Taking logs, we have

$$\log\left(\sum_{k=1}^{n} \frac{1}{k}\right) < \sum_{i=1}^{\ell} -\log\left(1 - \frac{1}{p_i}\right). \tag{1.5}$$

We claim that

$$-\log\left(1 - \frac{1}{p}\right) < \frac{1}{p} + \frac{1}{p^2}.$$

To see this, use calculus to verify that the function $f(x) = \log(1-x) + x + x^2$ is positive for $0 < x < 1$. So, by equation (1.5) we get

$$\log\left(\sum_{k=1}^{n} \frac{1}{k}\right) < \sum_{\substack{p \in \mathbb{P} \\ p \leq n}} \frac{1}{p} + \sum_{\substack{p \in \mathbb{P} \\ p \leq n}} \frac{1}{p^2}.$$

Taking $n \to \infty$ gives the desired result. □

Remark 1.15. Let S be any subset of prime numbers. Note that if we can show

$$\sum_{p \in S} \frac{1}{p}$$

is infinite, it must be the case that S is also infinite. This is of course true for any set of integers, but Theorem 1.14 tells us it is at least possible for this series to not be finite. This is in fact the method Dirichlet used to prove his theorem on primes in arithmetic progressions (see Theorem 1.13).

It is a famously open problem (called the *twin primes conjecture*) whether there are infinitely many primes p so that $p+2$ is also prime. Unfortunately the sum of reciprocals of twin primes converges, and so this approach above does not help us. The value the series of reciprocals of twin primes converges to is called *Brun's constant*. According to Keith Conrad, "Estimating this number is a difficult problem, and work on this in 1994 led to the discovery of a bug in an Intel Pentium chip."

Exercises

1. Prove Lemma 1.4.
2. Prove Lemma 1.5. (Hint: use strong induction).
3. Prove Lemma 1.6.
4. Complete the proof of Lemma 1.7. That is, show that
$$\operatorname{lcm}(a,b) = \prod_{i=1}^{\infty} p_i^{\max\{k_i,r_i\}}.$$
(Hint: observe that we can write $\max\{k_i,r_i\} = k_i + k_i'$ and $\max\{k_i,r_i\} = r_i + r_i'$ where $k_i', r_i' \geq 0$.)
5. For each pair of integers, compute $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ using any method discussed in Chapter 1. Make sure to show your work.
   (a) $a = 256, b = 160$
   (b) $a = 7544, b = 115$
   (c) $a = 8633, b = 8051$
6. This problem will complete the proof of Lemma 1.8. For integers x, y, show that $\min\{x,y\} + \max\{x,y\} = x + y$.
7. Let a, b, c be positive integers. If $a \mid bc$ and $\gcd(a,b) = 1$, show that $a \mid c$.
8. Prove that there are infinitely prime numbers p with $p \equiv 1 \pmod 4$.

Chapter 2

Arithmetic Functions

An *arithmetic function* is any function $f : \mathbb{Z}_{>0} \to \mathbb{C}$, and typically gives some description of arithmetic properties of the integers. These functions will also turn out to be useful in our study of primes and primitive roots in the following chapter. This chapter and some its exercises will follow Chapters 2 and 3 of [**Apo76**].

Some arithmetic functions of interest include:

(1) the prime counting function $\pi(n) = \#\{\text{primes } p : p \leq n\}$;

(2) the prime omega functions

$$\Omega(n) = \#\{\text{prime divisors of } n\}, \text{ and}$$

$$\omega(n) = \#\{\text{distinct prime divisors of } n\};$$

(3) the p-adic valuation function $\nu_p(n) = \max\{k : p^k \mid n\}$;

(4) the divisor functions

$$\sigma_k(n) = \sum_{d|n} d^k$$

(note that $\sigma_0(n)$ counts the number of positive divisors of n, and is typically denoted by $d(n)$, and $\sigma_1(n)$ gives the sum of the positive divisors of n, and is typically denoted by $\sigma(n)$); and

(5) the Euler totient function $\varphi(n) = \#\{\text{positive integers } k < n : \gcd(k, n) = 1\}$.

In this chapter, we'll look at some of these and further arithmetic functions in more detail. Many of the functions we study will share some of the following properties.

Definition 2.1. An arithmetic function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ is called *multiplicative* if

$$f(ab) = f(a)f(b) \tag{2.1}$$

whenever $\gcd(a, b) = 1$, and *completely multiplicative* if (2.1) holds for any pair of integers a, b. We call f *additive* if

$$f(ab) = f(a) + f(b) \tag{2.2}$$

whenever $\gcd(a, b) = 1$, and *completely additive* when (2.2) holds for any pair of integers a, b.

Example 2.2. For $\alpha \in \mathbb{C}$, the power function $N^{\alpha}(n) = n^{\alpha}$ is completely multiplicative. The functions $\Omega(n)$ and $\nu_p(n)$ are completely additive, and $\omega(n)$ is additive but not completely additive.

We leave the proof of the following theorem as an exercise.

Theorem 2.3. *Let f be an arithmetic function with $f(1) = 1$. Then,*

(1) f is multiplicative if and only if

$$f(p_1^{k_1} \cdots p_t^{k_t}) = f(p_1^{k_1}) \cdots f(p_t^{k_t})$$

where $p_1, \ldots, p_t$ are distinct primes, and $k_1, \ldots, k_t$ are nonnegative integers;

(2) f is completely multiplicative if and only if f is multiplicative and

$$f(p^k) = f(p)^k$$

for any prime p and nonnegative integer k.

This tells us that when an arithmetic function is multiplicative, it is enough to study the function on prime powers.

2.1. The Euler Totient Function and the Möbius Function

In this section, we show that $\varphi(n)$ is multiplicative. Note that $\varphi(n)$ is not completely multiplicative, since for example

$$\varphi(2 \cdot 2) \neq \varphi(2)\varphi(2).$$

Observe that the Euler totient function counts the number of elements in the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$; that is

$$\#(\mathbb{Z}/n\mathbb{Z})^{\times} = \varphi(n).$$

It is then possible to prove the totient function is multiplicative as a consequence of Sun-tzu's theorem (usually refered to as the "Chinese Remainder Theorem"). We prove this instead by demonstrating an identity between $\varphi(n)$ and the Möbius function (defined below). This identity will allow us to give a complete formula for $\varphi(n)$ in terms of the prime factors of n.

Definition 2.4. For an integer $n \geq 2$, the Möbius function is defined by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases},$$

and we set $\mu(1) = 1$.

Note that $\mu(n) = 0$ only when n is not square-free (that is, n has a square divisor). We have the following identity between the totient and Möbius functions.

Theorem 2.5. *For any positive integer n we have*

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

We will first need some lemmas.

Lemma 2.6. *For an integer $n \geq 2$ we have*

$$\sum_{d|n} \mu(d) = 0.$$

Proof. Suppose m has prime factorization

$$m = p_1^{k_1} \cdots p_t^{k_t}.$$

By Lemma 1.6 we have

$$\begin{aligned}
\sum_{d|m} \mu(d) &= \sum_{i=1}^{t} \sum_{\ell_i=0}^{k_i} \mu(p_1^{\ell_1} \cdots p_t^{\ell_t}) \\
&= \sum_{i=1}^{t} \sum_{\ell_i=0}^{1} \mu(p_1^{\ell_1} \cdots p_t^{\ell_t}) \\
&= \mu(0) + \binom{t}{1}(-1)^1 + \binom{t}{2}(-1)^2 + \cdots + \binom{t}{t}(-1)^t \\
&= (1-1)^t = 0.
\end{aligned}$$

□

Lemma 2.7. *For an integer $n \geq 1$ we have*

$$\sum_{d|n} \varphi(d) = n.$$

Proof. Let $S = \{1, 2, \ldots, n\}$ and partition S into the disjoint sets given by

$$A(d) = \{k \in S : \gcd(k, n) = d\}.$$

Note that $\gcd(k, n) = d$ if and only if $\gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1$ and so

$$\#A(d) = \varphi(n/d).$$

So we have

$$\begin{aligned}
\sum_{d|n} \varphi(d) &= \sum_{d|n} \varphi(n/d) \\
&= \sum_{d|n} \#A(d) \\
&= n,
\end{aligned}$$

where the final equality holds because the sets $A(d)$ partition S. □

We are now prepared to prove our identity.

Proof of Theorem 2.5. Observe that, for a given integer ℓ we have

$$\left\lfloor \frac{1}{\ell} \right\rfloor = \begin{cases} 1 & \text{if } \ell = 1 \\ 0 & \text{if } \ell \neq 1. \end{cases}$$

So by Lemma 2.6, since $\mu(1) = 1$ then for any integer $m \geq 1$ we can write

$$\sum_{d|m} \mu(d) = \left\lfloor \frac{1}{m} \right\rfloor . \tag{2.3}$$

We have

$$\begin{aligned}
\varphi(n) &= \sum_{\substack{k \in \{1,\dots,n\} \\ \gcd(k,n)=1}} 1 \\
&= \sum_{k=1}^{n} \left\lfloor \frac{1}{\gcd(k,n)} \right\rfloor \\
&= \sum_{k=1}^{n} \sum_{d|\gcd(n,k)} \mu(d), \text{ by equation (2.3)} \\
&= \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d) \\
&= \sum_{d|n} \sum_{\substack{k \in \{1,\dots,n\} \\ k \text{ is a multiple of } d}} \mu(d) \\
&= \sum_{d|n} \mu(d) \sum_{\substack{k \in \{1,\dots,n\} \\ k \text{ is a multiple of } d}} 1 \\
&= \sum_{d|n} \mu(d) \frac{n}{d},
\end{aligned}$$

where the final inequality follows by counting the number of multiples of a divisor of n between 1 and n. □

As a consequence, we now have the following formula for $\varphi(n)$ in terms of the prime factors of n.

Theorem 2.8 (The Product Formula for $\varphi(n)$). *For $n \geq 2$ we have*

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Observe that if n has prime factorization $n = p_1^{k_1} \cdots p_t^{k_t}$ this gives

$$\varphi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1).$$

Proof. Suppose n has distinct prime factors $p_1, \ldots, p_t$. For convenience, we use the notation $[t] := \{1, \ldots, t\}$. We have

$$\begin{aligned}
&\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_t}\right)\\
&= 1 - \sum_{i\in[t]} \frac{1}{p_i} + \sum_{\substack{i_1,i_2\in[t]\\ i_1\neq i_2}} \frac{1}{p_{i_1}p_{i_2}} - \sum_{\substack{i_1,i_2,i_3\in[t]\\ i_1\neq i_2\neq i_3}} \frac{1}{p_{i_1}p_{i_2}p_{i_3}} + \cdots + (-1)^t \frac{1}{p_1p_2\cdots p_t}\\
&= \sum_{\substack{d\mid n\\ d \text{ square-free}}} \frac{(-1)^{\omega(d)}}{d}\\
&= \sum_{d\mid n} \frac{\mu(d)}{d}.
\end{aligned}$$

So, the result follows by Theorem 2.5 □

We now have the following Corollary, whose proof is left as an exercise.

Corollary 2.9. For a prime p and positive integers m, n we have

(1) $\varphi(p^a) = p^a - p^{a-1}$ for integers $a \geq 1$;

(2) $\varphi(mn) = \varphi(m)\varphi(n)\dfrac{g}{\varphi(g)}$, where $g = \gcd(m, n)$;

(3) φ is multiplicative;

(4) $a \mid b$ implies that $\varphi(a) \mid \varphi(b)$;

(5) $\varphi(n)$ is even for all integers $n \geq 3$. Furthermore, if n has r distinct odd prime factors, then $2^r \mid \varphi(n)$.

2.2. Dirichlet Products and Möbius Inversion

In Theorem 2.5 of the previous section, we proved the identity

$$\varphi(n) = \sum_{d\mid n} \mu(d)\frac{n}{d}.$$

The sum on the right-hand side of this equation is an example of a Dirichlet product, defined below.

Definition 2.10. Let f and g be arithmetic functions. The *Dirichlet product*, or *convolution*, of f and g is given by

$$f * g = \sum_{d\mid n} f(d)g\left(\frac{n}{d}\right).$$

We set notation for some common arithmetic functions used throughout the section:

$$\begin{aligned} \iota(n) &= n, \\ \mathbf{1}(n) &= 1, \text{ and} \\ I(n) &= \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}. \end{aligned}$$

Note that this product allows us to put a ring structure on the set of arithmetic functions with inverses given by the following theorem.

Theorem 2.11. *If f is an arithmetic function with $f(1) \neq 0$ there is a unique arithmetic function f^{-1} called the Dirichlet Inverse of f so that*

$$f * f^{-1} = f^{-1} * f = 1.$$

Proof. We give the construction of f^{-1} as in Theorem 2.8 of [**Apo76**] and leave the proof for the reader. The inverse of an arithmetic function f is defined recursively by

$$f^{-1}(1) = \frac{1}{f(1)}, \text{ and } f^{-1}(n) = \frac{-1}{f(n)} \sum_{\substack{d \mid n \\ d \neq n}} f\left(\frac{n}{d}\right) f^{-1}(d).$$

□

We have the following.

Theorem 2.12. *The set of arithmetic functions f with $f(1) \neq 0$ form a commutative ring under Dirichlet products and function addition with multiplicative identity I and inverses given as in Theorem 2.11. Note that by function addition we mean*

$$(f + g)(n) := f(n) + g(n).$$

We leave this proof as an exercise.

Observe that we can now restate some of the results from the previous section.

- Restatement of Theorem 2.5: $\varphi = \mu * \iota$.
- Restatement of Lemma 2.6: $\mu * \mathbf{1} = I$.
- Restatement of Lemma 2.7: $\varphi * \mathbf{1} = \iota$.

Our restatement of Lemma 2.6 along with Lemma 2.12 allows us to prove the very useful Möbius Inversion formula.

Theorem 2.13 (Möbius Inversion)**.** *Let f and g be arithmetic functions. We have*

$$f(n) = \sum_{d \mid n} g(d)$$

if and only if

$$g(n) = \sum_{d \mid n} f(d) \mu\left(\frac{n}{d}\right).$$

That is, $f = g * \mathbf{1}$ if and only if $g = f * \mu$.

Proof. If $f = g * \mathbf{1}$ then multiplying by μ gives

$$\begin{aligned} f * \mu &= (g * \mathbf{1}) * \mu \\ &= g * (\mu * \mathbf{1}), \text{ by Theorem 2.12} \\ &= g * I, \text{ by Lemma 2.6} \\ &= g, \text{ by Theorem 2.12.} \end{aligned}$$

Conversely, if $g = f * \mu$ then multiplying by $\mathbf{1}$ gives

$$\begin{aligned} g * \mathbf{1} &= (f * \mu) * \mathbf{1} \\ &= f * (\mu * \mathbf{1}), \text{ by Theorem 2.12} \\ &= f * I, \text{ by Lemma 2.6} \\ &= f, \text{ by Theorem 2.12.} \end{aligned}$$

□

We see then that Möbius inversion just follows from the fact that μ and I are multiplicative inverses in the ring of arithmetic functions. Observe that Theorem 2.5 is now a simple application of Möbius inversion to Lemma 2.7.

2.3. Applications of Möbius Inversion

This section demonstrates some applications of Möbius Inversion found in Chapter 8 of [**Cla18**].

2.3.1. A formula for cyclotomic polynomials.

Recall a *primitive nth root of unity* is any complex number ζ of order n in $\mathbb{C}^\times$. That is,

$$n = \min\{k \mid \zeta^k = 1\}.$$

The nth *cyclotomic polynomial* is defined as

$$\Phi_n(x) := \prod_{\substack{\text{primitive } n\text{th} \\ \text{roots of unity}}} (x - \zeta).$$

Observe the following identity:

$$\prod_{d|n} \Phi_d(x) = x^n - 1. \tag{2.4}$$

This follows because both sides of equation (2.4) are monic polynomials whose roots are given by the nth roots of unity, each with multiplicity 1. We use Möbius inversion to obtain the following formula for $\Phi_n(x)$.

Theorem 2.14. *For any integer $n \geq 1$ we have*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

Proof. Taking logs of equation (2.4) we have

$$\sum_{d|n} \log \Phi_d(x) = \log(x^n - 1).$$

By Möbius inversion, this gives

$$\begin{aligned}\log \Phi_n(x) &= \sum_{d|n} \log(x^d - 1)\mu\left(\frac{n}{d}\right)\\ &= \log\left(\prod_{d|n}(x^d-1)^{\mu(n/d)}\right),\end{aligned}$$

and so exponentiating gives the desired result. □

2.3.2. The number of irreducible polynomials over a finite field. We have the following classical application of Möbius inversion.

Theorem 2.15. *For a prime p, the number of irreducible polynomials of degree n over $\mathbb{F}_p$ is equal to*

$$\frac{1}{n}\sum_{d|n} p^d \mu\left(\frac{n}{d}\right).$$

The result will follow quickly from the following Lemma and Möbius inversion.

Lemma 2.16. *For a positive integer n and prime p, let $f \in \mathbb{F}_p[t]$ be given by $f = t^{p^n} - t$. Then f is equal to the product*

$$\prod_{\substack{m\in M(d)\\ d|n}} m.$$

where $M(d)$ denotes the set of all irreducible monic polynomials in $\mathbb{F}_p$ of degree d.

Proof. For convenience, we use the notation $\mathbb{F}_{(m)} := \mathbb{F}_p[t]/(m)$ for each $m \in M(d)$. Then in $\mathbb{F}_{(m)}$ we have

$$\begin{aligned} t^{p^n} - t = f = 0\\ \Rightarrow t^{p^n} = t\end{aligned}$$

So the order of t in the $\mathbb{F}_{(m)}^\times$ divides $p^n - 1$. Since t generates $\mathbb{F}_{(m)}$ over $\mathbb{F}_p$ then we must have $|\mathbb{F}_{(m)}^\times|$ divides $p^n - 1$. But since $\mathbb{F}_{(m)}$ is a degree d extension of $\mathbb{F}_p$ we know that $|\mathbb{F}_{(m)}^\times| = p^d - 1$. So $(p^d - 1) \mid (p^n - 1)$. By Exercise 14 this occurs if and only if $d \mid n$. To obtain our result, we must show that f is square-free (so that f does not contain repeated products of $m \in M(d)$). Observe that we have

$$f' = p^n t^{p^n - 1} - 1 = -1$$

in $\mathbb{F}_p$. So, f is separable (meaning that its roots are distinct in $\bar{\mathbb{F}}_p$). Since separable polynomials are square-free in characteristic p (can you show this? suppose not and get a common divisor of f and f'), f must be square free as desired. □

Now we can apply Möbius inversion to get our result.

Proof of Theorem 2.15. Let $I_p(d)$ be the arithmetic function that counts the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[t]$. Observe that

$$\deg \prod_{\substack{m\in M(d)\\ d|n}} m = \sum_{d|n} dI_p(d),$$

and so by Lemma 2.16 we have

$$\sum_{d|n} dI_p(d) = \deg f = q^n.$$

Applying Möbius inversion (noting that $dI_p(d)$ is an arithmetic function) yields

$$nI_p(n) = \sum_{d|n} q^d \mu\left(\frac{n}{d}\right).$$

Dividing by n completes the proof. □

2.4. Multiplicative Functions and Dirichlet Products

In this section, we show that the set of multiplicative function form an abelian group under Dirichlet products, and give a simple formula for the Dirichlet inverse of a completely multiplicative function.

Theorem 2.17. *If f and g are multiplicative functions, so is $f * g$.*

Proof. Let $h = f * g$. Let m, n be coprime integers and recall that

$$h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right).$$

Since $\gcd(m,n) = 1$ then every divisor d of mn can be written in the form $d = ab$ where $a \mid m$ and $b \mid n$. Furthermore, we have

$$\gcd\left(\frac{m}{a}, \frac{n}{b}\right) \leq \gcd(m,n) = 1.$$

Using that f and g are multiplicative gives

$$\begin{aligned} h(mn) &= \sum_{a|m}\sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right) \\ &= \sum_{a|m}\sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) \\ &= (f*g)(m)(f*g)(n) \\ &= h(m)h(n). \end{aligned}$$ □

Theorem 2.17 shows that multiplicative functions are closed under Dirichlet products. Since we know that the full set of arithmetic functions forms a ring under Dirichlet products, it is enough to show that the Dirichlet inverse of a multiplicative function is multiplicative. Rather than using the construction for Dirichlet inverses given in Theorem 2.11 (which is tricky to deal with) we use the following Lemma.

Lemma 2.18. *If g and $f * g$ are multiplicative, then f is also multiplicative.*

Proof. Suppose that f is not multiplicative, and note that it suffices to show $f * g$ is not multiplicative. Since f is not multiplicative, there exist coprime integers m, n with

$$f(mn) \neq f(m)f(n).$$

Choose such m, n so that mn is minimal. If $mn = 1$ then we would have

$$f(1) = f(1 \cdot 1) \neq f(1)f(1) \Rightarrow f(1) \neq 1.$$

Note that

$$(f * g)(1) = f(1)g(1)$$

by definition of the Dirichlet product. Since $g(1), f(1) \in \mathbb{Z}_{\geq 1}$ and $f(1) \neq 1$ then this gives $(f * g)(1) \neq 1$. By part (1) of Theorem 2.3 this tells us that $f * g$ is not multiplicative.

If $mn > 1$ then $f(ab) = f(a)f(b)$ for all pairs of positive coprime integers a, b with $ab < mn$. Arguing as in Theorem 2.17 we have

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\
&= f(mn)g(1) + \sum_{\substack{a|m, b|n \\ ab \neq mn}} f(ab)g\left(\frac{mn}{ab}\right) \\
&= f(mn)g(1) + \sum_{\substack{a|m \\ a \neq m}} f(a)g\left(\frac{m}{a}\right) \sum_{\substack{b|n \\ b \neq n}} f(b)g\left(\frac{n}{b}\right) \\
&= f(mn)g(1) - f(m)g(1)f(n)g(1) + (f * g)(mn) \\
&= g(1)(f(mn) - f(m)f(n)) + (f * g)(m)(f * g)(n).
\end{aligned}$$

Since we assumed $f(mn) \neq f(m)f(n)$ and we know that $g(1) \neq 0$, since g is an arithmetic function, then we have $(f * g)(mn) \neq (f * g)(m)(f * g)(n)$, and so $f * g$ is not multiplicative. □

We now have our main result.

Theorem 2.19. *The set of multiplicative functions form an abelian group under Dirichlet products.*

Proof. By Theorem 2.17 we know that multiplicative functions are closed under Dirichlet products. Now, for a multiplicative function f, since $f * f^{-1} = I$ is multiplicative then by Lemma 2.18 f^{-1} must be multiplicative as well. □

Note that it is difficult to use the construction of Dirichlet inverses given in theorem 2.11 to identify your Dirichlet inverse. The following result gives a simple formula for finding Dirichlet inverses of completely multiplicative functions.

Theorem 2.20. *Let f be multiplicative. If f is completely multiplicative, then*

$$f^{-1}(n) = \mu(n)f(n)$$

for all $n \geq 1$.

Proof. Let $g(n) = \mu(n)f(n)$. If f is completely multiplicative, then we have

$$\begin{aligned}(g * f)(n) &= \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)\\ &= \sum_{d|n} \mu(d)f(n)\\ &= f(n)\sum_{d|n}\mu(d)\\ &= f(n)(\mathbf{1} * \mu)(n)\\ &= f(n)I(n)\\ &= I(n),\end{aligned}$$

where the final equality follows because $f(1)I(1) = 1 \cdot I(1)$ and

$$f(n)I(n) = f(n) \cdot 0 = 0$$

for all $n > 1$. So, $g = f^{-1}$. □

In fact, the converse of Theorem 2.20 also holds. We leave this as an exercise for the reader.As an application of Theorem 2.20 we can obtain the Dirichlet inverse of the Euler totient function.

Theorem 2.21. *We have*

$$\varphi^{-1}(n) = \sum_{d|n} d\mu(d).$$

Proof. By Theorem 2.5 we have $\varphi = \mu * \iota$ and so

$$\varphi^{-1} = \mu^{-1} * \iota^{-1}.$$

By Lemma 2.6 we have $\mu^{-1} = \mathbf{1}$, and because $\iota(n) = n$ is completely multiplicative we get

$$\iota^{-1} = \mu\,\iota.$$

So this gives

$$\varphi^{-1} = \mu\,\iota * \mathbf{1} = \sum_{d|n} d\mu(d).$$

□

2.5. The Divisor Function and Perfect Numbers

Recall that the divisor functions are given by

$$\sigma_k(n) = \sum_{d|n} d^k.$$

We use Dirichlet products to give a short proof that σ_k is multiplicative, and leave the elementary proof of this fact as an exercise.

Theorem 2.22. *For any integer $k \geq 0$ the divisor function $\sigma_k(n)$ is multiplicative.*

Proof. Note that $\sigma_k = \mathbf{1} * N^k$, where N^k is the power function, which we showed was multiplicative in Example 2.2. Since $\mathbf{1}$ is also multiplicative, then our result follows by Lemma 2.17. □

By Theorem 2.3, it is then enough to study σ_k on prime powers. For a prime p and integer $a \geq 0$, by Lemma 1.6 the divisors of p^a are precisely

$$1, p, p^2, \ldots, p^a.$$

Since our sums are geometric, we get

$$\sigma_k(p^a) = \sum_{i=0}^{a} p^{ki} = \begin{cases} \dfrac{p^{k(a+1)} - 1}{p^k - 1} & \text{if } k \neq 0 \\ a + 1 & \text{if } k = 0. \end{cases}$$

The divisor functions are of particular interest in study perfect numbers, defined below.

Definition 2.23. A positive integer n is called *perfect* if $\sigma(n) = 2n$.

Example 2.24. The first five perfect numbers are $6, 28, 496, 8128$.

The following Theorem gives a complete characterization of all even perfect numbers.

Theorem 2.25. *An even integer n is perfect if and only if*

$$n = 2^{k-1}p$$

for an integer $k \geq 0$ and prime p of the form $p = 2^k - 1$.

Proof. Suppose that n is of the form $n = 2^{k-1}p$. Since σ is multiplicative and $p = 2^k - 1$ is odd, we have

$$\begin{aligned} \sigma(n) &= \sigma(2^{k-1})\sigma(p) = (2^k - 1)(1 + p) \\ &= (2^k - 1)(2^k) = 2n \end{aligned}$$

So n is perfect. Next, suppose that n is any even perfect number. Write

$$n = 2^{k-1}m,$$

for an odd integer m and $k \geq 2$. Since σ is multiplicative, we get

$$\sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Since n is perfect, this gives

$$\begin{aligned} 2n &= (2^k - 1)\sigma(m) \\ \Rightarrow 2^k m &= (2^k - 1)\sigma(m). \end{aligned}$$

So we must have $(2^k - 1) \mid m$. Write $m = (2^k - 1)\ell$ and so by above we get

$$2^k \ell = \sigma(m).$$

Since ℓ and m are divisors of m this gives

$$2^k \ell = \sigma(m) \geq \ell + m = 2^k \ell,$$

and so we must have $\sigma(m) = m + \ell$. That is, m only has two divisors. Since we know that $(2^k - 1) \mid m$ and $k \geq 2$ (since m is odd) then we must have $m = 2^k - 1$ as desired. □

Primes of the form $p = 2^k - 1$ are called *Mersenne primes*, which we will discuss in the next chapter. It is expected that there are infinitely many Mersenne primes, but this proof remains open. As we'll see in the next chapter, there are fast primality testing algorithms for Mersenne primes, and so most of the largest known primes are Mersenne.

While Theorem 2.25 gives a characterization of the even perfect numbers (or rather, passes this characterization off to studying the Mersenne primes), it is still unknown whether there exists an odd perfect number.

2.6. Bell Series

The following formal power series play a similar role to generating functions in combinatorics. Given a multiplicative function f, we would like information about $f(p^n)$ for primes p. To find this, we consider the series with these values as coefficients.

Definition 2.26. Given an arithmetic function f and prime p, the *Bell series* of f modulo p is the formal power series

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n)x^n.$$

The following result will be left as an exercise.

Theorem 2.27. *Let f and g be multiplicative functions. Then $f = g$ if and only if $f_p(x) = g_p(x)$ for all primes p.*

The following Theorem demonstrates how one might use Bell series to obtain identities between multiplicative functions.

Theorem 2.28. *Recall that $\omega(n)$ counts the number of distinct prime factors of n. We have*

$$2^{\omega(n)} = \sum_{d|n} \mu^2(d)$$

To prove this identity, we need the following lemmas, which are left as exercises.

Lemma 2.29. *For a prime p, we have*

$$\mu_p(x) = 1 - x,\ \mu_p^2(x) = 1 + x,\ \text{ and } \mathbf{1}_p(x) = \frac{1}{1-x}.$$

Lemma 2.30. *For arithmetic functions f and g, let $h = f * g$. For every prime p we have*

$$h_p(x) = f_p(x)g_p(x).$$

Proof of Theorem 2.28. Note that $f(n) = 2^{\omega(n)}$ is multiplicative, and we have

$$\begin{aligned} f_p(x) &= 1 + \sum_{n=1}^{\infty} 2^{\omega(p^n)} x^n \\ &= 1 + \sum_{n=1}^{\infty} 2x^n \\ &= 1 + \frac{2x}{1-x} \\ &= \frac{1+x}{1-x}. \end{aligned}$$

By Lemma 2.29 this gives $f_p(x) = \mu_p^2(x)\iota_p(x)$, and so by Lemma 2.30 we have $f = \mu^2 * \iota$, which gives our result. □

Exercises

1. Prove Theorem 2.3
2. Show that μ is multiplicative, but not completely multiplicative.
3. Recall that $\lfloor x \rfloor$ denotes the largest integer m with $m \leq x$. Let
$$f(n) = \lfloor \sqrt{n} \rfloor - \lfloor \sqrt{n-1} \rfloor.$$
Show that f is multiplicative but not completely multiplicative.
4. Determine if the following statement is true: if f is multiplicative, then
$$F(n) = \prod_{d|n} f(d)$$
is also multiplicative. Provide a proof or counterexample.
5. For any real number $\alpha > 1$, prove that an arithmetic function f is additive if and only if α^f is multiplicative.
6. Prove Corollary 2.9.
7. Find all positive integers n satisfying the following.
   (a) $\varphi(n) = m$ where $m = 1, 2, 3$, or 4
   (b) $\varphi(n) = 6$
   (c) $\varphi(n) = 12$
   (d) $\varphi(n) = n/2$
   (e) $\varphi(n) = \varphi(2n)$
8. Determine which of the following statements are true. Provide a proof or counterexample.
   (a) If $\gcd(m, n) = 1$ then $\gcd(\varphi(m), \varphi(n)) = 1$.
   (b) If n is composite, then $\gcd(n, \varphi(n)) > 1$.
   (c) If the set of distinct primes dividing m and the set of distinct primes dividing n are equal, then $n\varphi(m) = m\varphi(n)$.
9. Prove that for all n with $\omega(n) \leq 8$ we have $\varphi(n) > n/6$.

10. For a fixed positive integer k, show that if the equation $\varphi(n) = k$ has only one integer solution $n > 0$, then $36 \mid n$.
11. For a fixed positive integer k, show that the equation $\varphi(n) = k$ has only finitely many integer solutions $n > 0$.
12. Show that a positive integer n is composite if and only if $\varphi(n) \leq n - \sqrt{n}$.
13. Prove Theorem 2.12 (you may assume the set of arithmetic functions forms a group under addition). That is, for arithmetic functions f and g, show that
    (a) $f * g = g * f$,
    (b) $(f * g) * h = f * (g * h)$,
    (c) $f * I = f$, and
    (d) $f * (g + h) = f * g + f * h$.
14. This problem will complete the proof of Lemma 2.16. Show that
$$(p^d - 1) \mid (p^n - 1)$$
if and only if $d \mid n$.
15. Compute $\Phi_{12}(x)$ and use this to find an expression for the four 12th roots of unity in terms of radicals.
16. Suppose that n and k are positive integers with prime factorizations
$$n = p_1^{a_1} \cdots p_t^{a_t} \text{ and } k = p_1^{b_1} \cdots p_t^{b_t}$$
with $a_i, b_i \geq 1$. Show that $\Phi_n(x^k) = \Phi_{nk}(x)$.
17. Prove the converse of Theorem 2.20. That is, show that for a multiplicative function f, if
$$f^{-1}(n) = \mu(n) f(n)$$
for all $n \geq 1$ then f is completely multiplicative. (Hint: use part (2) of Theorem 2.3).
18. For a multiplicative function f, prove the following:
    (a) $f^{-1}(n) = \mu(n) f(n)$ for every square-free integer $n \geq 1$;
    (b) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ for every prime p.
19. Suppose that f is multiplicative. Prove that f is completely multiplicative if and only if $f^{-1}(p^a) = 0$ for all primes p and integer $n \geq 2$.
20. Give an elementary proof that the divisor functions $\sigma_k(n)$ are multiplicative.
21. Prove Theorem 2.27.
22. Prove Lemma 2.29.

Chapter 3

Prime Numbers

In Chapter 1 we saw that the primes form the “building blocks” of the integers. In this chapter, we’ll explore some of the properties of prime numbers, including their number and density, occurrence and patterns, primality tests, the structure of $(\mathbb{Z}/p\mathbb{Z})^\times$, and some cryptographic applications of these topics.

3.1. Proofs of the Infinitude of Primes

It has been known at least since the writing of Euclid’s *Elements* (around 300 BCE) that there are infinitely many prime numbers. Since then, number theorists have been reproving this fact. Exploring various proofs gives us new perspectives on the primes. We present Euclid’s original proof, as well as some of the proofs outlined in Chapter 1 of [**AZ18**]. Note that we have already seen one proof of the infinitude of the primes as a corollary to Theorem 1.14

Our first proof, due to Euclid, gives the motivating structure to the proofs seen in Section 1.3.3.

Eulid’s Proof. Suppose for a contradiction that there are only finitely many primes, call them $\{p_1, p_2, \ldots, p_k\}$. Then consider

$$Q = p_1p_2 \cdots p_k + 1$$

and note that $p_i \nmid Q$ for any i. So, for any prime divisor $p \mid Q$ we have $p \neq p_i$. So, p is not in our finite set of primes. □

The following proof uses many of the ideas we saw in Theorem 1.14.

Lower bounding the prime counting function. Recall the prime counting function is defined by

$$\pi(x) = \#\{\text{primes } p \mid p \leq x\}.$$

Note that we have

$$\begin{aligned}\log x &= \int_1^x \frac{1}{t}dt\\ &\leq 1+\frac{1}{2}+\cdots+\frac{1}{n}\\ &\leq \sum \frac{1}{k}.\end{aligned}$$

where the final sum goes over integers with prime $p \leq n$ (note that we saw this inequality in the proof of Theorem 1.14). Next, observe that

$$\sum \frac{1}{k} = \prod_{\substack{p\in\mathbb{P}\\ p\leq x}} \sum_{k\geq 0} \frac{1}{p^k} = \prod_{i=1}^{\pi(x)} \frac{1}{1-\frac{1}{p_k}},$$

where p_k denotes the kth prime. Since $p_k \geq k+1$ we get

$$\frac{1}{1-\frac{1}{p_k}} = \frac{p_k}{p_k-1} = 1+\frac{1}{p_k-1} \leq 1+\frac{1}{k} = \frac{k+1}{k}.$$

Putting this all together gives

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \frac{2}{1}\cdot\frac{3}{2}\cdot\frac{4}{3}\cdots\frac{\pi(x)+1}{\pi(x)} = \pi(x)+1.$$

So, $\pi(x) \geq \log x - 1$. This gives $\pi(x) \to \infty$ as $x \to \infty$, and so there must be infinitely many primes. □

The following two proofs show that certain sequences contain infinitely many prime divisors.

Proof with Fermat Numbers. The sequence of Fermat numbers is defined by $F_n = 2^{2^n}+1$, for $n \in \mathbb{Z}_{\geq 0}$. We claim that

$$\gcd(F_m, F_n) = 1$$

for any $m \neq n$, from which the infinitude of the primes follows immediately. To see this claim, it suffices to prove the identity

$$\prod_{k=0}^{n-1} F_k = F_n - 2,$$

for any integer $n \geq 1$. We leave the details as an exercise. □

Proof with Mersenne Numbers. Recall that Mersenne numbers are defined by $M_n = 2^n - 1$. For a contradiction, suppose that p is the largest prime number. Now, let q be a prime dividing M_p. Then, $2^p \equiv 1 (\mathrm{mod}\, q)$. So, the order of 2 divides p in $(\mathbb{Z}/q\mathbb{Z})^\times$. But since p is prime, the order of 2 must be equal to p in this group. By Lagrange's theorem, this gives $p \mid |(Z/q\mathbb{Z})^\times| = q-1$. Hence, $p < q$, which contradicts p being the largest prime. □

3.2. Primes in Lucas Sequences

The final two proofs in the previous section tell us that there are infinitely many prime *divisors* in the Fermat and Mersenne sequences. It is an open question whether there are infinitely many prime *terms* in these sequence. Results on the number of prime terms in nontrivial integer sequences are typically out of reach. Recall that Dirichlet's Theorem on primes in arithmetic progressions tells us there are infinitely many primes in the sequence

$$a, a+n, a+2n, \dots$$

when $\gcd(a,n) = 1$. While these sequences are (relatively) simple, this result already requires a good deal of machinery from analytic number theory to prove, so it is reasonable to lower our expectations for results on prime occurrence in more complicated sequences. In this section, we show that the Lucas sequences not only contain infinitely many prime divisors, but *every* term past a certain point contains a new prime divisor. First, we give some definitions.

Definition 3.1. A *linear recurrence sequence* $X = \{x_n\}$ is any integer sequence satisfying a recurrence of the form

$$x_{n+d} = \sum_{i=1}^{d} a_i x_{n+d-i},$$

for $a_i \in \mathbb{Z}$. When this recurrence is minimal, we say that X has *order d* and we call the values $x_0, \dots, x_{d-1}$ the *initial conditions* of the sequence X. The *characteristic roots* of X are the roots of the polynomial

$$f_X(t) = t^d - a_1 t^{d-1} - \cdots - a_d.$$

A linear recurrence sequence you are likely familiar with is the Fibonacci sequence $\{f_n\}$, which has initial conditions $f_0 = 0, f_1 = 1$ and satisfies the order 2 recurrence

$$f_{n+2} = f_{n+1} + f_n.$$

We have the following generalization of this sequence.

Definition 3.2. Given nonzero coprime integers P, Q, the *Lucas sequence* with integer parameters (P, Q) is the order two sequence $U(P,Q) = \{u_n\}$ with initial conditions $u_0 = 0$ and $u_1 = 1$ and satisfying

$$u_{n+2} = Pu_{n+1} - Qu_n.$$

Our goal in this section is to study prime divisors of Lucas sequences. To state our main result, we first need a few more definitions.

Definition 3.3. Given a prime p and sequence $X = \{x_n\}$, the *rank of apparition* (or *index*) of p in X is the value

$$m_p = \min\{m : p \mid x_m\}.$$

We call p a *primitive divisor* of the term x_m if $m = m_p$. That is, x_m is the first term in our sequence divisible by p. The *Zsigmondy set* of X is the set of terms $\mathcal{Z}(X)$ in X with no primitive divisors; that is

$$\mathcal{Z}(x) = \{x_m : m_p < m \text{ for all primes } p \mid x_m\}.$$

Example 3.4. Observe that $f_6 = 8$ is contained in the Zsigmondy set of the Fibonacci sequence, since 2 is the only prime divisor of f_6 but $m_2 = 3$.

In [**Car14**], Carmichael showed that for any Lucas sequence U with distinct real characteristic roots we have $\mathcal{Z}(U) \subseteq \{1, 2, 6, 12\}$. This result was extended in [**BHV01**] by Bilu, Hanrot and Voutier, who showed that the Zsigmondy set of any Lucas sequence (with real or complex-valued roots) and Lehmer sequence (a generalization of the Lucas sequences) is finite. The Zsigmondy set of Elliptic Divisibility Sequences, which are certain nonlinear recurrence sequences associated to the integer points on an elliptic curve, are known to be finite. Explicit information on bounds of the Zsigmondy set of Elliptic Divisibility Sequences and other recurrence sequences are topics of current interest (see [**Sil88**], [**IS12**], [**Sil13**], for example).

In this section, we'll prove Carmichael's theorem for the Fibonacci numbers. We first need some preliminaries.

Lemma 3.5 (Binet's Formula)**.** *Let α, β be the characteristic roots of the Lucas sequence $\{u_n\}$ with parameters (P, Q); that is, α, β are roots of $T^2 - PT + Q$. Then,*

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

We leave this proof as an exercise.

Recall the nth cyclotomic polynomial is given by

$$\Phi_n(x) = \prod_{\substack{\text{primitive } n\text{th} \\ \text{roots of unity } \zeta_n}} (x - \zeta_n).$$

We define the *homogeneous nth cyclotomic polynomial* to be

$$\Phi_n(x, y) := \prod (x - \zeta_n y).$$

Recall equation (2.4) gave

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

and so replacing x with x/y gives

$$x^n - y^n = \prod_{d|n} \Phi_d(x, y).$$

From this and Binet's formula (Lemma 3.5 above), we have

$$u_n = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(\alpha, \beta). \tag{3.1}$$

We will need to blackbox the following Lemma (we refer the reader to the proof of Corollary 2.2 in [**BHV01**], for example).

Lemma 3.6. *If α, β are characteristic roots of a Lucas sequence, then $\Phi_n(\alpha, \beta) \in \mathbb{Z}$*

From the discussion above and Lemma 3.6 we have the following.

Lemma 3.7. *For any Lucas sequence $\{u_n\}$, a prime p is a primitive divisor of u_n if and only if p is a primitive divisor of $\Phi_n(\alpha, \beta)$.*

We just need two more lemmas, and then we'll be prepared to prove Carmichael's Theorem for the Fibonacci sequence.

Lemma 3.8. *For an integer $n \neq 1, 2, 6$, suppose that n has distinct prime divisors $p_1, \ldots, p_k$. If*

$$|\Phi_n(\alpha, \beta)| > p_1 p_2 \cdots p_k,$$

then u_n contains a primitive divisor.

Proof. (Yubota's paper is missing an important step to this proof. This should follow from the fact that u_n is a divisibility sequence and so $p \mid u_n$ precisely when $m_p \mid n$. Unfortunately it's difficult to track down this argument; time permitting we may return to this, but for now let's blackbox it). □

Lemma 3.9. *If $n > 2$ and a is real with $|a| < 1/2$, then $\Phi_n(a) > 1 - |a| - |a|^2$.*

Proof. Recall from Theorem 2.14 we have

$$\Phi_n(a) = \prod_{d|n} (1 - a^{n/d})^{\mu(d)}.$$

Since $|a| < 1/2 \Rightarrow |a|^i < 1/2$ for any integer $i \geq 1$. So we have

$$-\frac{1}{2} < -|a|^i < 0$$

$$\Rightarrow \frac{1}{2} < 1 - |a|^i < 1.$$

This gives $(1 - |a|^i)^{\mu(d)} \geq 1 - |a|^i$, since $\mu(d) = 0, 1,$ or -1. Also observe that when $0 \leq x \leq 1$ and $0 \leq y \leq 1$ then

$$(1 - x)(1 - y) = 1 - x - y + xy \geq 1 - x - y$$

Putting this all together gives

$$\begin{aligned}
\Phi_n(a) &\geq \prod_{i=1}^{\infty} (1 - |a|^i) \\
&\geq (1 - |a|)(1 - |a|^2 - |a|^3 - |a|^4 - \cdots) \\
&= (1 - |a|) \left(1 - \frac{|a|^2}{1 - |a|}\right) \\
&= 1 - |a| - |a|^2.
\end{aligned}$$

□

We are now prepared to prove the following.

Theorem 3.10 (Carmichael's Theorem for the Fibonacci Sequence)**.** *Let $F = \{f_n\}$ be the Fibonacci sequence. Then, $\mathcal{Z}(F) = \{1, 2, 6, 12\}$.*

Proof. Observe first that the primitive nth roots of unity are precisely given by $\zeta = e^{2\pi ik/n}$ where $\gcd(k,n)=1$. So

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}} (x-\zeta^k),$$

which gives $\deg \Phi_n(x) = \varphi(n)$. So we have

$$\Phi_n(\alpha,\beta) = \alpha^{\varphi(n)}\Phi_n(\beta/\alpha). \tag{3.2}$$

Now, since the characteristic roots of the Fibonacci sequence are given by

$$\alpha = \frac{1+\sqrt{5}}{2} \text{ and } \beta = \frac{1-\sqrt{5}}{2},$$

and $|\beta/\alpha| = (3-\sqrt{5})/2 < 1/2$ then

$$\Phi_n(\beta/\alpha) \geq 1 - |\beta/\alpha| - |\beta/\alpha|^2 = 2\sqrt{5}-4 > 2/5.$$

So, from (3.2) and noting that $\alpha > 3/2$ we get

$$\Phi_n(\alpha,\beta) > (2/5)(3/2)^{\varphi(n)}.$$

So, by Lemma 3.8 what's left to show is that for an integer $n \neq 1,2,6,12$ with prime factors $p_1,\ldots,p_t$ we have

$$(2/5)(3/2)^{\varphi(n)} > p_1p_2\cdots p_t. \tag{3.3}$$

To do this, we will use the following fact, which is left as an exercise: let x,y be real numbers with $x>y>3$ and $m>2$ be an integer. Then

$$x^{m-1} > my. \tag{3.4}$$

Order our primes so that $p_1 < \cdots < p_t$. Suppose first that $p_1 \geq 11$. Then

$$(2/5)(3/2)^{\varphi(p_1)} > (2/5)(3/2)^{10} \approx 23 > p_1$$

$$\Rightarrow (3/2)^{\varphi(p_1)} > \frac{5}{2}p_1.$$

Using (3.4) this gives

$$(3/2)^{\varphi(p_1)\varphi(p_2)\cdots\varphi(p_t)} > (5/2)p_1p_2\cdots p_t.$$

Since φ is multiplicative, then by above we have

$$(2/5)(3/2)^{\varphi(n)} > (2/5)(3/2)^{\varphi(p_1)\cdots\varphi(p_t)} > p_1p_2\cdots p_t.$$

So, what's left to show is that equation (3.3) holds for integers $n \neq 1,2,6,12$ of the form

$$n = 2^a3^b5^c7^d.$$

If $a \geq 4$, $b \geq 3$, $c \geq 2$ or $d \geq 2$ then we can proceed similarly to above. The remaining cases can be checked by hand. We refer the reader to Yubota's paper for these details. □

3.3. Prime Density

In the previous section, we derived the following lower bound for the prime counting function

$$\pi(x) \geq \log x - 1.$$

The best known lower bounds are on the order of $x/\log(x)$, which matches what we know from the Prime Number Theorem, which states

$$\pi(x) \sim \frac{x}{\log(x)}.$$

Recall this notation means

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

In this section, we use elementary methods to show that there are much less primes than integers on a given interval. The correct formalism for this is the natural density, defined below.

Definition 3.11. Let A be a set of positive integers, and set

$$A(n) = \#\{a \in \mathbb{A} \mid a \leq n\}.$$

Then A has *(natural) density* $\delta(A) = \alpha$ if

$$\lim_{n\to\infty} \frac{A(n)}{n} = \alpha.$$

Example 3.12. For any positive integers a and N, the density of the set of positive integers satisfying $x \equiv a (\operatorname{mod} N)$ is $\frac{1}{N}$. In particular, the set of all positive integers whose last decimal digit is 1 has density $\frac{1}{10}$.

We have the following.

Theorem 3.13. *The set of prime numbers has natural density zero.*

Proof. The following proof is due to Erdős. We will study the binomial coefficient $\binom{2n}{n}$. First, note that a set with $2n$ elements has $2^{2n} = 4^n$ subsets. Since the number of n-element subsets of such a set is $\binom{2n}{n}$ we have the inequality

$$\binom{2n}{n} < 4^n.$$

Furthermore, $\binom{2n}{n} \in \mathbb{Z}$ and contains all primes p with $n+1 \leq p \leq 2n$. So,

$$\binom{2n}{n} > n^{\pi(2n)-\pi(n)}.$$

Combining the above gives $n^{\pi(2n)-\pi(n)} < 4^n$ and so taking logs we have

$$\pi(2n) - \pi(n) < \log(4) \cdot \frac{n}{\log n}.$$

Substituting $n = 2^k$ and summing gives

$$\sum_{k=2}^{2m} (\pi(2^k) - \pi(2^{k-1})) < \sum_{k=2}^{2m} \frac{2^k}{k-1}$$

On the left hand side we have a telescoping sum and so

$$\begin{aligned}\pi(2^{2m}) - \pi(2) &< \sum_{k=2}^{2m} \frac{2^k}{k-1} \\ &< \sum_{k=2}^{m} 2^k + \sum_{k=m+1}^{2m} \frac{2^k}{m} \\ &< 2^{m+1} + \frac{2^{2m+1}}{m}.\end{aligned}$$

So we know have an upper bound for $\pi(4^m)$ given by

$$\pi(4^m) < 1 + 2^{m+1} + \frac{2^{2m+1}}{m}. \tag{3.5}$$

Finally, for any real number x, there exists an integer m with $4^{m-1} < x \leq 4^m$ which gives

$$m - 1 < \log_4(x) \leq m.$$

Combining this with (3.5) we get

$$\begin{aligned}\pi(x) &\leq \pi(4^m) \\ &< 1 + 2^{m+1} + \frac{2^{2m+1}}{m} \\ &< 1 + 2^{\log_4(x)+2} + \frac{2^{2\log_4(x)+3}}{\log_4(x)} \\ &= 1 + 4\sqrt{x} + \frac{8x}{\log_4(x)}.\end{aligned}$$

So we have

$$\frac{\pi(x)}{x} < \frac{1}{x} + \frac{4}{\sqrt{x}} + \frac{8}{\log_4(x)} \to 0, \text{ as } x \to \infty.$$

□

3.4. Primality Tests

In the previous sections, we looked at patterns for primes in the set of integers. In this section, we instead consider how one might determine whether a single given integer p is prime. The naive approach would be to check all integers $2, 3, \ldots, p-1$ to see whether they divide p. In Exercise 7 we'll show that it suffices to only check for divisors up to $\sqrt{p}$. But for large primes p this becomes computationally infeasible. In this section, we present methods to check whether an integer is prime with "high probability". We will then see a fast deterministic test for Mersenne primes. Much of this chapter will follow Section 3.4 of [**HPS14**].

3.4.1. The Fermat Test and Carmichael Numbers.

Recall, for a prime p and integer $a \not\equiv 0 (\bmod p)$ we have

$$a^{p-1} \equiv 1 (\bmod p). \tag{3.6}$$

This is true either by Fermat's little theorem, or by Lagrange, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$. Note that this gives an immediate test for *compositeness*. For example,

$$2^6 = 64 \equiv 4 (\operatorname{mod} 6),$$

so we can conclude that 6 is not prime. Similarly,

$$2^{12257} \equiv 8502 (\operatorname{mod} 12257),$$

and so 12257 is not prime either. Of course, the converse isn't necessarily true. For example,

$$2^{1386} \equiv 1 (\operatorname{mod} 1387),$$

but $1387 = 19 \cdot 73$ is not prime. The following theorem will say that the situation above happens infrequently enough to give a reasonably good test for *primality*, except for some exceptional cases (unfortunately these exceptional cases end up causing a lot of trouble).

Theorem 3.14 (Fermat's Primality Test)**.** *Suppose that n is composite and there exists an integer a relatively prime to n with*

$$a^{n-1} \not\equiv 1 (mod n).$$

Then, at least half of the integers $w \in \{0, 1, \dots, n-1\}$ satisfy

$$w^{n-1} \not\equiv 1 (mod n).$$

We call such an integer w a Fermat witnesses for (the compositeness of) n. We call such a witness trivial if $\gcd(w, n) \neq 1$.

Proof. Let $G = \{a \mid a^{n-1} \equiv 1 (\operatorname{mod} n)\}$ and note that G is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Since there exists $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ that's not in G, then G has index at least 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$. That is,

$$|(\mathbb{Z}/n\mathbb{Z})^\times / G| \geq 2.$$

So, at least half of the elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ are Fermat witnesses for n. Since elements $w \in \{1, \dots, n\}$ with $\gcd(n, w) \neq 1$ are also Fermat witnesses, our claim follows. □

Observe that Theorem 3.14 does in fact give a probabilistic primality test. For example, assuming the conditions of Theorem 3.14 are satisfied, if we find that 10 integers $a \in \{1, \dots, p-1\}$ are *not* Fermat witnesses to n, then the "probability" that a is not prime is $1/2^{10} \approx 0.000098$. Meaning (roughly) that we can say with over 99% accuracy that n is prime. The trouble is that we have no way of testing whether the conditions of Theorem 3.14 are satisfied without finding a Fermat witness to n. And even worse, there exist composite numbers with *no* nontrivial Fermat witnesses.

Definition 3.15. A composite integer n is called *Carmichael* if it does not have any nontrivial Fermat witnesses. That is

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

for all $a \in \{1, \dots, n-1\}$ with $\gcd(a, n) = 1$.

Example 3.16. Observe that $n = 561$ is composite, with $n = 3 \cdot 11 \cdot 17$. We claim that n is Carmichael. To see this, we check that for all prime divisors p of n we have $(p-1) \mid (n-1)$:

$$3 - 1 = 2 \text{ divides } 560 = 2 \cdot 280$$

$$11 - 1 = 10 \text{ divides } 560 = 10 \cdot 56$$

$$17 - 1 = 16 \text{ divides} 560 = 16 \cdot 35.$$

Now, take any $a \in \{1, \ldots, n-1\}$ with $\gcd(a, n) = 1$. Then, $\gcd(a, p) = 1$ for all prime divisors of n and we have

$$a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 (\operatorname{mod} 3).$$

Similarly, we have

$$a^{560} \equiv 1 (\operatorname{mod} 11) \text{ and } a^{560} \equiv 1 (\operatorname{mod} 17).$$

So, $a^{560} - 1$ is divisible by the distinct primes $3, 11, 17$ and so $a^{560} - 1$ must be divisible by their product.

The following gives a characterization of all such numbers.

Theorem 3.17 (Korselt's criterion)**.** *For an integer n, $a^n \equiv a (mod n)$ for all itnegers a if and only if n is square-free and $(p-1) \mid (n-1)$ for all primes p dividing n.*

A proof of this criterion can be found in Theorem 2 of [**Cona**] from Conrad's expository notes. In [**AGP94**], Alford, Granville, and Pomerance showed that there are infinitely many Carmichael numbers, but little else is known about their occurrence. So for now, the Fermat test tells us with high probability if an integer is either prime or Carmichael, but has no way to distinguish between these cases. In the next section, we get a true probabilistic primality test.

3.4.2. The Miller-Rabin Test.

The Miller-Rabin primality test will extend the idea of the Fermat test by looking more carefully at the divisors of $p - 1$. This test was originally developed by Gary Miller here at CMU in the 1970s and was later updated by Michael Rabin in the 1980s. The key observation is as follows.

Theorem 3.18. *Let p be prime and write*

$$p - 1 = 2^k q,$$

for an integer $k \geq 1$ and odd integer q. Then for any $a \in \{1, \ldots, p-1\}$ one of the following must hold

(1) $a^q \equiv 1 (mod p)$, or

(2) $a^{2^\ell} q \equiv -1 (mod p)$ for some $\ell \in \{1, \ldots, k-1\}$.

Proof. Recall that $a^{p-1} \equiv 1 (\operatorname{mod} p)$. So we get

$$(a^q)^{2^k} \equiv 1 (\operatorname{mod} p).$$

If $a^q \equiv 1 (\operatorname{mod} p)$ then we're done. If not, observe that we have

$$(a^q)^{2^\ell} \not\equiv 1 (\operatorname{mod} p) \text{ and } (a^q)^{2^{\ell+1}} \equiv 1 (\operatorname{mod} p)$$

for some $\ell \in \{1, \ldots, k-1\}$. Furthermore, since p is prime, if $x^2 \equiv 1(\operatorname{mod} p)$ then $x \equiv \pm 1(\operatorname{mod} p)$ for any integer x. So we must have $(a^q)^{2^\ell} \equiv -1(\operatorname{mod} p)$ as desired. □

The following result gives an unconditional probabilistic primality test.

Theorem 3.19 (Miller-Rabin test)**.** *Suppose that n is an odd composite integer and write*

$$n-1 = 2^k q$$

where q is odd. Then at least half of the integers $w \in \{1, \ldots, n-1\}$ satisfy

$$w^q \not\equiv 1(mod\, n) \text{ and } (w^q)^{2^\ell} \not\equiv -1(mod\, n)$$

for all $\ell \in \{1, \ldots, k-1\}$. We call such an integer w a Miller-Rabin witness for n. As before, we say that w is a trivial witness if $\gcd(w, n) \neq 1$.

In fact, it's true that at least 75% of integers in $\{1, \ldots, k-1\}$ are Miller-Rabin witnesses for n. The proof of this is not much more difficult than what we discuss below, but is more lengthy than we have time for. We refer the reader to Section 5 of [**Conf**] for this argument. Note that every Miller-Rabin witness is a Fermat witness of n, so Theorem 3.14 could come as a corollary to Theorem 3.19.

Proof. We follow the proof given in [**Conf**]. As in the proof of Theorem 3.14, it suffices to show that the set of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ that are *not* Miller-Rabin witnesses for n are contained in a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. For the sake of time, we will only discuss the proof in the case that n is a prime power, and refer the reader to Theorem 4.1 of [**Conf**] for the case when n is not a prime power.

First, suppose that $n = p^\alpha$ for a prime p and $\alpha \geq 1$. We claim in this case that the set of integers $a \in \{1, \ldots, p-1\}$ that are not Miller-Rabin witnesses is equal to

$$\{a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid a^{p-1} \equiv 1(\operatorname{mod} n)\}.$$

To see this, note that $\gcd(a, n) = 1$ (otherwise a would trivially be a Miller-Rabin witness) and so by Lagrange's theorem we know that the order of a divides $\varphi(n)$. Also, since a is not a Miller-Rabin witnesses, then one of the following congruences hold

$$a^q \equiv 1(\operatorname{mod} n) \text{ or } a^{q2^\ell} \equiv -1(\operatorname{mod} n) \Rightarrow a^{q2^{\ell+1}} \equiv 1(\operatorname{mod} n)$$

for some $\ell \in \{1, \ldots, k-1\}$. In either case, we get that the order of a divides $n-1$. So, the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ must divide

$$\gcd(\varphi(n), n-1) = \gcd(p^{\alpha-1}(p-1), p^\alpha - 1) = p-1.$$

So, $a^{p-1} \equiv 1(\operatorname{mod} n)$. Conversely, suppose that $a^{p-1} \equiv 1(\operatorname{mod} n)$. Note that $(p-1) \mid (p^\alpha - 1) = 2^k q$ and so we can write $p - 1 = 2^j r$ where $j \leq k$ and $r \mid q$. Moreover, since

$$(a^r)^{2^j} = a^{p-1} \equiv 1(\operatorname{mod} n)$$

then the order of a^r divides 2^j. If the order of a^r is 1, then recalling that $q \mid r$

$$a^q = (a^r)^{q/r} \equiv 1(\operatorname{mod} n),$$

and so a is not a Miller-Rabin witness. If the order of a^r is larger than 1, say 2^ℓ then

$$(a^r)^{2^\ell} \equiv 1 (\operatorname{mod} p^\alpha)$$

and so by Exercise 11 we get

$$a^{q2^{\ell-1}} = (a^{r2^{\ell-1}})^{q/r} \equiv (-1)^{q/r} \equiv -1 (\operatorname{mod} p^\alpha),$$

recalling that $r \mid q$ are both odd. So a is not a Miller-Rabin witness in this case either. It is straightforward to check that

$$\{a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid a^{p-1} \equiv 1 (\operatorname{mod} n)\}$$

is a subgroup of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Furthermore, this is a proper subgroup, because $p+1$ has order $p^{\alpha-1}$ in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ (which you'll show in Exercise 12). □

It is actually expected that the Miller-Rabin test is deterministic. In particular, we have the following.

Theorem 3.20 ([**Bac90**]). *If the generalized Riemann hypothesis is true, then every odd composite integer n has a Miller-Rabin witness no larger than $2(\log n)^2$.*

Unfortunately, the Riemann hypothesis is very much an open problem, so for now this test is only probabilistic. While there does exist a polynomial-time deterministic primality test (called the AKS primality test, which we will not discuss here), it is much slower than the Miller-Rabin test. For cryptographic applications, Miller-Rabin is widely used.

3.4.3. The Lucas-Lehmer Test for Mersenne Primes.

While it is generally quite slow to search for large primes at random, there is a very fast deterministic algorithm to test whether a Mersenne number is prime. Recall that Mersenne numbers are of the form $M_n = 2^n - 1$. By Exercise 10 for M_p to be prime, we must have p prime as well.

The Lucas-Lehmer test for Mersenne primes considers the order one recurrence sequence $\{S_n\}$ with initial condition $S_1 = 4$ and recurrence

$$S_n = S_{n-1}^2 - 2.$$

Theorem 3.21 (The Lucas-Lehmer Primality Test). *Let p be prime. If $M_p \mid S_{p-1}$ them M_p is prime.*

Proof. We follow the proof given by J. W. Bruce in [**Bru93**], which gives a more elementary version of the proof from [**Ros88**]. For an exposition on the motivation behind this proof, see Terry Tao's blogpost [**Tao**].

For a contradiction, suppose that M_p is composite. Let q be its smallest prime divisor, and observe that

$$q^2 \leq M_p.$$

Note that $\mathbb{F} := (\mathbb{Z}/q\mathbb{Z})[\sqrt{3}]$ is a finite field with q^2 elements. Next consider

$$\omega = 2 + \sqrt{3} \text{ and } \omega = 2 - \sqrt{3}.$$

Since $\omega\bar{\omega} = 1$ then $\omega \in \mathbb{F}^\times$. In Exercise 10 we'll show that

$$S_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}.$$

Since we've assumed that $M_p \mid S_{p-1}$ and $q \mid M_p$ then thinking of the following equalities in $\mathbb{F}$ we have

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = 0$$
$$\Rightarrow \omega^{2^{p-2}} = -\bar{\omega}^{2^{p-2}}$$

and so multiplying both sides by $\omega^{2^{p-2}}$ gives

$$\omega^{2^{p-1}} = -1 \Rightarrow \omega^{2^p} = 1$$

in $\mathbb{F}$. That is, ω has order dividing 2^p in $\mathbb{F}^\times$. So,

$$2^p \leq |\mathbb{F}^\times| = q^2 - 1 \leq M_p - 1 = 2^p - 2,$$

a contradiction. □

Example 3.22. Let's show that $M_{13} = 2^{13} - 1 = 8191$ is prime. Note that we need to compute S_{12} but at each step we can reduce mod 8191. We have

n	$S_n (\mathrm{mod}\, M_p)$
1	4
2	14
3	194
4	4870
5	3953
6	5970
7	1857
8	36
9	1294
10	3470
11	128
12	0

Since $S_{12} \equiv 0 (\mathrm{mod}\, M_p)$ then by Theorem 3.21 we know that 8191 is prime. Recall this tells us that $n = 2^{12}(2^{13} - 1) = 33,550,336$ is perfect.

This algorithm is very efficient. While we do need to compute p terms of the recurrence sequence $\{S_n\}$ and check this congruence $S_p \equiv 0 (\mathrm{mod}\, M_p)$ this much faster than checking all possible divisors of $M_p = 2^p - 1$. Furthermore, we can reduce the terms of our sequence at each iteration mod M_p. Most of the largest known primes are Mersenne. As of September this year, the largest known prime is

$$2^{82,589,933} - 1.$$

Exercises

1. Show that
$$\prod_{k=0}^{n-1} F_k = F_n - 2,$$
for any integer $n \geq 1$. Use this to conclude that there are infinitely many prime numbers.
2. Show that $1, 2, 6$ and 12 are all in the Zsigmondy set of the Fibonacci sequence.
3. Prove Lemma 3.5. (Hint: induct on n)
4. The following problem will help finish the proof of Theorem 3.10: let x, y be real numbers with $x > y > 3$ and $m > 2$ be an integer. Then $x^{m-1} > my$.
5. Show that the set of odd positive integers has density 1/2.
6. Show that the set of integers with an odd number of decimal digits does not have a natural density.
7. Show that a composite integer n contains a divisor d with $d \leq \sqrt{n}$.
8. Prove that every Carmichael number must be odd.
9. Prove that a Carmichael number must be a product of distinct primes.
10. Prove that if n is a composite number, then $2^n - 1$ is not prime.
11. This problem will help finish the proof of Theorem 3.19: show that for an odd prime p and integer $\alpha \geq 1$, if $x^2 \equiv 1 (\bmod p^\alpha)$ then $x \equiv \pm 1 (\bmod p^\alpha)$.
12. This problem will also help to finish the proof of Theorem **??**: show that for any prime p and integer $\alpha \geq 1$, $p+1$ has order $p^{\alpha-1}$ in $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. (Hint: use the binomial theorem).
13. This problem will help finish the proof of Theorem 3.21. With the notation set in Theorem 3.21, show that for any integer $m \geq 1$ we have $S_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$.
14. Use the Miller-Rabin test to determine which of the following integers are prime with at least 99% accuracy. For those that are composite, provide a Miller-Rabin witness.
    (a) $n = 294409$
    (b) $n = 294439$
    (c) $n = 118901509$
    (d) $n = 118915387$
15. Use the Lucas-Lehmer test to show that the Mersenne numbers M_n are prime when $n = 17$ and $n = 19$.

Chapter 4

Diophantine Analysis

4.1. Introduction

Recall that our goal in this course is to survey some of the techniques used to study the integers under the operations of addition and multiplication. Since polynomial equations capture relations of these operations under the integers, it is naturally of interest to study their integer solution set. In this chapter, we give some of the fundamental definitions and discuss elementary techniques to study Diophantine equations. We will revisit this topic using the tools of algebraic number theory in a future chapter.

Given a polynomial $F \in \mathbb{Q}[X_1, \ldots, X_n]$ a *Diophantine equation* is any equation of the form

$$F(X_1, \ldots, X_n) = 0.$$

Diophantine analysis is the area of number theory concerned with finding integer (or rational) solutions to equations of this type. More specifically, given a Diophantine equation, a Diophantine problem might ask us to:

(1) Determine whether an integer or rational solution exists;

(2) Count the number of solutions or describe their distribution or density;

(3) Provide explicit descriptions of the solution set;

(4) Determine the arithmetic properties of the solution set.

This area of number theory is named after the Greek mathematician Diophantus of Alexandria, who authored the series *Arithmetica* around the 3rd century AD, and is attributed to beginning the formal study of such equations.

In the 1900s, David Hilbert posed the question of whether there is a general algorithm to determine the existence of integer solutions to a Diophantine equation. Unfortunately (or fortunately, depending on your perspective), in the 1970s Yuri Matiyasevich was able to answer this with a definitive “no”. The field of Diophantine analysis uses a wide array of techniques and pulls from many areas. In this chapter, we look at some Diophantine equations that can be solved through elementary methods, and consider some general strategies to solve Diophantine problems.

4.2. Linear Diophantine Equations

The following theorem completely characterizes solutions to linear Diophantine equations in two variables.

Theorem 4.1. *For integers a, b, c, the equation*

$$aX + bY = c \tag{4.1}$$

has an integer solution if and only if $d = \gcd(a, b)$ divides c. Moreover, if (x_0, y_0) is a solution to (4.1) then all solutions are of the form $(x(n), y(n))$ where

$$x(n) = x_0 + (b/d)n \text{ and } y(n) = y_0 - (a/d)n.$$

Proof. If $d \nmid c$, it is clear that equation (4.1) has no integer solutions. So, suppose that $d \mid c$. By the Euclidean algorithm, there exist $x, y \in \mathbb{Z}$ so that

$$ax + by = d,$$

and so $(x \cdot \frac{c}{d}, y \cdot \frac{c}{d})$ is a solution to (4.1). Next, suppose that (x_0, y_0) is any solution to (4.1). Then, for any other solution (x, y) we have

$$a(x - x_0) + b(y - y_0) = 0$$

$$\Rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Note that $\gcd(a/d, b/d) = 1$ and so $\frac{a}{d}$ divides $y_0 - y$. That is, there's an integer n with

$$y_0 - y = n \cdot \frac{a}{d} \Rightarrow y = y_0 - n \cdot \frac{a}{d}.$$

Plugging this into the equation above gives $x = x_0 + (b/d)n$. □

The following theorem is left as an exercise.

Theorem 4.2. *For nonzero integers $a_1, \ldots, a_n$, the equation*

$$a_1X_1 + \cdots + a_nX_n = c$$

has integer solutions if and only if $d = \gcd(a_1, \ldots, a_n)$ divides c. Furthermore, if there exists a solution, there are infinitely many.

Question for myself and all of you: is there a characterization to linear Diophantine equations in n varialbes similar to Theorem 4.1? (I'll add this as a bonus to Homework 6)

4.3. Congruences

The following simple observation is often useful in proving the nonexistence of solutions. Furthermore, this will motivate the "local-global" approach we discuss in a future section.

Proposition 4.3. If the Diophantine equation $F(X_1, \dots, X_n) = 0$ has an integer solution, then $F(X_1, \dots, X_n) \equiv 0 \bmod m$ has a solution in $(\mathbb{Z}/m\mathbb{Z})^2$ for any integer modulus n.

Proof. This is straightforward, since if $F(x_1, \dots, x_n) = 0$, then reducing everything modulo m gives $F(\bar{x}_1, \dots, \bar{x}_n) = 0$, where $\bar{x}_i \equiv x_i \bmod n$. □

The trick to this strategy is finding a suitable modulus. We give a few examples here, and leave some examples as exercises.

Example 4.4. Observe that $X^2 + Y^2 = 4Z + 3$ has no integer solutions, since reducing this equation modulo 4 we have

$$X^2 + Y^2 \equiv 3 (\bmod 4).$$

But, the squares mod 4 are precisely 0 and 1, neither of which sum to 3.

Example 4.5. We claim that the equation $Y^2 = X^3 + 7$ has no integral solutions.

Suppose that (x, y) is an integral solution. Note that if x were even, then we'd have

$$y^2 \equiv 7 (\bmod 8).$$

But the only squares modulo 8 are 0, 1, and 4. So, we must have x even, which means that y is odd. Next, observe that

$$y^2 = x^3 + 7 \Rightarrow y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4).$$

Furthermore, we can write $x^2 - 2x + 4 = (x-1)^2 + 3$. Since x is odd, then $x - 1$ is even and so $(x-1)^2 \equiv 0 (\bmod 4)$. So we have

$$(x-1)^2 + 3 \equiv 3 (\bmod 4).$$

Since x is odd, and $(x-1)^2 + 3$ is positive, this tells us that $(x-1)^2 + 3$ has a prime factor congruent to 3 modulo 4 (since otherwise all of its prime factors would be 1 modulo 4, contradicting what we found above by the fundamental theorem of arithmetic). Call this prime divisor p. Since $p \mid (x^2 - 2x + 4)$ then $p \mid (y^2 + 1)$. But that means

$$-1 = y^2 (\bmod p).$$

That is, -1 is a square modulo p. We claim this is a contradiction. To see this, raise the congruence above to the $(p-1)/2$ power to get

$$(-1)^{(p-1)/2} \equiv y^{p-1} \equiv 1 (\bmod p),$$

where the final equality follows by Fermat's little theorem (or Lagrange, depending on your style). Since $-1 \not\equiv 1 (\bmod p)$ for primes $p > 2$ then we must have $(p-1)/2$ even. That is, $p \equiv 1 (\bmod 4)$, but this contradicts the fact that p was a divisor congruent to 3 modulo 4.

Remark 4.6. Equations of the form $Y^2 = X^3 + n$ are called *Mordell equations*, and make up a special family of elliptic curves. It's known that every Mordell equation contains only finitely many integral ponits (in fact, this is true for any elliptic curve). There are a few general methods to solving a Mordell equation, but no known classification of solutions in general. In fact, Mordell equations are a topic of modern study (see [**BG15**], for example) Toward the end of this chapter, we give one more method to solve Mordell equations, which will be revisited at the end of the class.

Remark 4.7. Note that the converse of Proposition 4.3 does not hold. For example, it is clear that the equation $x^2 + 1 = 0$ has no integer solutions (since it has no rational solution) but modulo 5, $x = 2$ is a solution. In the following sections, we will show that in certain cases, it is enough to show that an equation has solutions modulo all possible primes. This is called a "local-global" approach.

4.4. Homogeneous Diophantine Equations

Note that so far, we've only been discussing integer solutions to Diophantine equations. Typically the area of Diophantine analysis restricts itself to these problems. In this section, we give a hint toward how the question of rational points is studied.

Definition 4.8. A polynomial F is said to be *homogeneous* if all of its terms are of equal degree. Otherwise, F is said to be *nonhomogeneous*. When F is nonhomogeneous, the degree of F is defined to be the largest degree of its terms.

Note that if F is homogeneous of degree d, then for any $\lambda \in \mathbb{Z}$ we have

$$F(\lambda X_1, \ldots, \lambda X_n) = \lambda^d F(X_1, \ldots, X_n).$$

So, for Diophantine equations defined by homogeneous polynomials, it suffices to study only the integer solution $(x_1, \ldots, x_n)$ with $\gcd(x_1, \ldots, x_n) = 1$.

Example 4.9. Observe that

$$F(X, Y, Z) = XY^2 - 3XYZ + Z^3$$

is homogeneous of degree 3, while

$$G(X, Y) = XY^2 - 3XY + 1$$

is nonhomogeneous of degree 3. However, the Diophantine equations

$$F(X, Y, Z) = 0 \text{ and } G(X, Y) = 0$$

are quite similar, since $Z^3 G(X/Z, Y/Z) = F(X, Y, Z)$. This gives a general strategy.

Definition 4.10. Given a polynomial $F(X_1, \ldots, X_n)$ of degree d the *homogenization* of F is the polynomial

$$F_H(X_1, \ldots, X_n, Z) := Z^d F(X_1/Z, \ldots, X_n/Z).$$

Observe that the homogenization of a polynomial is homogeneous. To see this, write

$$F(X_1, \ldots, X_n) = \sum a_i X_1^{k_{i1}} \cdots X_n^{k_{in}}.$$

Then,

$$F_H(X_1, \ldots, X_n, Z) = \sum a_i Z^{d - \sum k_{ij}} X_1^{k_{i1}} \cdots X_n^{k_{in}}.$$

So each term has degree $d - \sum k_{ij} + \sum k_{ij} = d$.

We have the following key observation.

Proposition 4.11. With the notation as above, the rational solutions to

$$F(X_1, \ldots, X_n) = 0$$

are in one-to-one correspondence with the integer solutions to $(x_1, \ldots, x_n, z)$

$$F_H(X_1, \ldots, X_n, Z) = 0$$

with $\gcd(x_1, \ldots, x_n, z) = 1$ and $z \neq 0$ to

Recall that the integer and rational solutions to a homogeneous Diophantine equation are equivalent. It turns out that the rational solution set of a homogeneous Diophantine equation makes up a well-behaved subset of a "projective variety", which are some of the main objects studied in algebraic geometry. It is often the case, then, that rational solutions to Diophantine equations are studied through this lens. Typically when people say "Diophantine analysis" this means the study of integer points on Diophantine equations, while the field of "arithmetic geometry" concerns rational solutions. These areas of course overlap quite a bit and it is not quite so clear cut. In the following section, we will see a characterization of solutions to homogeneous Diophantine equations of degree 2.

4.5. p-adic Numbers and the Local-Global Principle

In a previous section, we saw that solutions to a Diophantine equation in the integers imply solutions in $\mathbb{Z}/p\mathbb{Z}$, but unfortunately that the converse does not hold. If we replace $\mathbb{Z}$ with the p-adic integers (defined below), such a result does hold. While this doesn't seem to help our Diophantine problem at first glance, in this section we'll see that studying solutions "locally" (in the p-adic integer) can sometimes help us learn information about "global" (integer) solutions.

4.5.1. A brief introduction to p-adic numbers.

We first give the algebraic definition of the p-adic integers, as in [**Ser73**].

Definition 4.12. For a prime p, the *p-adic integers* $\mathbb{Z}_p$ as a set has as elements infinite tuples $(\ldots, x_2, x_1)$ with $x_m \in (\mathbb{Z}/p^m\mathbb{Z})$ that satisfy the condition

$$x_{m+1} \equiv x_m (\operatorname{mod} p^m).$$

We give $\mathbb{Z}_p$ a ring structure by considering it as a subring of $\prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$.

We typically write our tuples in opposite order for the following reason (which will not make any sense if you haven't seen category theory). If we let

$$\psi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}, x \mapsto x (\operatorname{mod} p^{n-1})$$

then we have a projective system

$$\cdots \to \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\psi_n} \cdots \xrightarrow{\psi_3} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\psi_2} \mathbb{Z}/p\mathbb{Z}.$$

Then, $\mathbb{Z}_p$ is precisely the inverse limit of this system

$$\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}.$$

Observe that we could instead represent the elements of $\mathbb{Z}_p$ as a formal power series. If we let

$$x = \sum_{n=0}^{\infty} b_i p^i$$

where $b_i \in \{0, \ldots, p-1\}$ then setting

$$\begin{aligned} x_1 &= x(\operatorname{mod} p) = b_0 \\ x_2 &= x(\operatorname{mod} p^2) = b_1 p + b_0 \\ &\vdots \\ x_n &= x(\operatorname{mod} p^n) = b_n p^n + \cdots + b_1 p + b_0 \end{aligned}$$

we see that $(\ldots, x_2, x_1) \in \mathbb{Z}_p$. Furthermore, any element in $\mathbb{Z}_p$ can be represented in this way. Oftentimes people will use this representation to write a p-adic integer in "decimal form" as $x = \ldots b_2 b_1 b_0$.

Example 4.13. Consider the element $x = (\ldots, 10, 10, 10, 1, 1) \in \mathbb{Z}_3$. Then we could write

$$x = \cdots + 0 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3^1 + 1 \cdot 3^0$$

and so in decimal form we have

$$x = 101.$$

Note as well that there is a natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ by sending

$$x \mapsto (\ldots, x(\operatorname{mod} p^3), x(\operatorname{mod} p^2), x(\operatorname{mod} p)).$$

Furthermore, the elements in $\mathbb{Z}_p$ that are mapped to by elements of $\mathbb{Z}$ are precisely those elements with terminating p-adic decimal representations.

Definition 4.14. Given a p-adic integer $x = (\ldots, x_3, x_2, x_1)$, if we have $x_k = 0$ for some $k \geq 1$ then we must have $x_\ell = 0$ for all $\ell = 1, \ldots, k$. That is, x is of the form

$$x = (\ldots, x_{k+1}, x_k, 0, 0, \ldots, 0).$$

The *p-adic valuation* of $x \in \mathbb{Z}_p$ is defined as follows

$$\nu_p(x) = \min\{n \mid x_n \neq 0\}.$$

Observe that this matches our notion of p-adic valuations in the integers, since for any $x \in \mathbb{Z}_p$ if $n = \nu_p(x)$ and we write

$$x = (\ldots, x_{n+1}, x_n, 0, \ldots, 0)$$

then it must be the case that $x_n = ap^n$ with $a \not\equiv 0(\operatorname{mod} p)$. So, we can write

$$x = (\ldots, p^n, p^n, 0, \ldots, 0) \cdot (\ldots, y_{n+2}, a, 0, \ldots, 0).$$

But $(\ldots, p^n, p^n, 0, \ldots, 0)$ is precisely the embedding of p^n into $\mathbb{Z}_p$. So, $\nu_p(x)$ is precisely the largest power of p we can factor out of our p-adic integer.

In exercise 6 we'll show that $\mathbb{Z}_p$ is in fact an integral domain, and so we can define the following.

Definition 4.15. The *p-adic numbers* $\mathbb{Q}_p$ are the field of fractions of $\mathbb{Z}_p$.

Remark 4.16. It can be shown that the units in $\mathbb{Z}_p$ are precisely those elements not divisible by p, which gives $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. So, elements in $\mathbb{Q}_p$ can be represented as infinite series

$$\sum_{i=-k}^{\infty} b_i p^i$$

and in decimal form as

$$\dots b_2 b_1 b_0 b_{-1} b_{-2} \dots b_{-k}.$$

Remark 4.17. Note that the p-adic numbers can also be defined analytically as the completion of $\mathbb{Q}$ with respect to the p-adic aboslute value, defined as

$$|x|_p := p^{-\nu_p(x)}.$$

Extending this absolute value to $\mathbb{Q}_p$ we can define

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \nu_p(x) \leq 1\}.$$

It can be shown that this matches our algebraic definition by using the uniqueness of completions. For the details of this and the previous remark, see Chapter 2 of [**Ser73**].

Next, we discuss how the solutions to polynomials equations defined over $\mathbb{Z}_p$ can be completely understood through their $\bmod p$ solutions.

4.5.2. Henel's Lemma.

The results in this section give a simple way to check for solutions to Diophantine equations over $\mathbb{Z}_p$. The proof of the results below are essentially a p-adic version of Newton's method. For time, we refer the reader to Section 2.2 of [**Ser73**] for these details. We first need some definitions.

Definition 4.18. Given a ring R and $f(X) = a_n X^n + \dots + a_1 X + a_0$, the *formal derivative* of f is defined as

$$f'(X) := n a_n X^{n-1} + \dots + 2a_2 X + a_1.$$

A solution $x \in R$ to $f(X) = 0$ is called a *simple zero* if $f'(x) \neq 0$.

The above definition also generalizes to polynomials in n variables.

Definition 4.19. Given a ring R and polynomial

$$f(X_1, \dots, X_n) = \sum a_i X_1^{k_{i1}} \cdots X_n^{k_{in}}$$

for $a_i \in R$, the *formal partial derivative* of f is defined as

$$f_{X_1} := \sum k_{i1} a_i X_1^{k_{i1}-1} X_2^{k_{i2}} \cdots X_n^{k_{in}},$$

and the remaining partial derivatives are defined similarly. We call a solution $x \in R^n$ to $f(X_1, \dots, X_n) = 0$ a *simple zero* if $f_{X_i}(x) \neq 0$ for some $i \in \{1, \dots, n\}$.

Example 4.20. Let $f(X, Y) = X^2 + Y^2 + 4$ in $(\mathbb{Z}/7\mathbb{Z})[X, Y]$. Then,

$$f(1, 3) = 14 \equiv 0 (\bmod 7)$$

and we have $f_X = 2X$ which gives $f_X(1, 3) \not\equiv 0 (\bmod 7)$. So, $(1, 3)$ is a simple zero of f. The following results will tell us that in fact $(1, 3)$ lifts to a zero in $\mathbb{Z}_7$.

Theorem 4.21 (Hensel's lemma). *For a polynomial f defined over $\mathbb{Z}_p$, every simple zero of f in $\mathbb{Z}/p\mathbb{Z}$ lifts to a zero in $\mathbb{Z}_p$. That is, if $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and $x \in \mathbb{Z}_p^n$ satisfies*

$$f(x) \equiv 0 (mod p) \text{ and } f_{X_i}(x) \not\equiv 0 (mod p)$$

for some $i \in \{1, \ldots, n\}$, then there is a unique $\tilde{x} \in \mathbb{Z}_p^n$ so that $f(\tilde{x}) = 0$ in $\mathbb{Z}_p$ and $\tilde{x} \equiv x (mod p)$.

4.5.3. The Local-Global principle. At first glance, it does not appear that Hensels' lemma helps with our Diophantine problem of finding integer solutions to polynomial equations. However, there is a sort of philosophy that in certain situations, to study a problem over $\mathbb{Q}$ it is enough to study it over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p. We call $\mathbb{R}$ and $\mathbb{Q}_p$ "local fields" and $\mathbb{Q}$ a global field. Note that the local fields are precisely the fields created by completing $\mathbb{Q}$ at its absolute values (by Ostrowski's theorem, which we have not discussed here, all absolute values are equivalent to either $|\cdot|_p$ or the usual absolute value $|\cdot|$). In the next section, we show that a local-global principle holds for quadratic forms.

4.5.4. Quadratic Forms. A *quadratic form* is a homogeneous polynomial of degree 2. We state a simplified version of the Hasse-Minkowski theorem below.

Theorem 4.22 (Hasse-Minkowski). *The equation $F(X_1, \ldots, X_n) = 0$ has a rational solution if and only if it has a solution over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.*

Proof. We give a sketch for the simplest part of this proof, and refer the reader to Adam Gamzon honor's thesis [**Gam06**] for a very clear and detailed writeup of this result. First observe that any quadratic form

$$F(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j$$

can be represented as

$$F(X_1, \ldots, X_n) = \begin{pmatrix} X_1 & \cdots & X_n \end{pmatrix} A \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

By diagonalizing A, we can make a change of variables that preserves integral solutions to $F(X_1, \ldots, X_n) = 0$ so that we can write

$$F(X_1, \ldots, X_n) = a_1 X_1 + \cdots + a_n X_n.$$

(see the upcoming Exercise 8, which I'll aim to think more carefully about soon!). The argument for Hasse-Minkowski considers the cases of $n = 2, 3$, and 4 separately by using various reductions, and then generalizes to $n \geq 5$. Let's just discuss the case when $n = 2$ to get some feel for how these arguments work.

Note that if $aX^2 + bY^2 = 0$ has a solution over a field k if and only if $-b/a$ is a square in k. Now, since $\mathbb{Q}$ is a subset of $\mathbb{R}$ and $\mathbb{Q}_p$, one direction of Hasse-Minkowski is clear. So suppose conversely that $aX^2 + bY^2 = 0$ has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p. Then, we must have $c = -b/a$ a square in $\mathbb{R}$ and $\mathbb{Q}_p$. We claim this implies c is a square in $\mathbb{Q}$. To see this, first note that c being a square in $\mathbb{R}$ means that $c > 0$. Now, write

$$c = p_1^{e_1} \cdots p_t^{e_t}$$

for $e_i \in \mathbb{Z}$, noting that $c \in \mathbb{Z} \hookrightarrow \mathbb{Z}_p$. Since c is a square in $\mathbb{Z}_p$ for all primes p we have $\nu_{p_i}(c)$ (which we recall is defined identically in $\mathbb{Z}$ and in $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$) is even for all i. Which gives c as a square. □

We finish this section with an application of Hasse-Minkowski. We first need a lemma, whose proof we omit (again, we refer the reader to the honor's thesis [**Gam06**] for the details).

Lemma 4.23. *If there exists a nontrivial integer solution to*

$$X^2 + Y^2 + Z^2 \equiv 0 (mod p)$$

then there exists a nontrivial integer solution to

$$X^2 + Y^2 + Z^2 \equiv k (mod p)$$

for any integer k. Note here that by "nontrivial" we mean a solution not equal to $(0, 0, 0)$.

Sweeping many details under the rug, we are now prepared to prove the following.

Theorem 4.24 (Lagrange)**.** *Every positive integer is a sum of four squares.*

Proof. Let $n \in \mathbb{Z}_{>0}$. Write $n = 4^a n'$ with $4 \nmid n'$. Suppose first that $n' \not\equiv 7 (\operatorname{mod} 8)$. We first show that n' is a sum of three squares. That is, we show there is a solution to the equation

$$X^2 + Y^2 + Z^2 = n'.$$

To see this, consider the equation

$$X^2 \equiv (-Y^2 - 1) (\operatorname{mod} p)$$

for an odd prime p. Note that the sets

$$\{x^2 \mid x \in \{0, \ldots, p-1\}\} \text{ and } \{-y^2 - 1 \mid y \in \{0, \ldots, p-1\}\}$$

both have precisely $(p+1)/2$ elements. Since there are only p available congruence classes, there must be a solution $(x, y, 1)$ to

$$X^2 + Y^2 + Z^2 \equiv 0 (\operatorname{mod} p),$$

and so by Lemma 4.23 we have a nontrivial solution (x, y, z) to

$$X^2 + Y^2 + Z^2 \equiv n' (\operatorname{mod} p).$$

Now, by Hensel's lemma, this lifts to a solution in $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ for all odd primes p. The solution in $\mathbb{Q}_2$ is a bit more delicate (not much more complicated, but we'd have to state some things more carefully), so let's take as fact there's a solution here as well. Finally, we have a solution $(\sqrt{n'}, 0, 0)$ to $X^2 + Y^2 + Z^2 = n'$ in $\mathbb{R}$. So, by Hasse-Minkowski there is an integer solution to

$$X^2 + Y^2 + Z^2 = n'.$$

Finally, if $n' \equiv 7 (\operatorname{mod} 8)$ then $n' - 1$ can be written as a sum of three squares as above, and so n' is a sum of four squares. □

4.6. Solutions by Unique Factorization

So far, our methods to study Diophantine equations have been "local", either by considering solutions in $\mathbb{Z}/p\mathbb{Z}$ or in $\mathbb{Z}_p$. There is also a global approach, which will lead naturally to our discussion in the next chapter. We consider a few examples.

Example 4.25. We claim that the only integral solution to $Y^2 = X^3 + X$ is $(0, 0, 0)$. To see this, suppose that (x, y, z) is a solution to this equation. Then we can write

$$y^2 = x(x^2 + 1).$$

But since $\gcd(x, x^2 + 1) = 1$ we must have x and $x^2 + 1$ equal to integer squares. In particular, this means that x^2 and $x^2 + 1$ are integer squares. The only way for this to happen is for $x^2 = 0$ which gives the desired solution.

Example 4.26. Next, we claim that the only integral solutions to $Y^2 = X^3 + 16$ are $(0, \pm 4)$. To see this, suppose that (x, y, z) is a solution to this equation. Then we can write

$$x^3 = (y + 4)(y - 4).$$

Suppose first that y is odd. Note that if $d \mid (y + 4)$ and $d \mid (y - 4)$ then we have

$$d \mid 2y \text{ and } d \mid 8.$$

Since $y + 4$ is odd we must have $\gcd(y + 4, y - 4) = 1$. So, it must be that both $y+4$ and $y-4$ are cubes. But, all cubes modulo 8 are odd, a contradiction because $y+4$ and $y-4$ have a difference of 8. Hence, y must be even. Next, since y is even x must also be even. So,

$$8 \mid (x^3 + 16) = y^2$$

and so $4 \mid y$ (otherwise, $\nu_2(y) = 1$ and so $\nu_2(y^2) = 2$ meaning $8 \nmid y^2$). Let $y = 4y'$. Then we get

$$16(y')^2 = x^3 + 16,$$

and so $16 \mid x^3 \Rightarrow 4 \mid x$. Write $x = 4x'$. From above, we see this makes y' odd and so we can write $y' = 2m + 1$. Putting this all together gives

$$\begin{aligned} 16(2m + 1)^2 &= (4x')^3 + 16 \\ \Rightarrow 4m^2 + 4m + 1 &= 4(x')^3 + 1 \\ \Rightarrow m(m + 1) &= (x')^3. \end{aligned}$$

But since $\gcd(m, m + 1) = 1$ when $m \geq 1$ it must be the case that m and $m + 1$ are both cubes. As before, there aren't many options for consecutive cubes, so we must have one of m or $m + 1$ equal to zero. That is, $x' = 0$ which gives $x = 0$ and so $y = \pm 4$.

You can solve a number of Diophantine equations in this way, but there is a very unfortunate roadblock to this approach. For example, say that we tried to find integer solutions to $Y^2 = X^3 - 5$. If we use the strategy of the previous examples, we'll need to factor over the larger ring $\mathbb{Z}[\sqrt{-5}]$. That is, if we have a solution (x, y, z) we could write

$$x^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

Perhaps we would like to argue that $y \pm \sqrt{-5}$ are relatively prime in this ring, and so each element must be a cube. Unfortunately, this would require that $\mathbb{Z}[\sqrt{-5}]$

has something like a fundamental theorem of arithmetic. That is, we would need this ring to be a UFD! But of course

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

verifies this ring does not have unique factorization.

Possibly the most famous Diophantine equation comes from Fermat, who claimed in the 17th century (without proof, because the margin of the book he was reading was “too narrow” to contain it) that the equation

$$X^n + Y^n = Z^n$$

has no nontrivial integer solutions when $n > 2$. The mathematician Gabriel Lamé thought he had produced a proof of this theorem in the 19th century using a similar method to what we’ve seen above. Unfortunately Lamés proof incorrectly assumed unique factorization in the cyclotomic fields $\mathbb{Z}[\zeta]$, where ζ an nth root of unity. It was later pointed out by Liouville that in fact these rings are not always UFDs (a fact proven around that time by Kummer). This is where the story of algebraic number theory begins. In the next chapter, we will study rings that are in some natural way analogous to the integers, and show that there is a way to extend the arithmetic properties of the integers to these objects that can help us resolve some Diophantine problems. While we will not be able to solve Fermat’s last theorem in full with these methods (this was only recently proven in the 1990s by Andrew Wiles, building off the work of many others), we will prove this theorem for a large family of Fermat equations. We will also revisit some Mordell equations and further Diophantine problems with this machinery.

Exercises

1. Show that for a polynomial F the homogenization F_H is in fact a homogeneous polynomial.
2. Prove Theorem 4.2.
3. Show that the only integral solution to $X^2 + Y^2 = (4a + 3)Z^2$ is $(0, 0, 0)$ for any $a \in \mathbb{Z}$.
4. Show that the Mordell equation $Y^2 = X^3 - 5$ has no integral solutions. *(Hint: rewrite this equation as $Y^2 + 4 = X^3 - 1$ and look modulo 4).*
5. Using Definition 4.12, prove that $\mathbb{Z}_p$ and $\mathbb{Z}[[X]]/(X-p)$ are isomorphic as rings.
6. Show that $\mathbb{Z}_p$ is an integral domain.
7. Show that the units in $\mathbb{Z}_p$ are precisely the elements not divisible by p.
8. (I’m going to think more about how to scaffold this diagonalization argument, I need to define some things carefully and be thoughtful about my phrasing)

Chapter 5

Algebraic Number Theory

In this Chapter, we cover some of the basic concepts of algebraic number theory. Once we develop some of the basic tools from this area, we will see a succinct proof of quadratic reciprocity, and show how some of the machinery from this chapter can be used to study further Diophantine problems. This chapter and its exercises will largely pull from Stewart and Tall's introductory text on algebraic number theory (see [**ST16**]).

5.1. Background and Basics

Recall in the previous chapter, if we would like to use our global tool of factoring a Diophantine equation, it is often useful to be able to factor over something larger than $\mathbb{Z}$. The main objects of algebraic number theory are precisely those elements; that is, elements which arise as roots of polynomials over $\mathbb{Z}$.

As a disclaimer, many people think of algebraic number theory as the area of mathematics that uses algebra to study number theory. This is somewhat true, but I think it is more fruitful to think of this area as *algebraic number* theory, rather than *algebraic* number theory; that is, as the area of mathematics that studies the algebraic numbers, and leads to some number theoretic consequences.

We have the following definitions.

Definition 5.1. Let α be a complex number.

(1) If α is the root of a monic polynomial (that is, the leading coefficient of f is 1) with rational coefficients, then α is called an *algebraic number*.

(2) If f has integer coefficients then α is called an *algebraic integer*.

(3) If f is a polynomial of smallest degree with α as a root, we call f the *minimal polynomial* of α, and often use the notation $f(X) =: m_\alpha(X)$. Note that Exercise 1 tells us this is well defined.

(4) The *degree* of an algebraic number is the degree of its minimal polynomial.

Example 5.2. We have that $\alpha = \sqrt{-5}$ is an algebraic integer with

$$m_\alpha(X) = X^2 + 5.$$

Note that $\beta = \sqrt{-5}/2$ is an algebraic number (but not an algebraic integer) with

$$m_\beta(X) = X^2 + \frac{5}{4}.$$

The (primitive) nth roots of unity ζ are also algebraic integers, since they are roots of the monic polynomial

$$f(X) = X^n - 1.$$

However, since $(X-1) \mid f(X)$, this polynomial is not of minimal degree when $\zeta \neq 1$. In a future section, we'll see that the cyclotomic polynomial $\Phi_n(X)$ studied in previous chapters is the minimal polynomial of any nth root of unity ζ.

Determining when a polynomial containing α as a root is the minimal polynomial can be quite difficult. The following Lemma gives one strategy.

Lemma 5.3. *For an algebraic number α and polynomial $f \in \mathbb{Z}[X]$ with $f(\alpha) = 0$, f is the minimal polynomial of α if and only if f is irreducible over $\mathbb{Q}$.*

Proof. If f is reducible, there exist $g, h \in \mathbb{Q}[X]$ with $f = gh$ and $\deg g, \deg h < \deg f$. So, we have $g(\alpha) = 0$ or $h(\alpha) = 0$, and so f is not a polynomial of smallest degree having α as a root. Conversely, suppose that f is irreducible with $f(\alpha) = 0$. Using the division algorithm in $\mathbb{Q}[X]$ we can divide m_α into f to get

$$f(X) = m_\alpha(X)q(X) + r(X)$$

with $0 \leq \deg r < \deg m_\alpha$. Plugging in α gives $r(\alpha) = 0$, and since m_α must be the polynomial of minimal degree with α has a root, we must have $\deg r = 0$. Furthermore, if $r(X) = c$ for a constant c then we'd have $c = r(\alpha) = 0$ so r is identically zero. So, m_α divides f, but since f is irreducible and monic, we must have $f = m_\alpha$. $\square$

Example 5.4. Let's find the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$. By Lemma 5.3 it suffices to find an irreducible polynomial with α as a root. We have

$$\alpha^2 = 7 + 2\sqrt{10}$$
$$\alpha^4 = 89 + 28\sqrt{10}$$

and so $\alpha^4 - 14\alpha^2 = -9$, which gives α as a root of

$$f(X) = X^4 - 14X^2 + 9.$$

This tells us that α is an algebraic integer. Next, we claim this polynomial is irreducible, so that α has degree 4. Suppose first that we could write

$$f(X) = (X - a)g(X)$$

for a cubic polynomial g. Reducing everything mod 7 gives

$$X^4 + 2 \equiv (X - a)g(X) (\bmod 7)$$
$$\Rightarrow a^4 \equiv -2 (\bmod 7).$$

But, the only squares mod 7 are 0, 1, 2 and 4, so no such value a can exist. That is, f does not have a linear factor. We leave it as an exercise to show that f also does not have a quadratic factor, and so f is irreducible.

Remark 5.5. In general it is quite challenging to determine whether a given polynomial is irreducible. Further techniques (such as the Eisenstein criterion and Gauss' lemma) are standard material in an field theory course. Many computer software programs can also check irreducibly of polynomials of small degree. For the sake of time, we omit any more of this discussion here.

Remark 5.6. A complex integer that is not algebraic is called *transcendental.* In Exercise 4 you'll show that transcendental numbers exist by proving that the set of algebraic numbers $\mathbb{A}$ is countably infinite. Giving an explicit construction of a transcendental number is quite challenging. The first such construction is attributed to Liouville in the 1800s. Using techniques in Diophantine approximation, Liouville showed that the constant (now referred to as the Liouville constant)

$$\sum_{n=1}^{\infty} 10^{-n!}$$

is transcendental. Later on, Lindemann showed π is transcendental. Diophantine approximation is a beautiful area of number theory with many contemporary applications. If you're interested in the area, I suggest taking a look at Schmidt's book [**Sch96**].

Next, we consider what fields we end up with when "adjoining" algebraic numbers to $\mathbb{Q}$. We first recall some of the basics from field theory.

5.1.1. Field Theory Basics.

Given a fields L and F, if $F \subseteq L$ we call L a *field extension* of F. Note that L is naturally an F-vector space, with vector addition just usual addition in L, and for $\lambda \in F$ and $v \in L$ scalar multiplication λv is just multiplication in L.

Definition 5.7. The dimension of L as an F-vector space is called the *degree* of L over F, and is denoted $[L : K]$.

We have the following.

Theorem 5.8 (Tower Law). *Given field extensions $K \subseteq L \subseteq M$ we have*

$$[M : K] = [M : L][L : K]$$

Proof. If $\{m_i\}_{i\in I}$ is a basis for M over L and $\{\ell_j\}_{j\in J}$ is a basis for L over K, it can be shown that $\{m_i\ell_j\}_{i\in I, j\in J}$ is a basis for M over K. □

One way to construct field extensions is to adjoin on some elements of a larger field. Given $\alpha_1, \ldots, \alpha_n \in L$, we let

$$K(\alpha_1, \ldots, \alpha_n)$$

denote be the smallest subfield of L containing K and $\alpha_1, \ldots, \alpha_n$. It is not difficult to check that the elements of $K(\alpha_1, \ldots, \alpha_n)$ are precisely those of the form

$$\frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)}$$

with $p, q \in K[X_1, \ldots, X_n]$. Similarly, given ring R and S with $R \subseteq S$ and $\alpha_1, \ldots, \alpha_n \in S$, we let

$$R[\alpha_1, \ldots, \alpha_n]$$

denote the smallest ring containing $\alpha_1, \ldots, \alpha_n$ and observe this ring precisely contains the elements

$$p(\alpha_1, \ldots, \alpha_n)$$

with $p \in R[X_1, \ldots, X_n]$. So, we can see that

$$K(\alpha_1, \ldots, \alpha_n) = \mathrm{Frac}(K[\alpha_1, \ldots, \alpha_n]).$$

5.1.2. Number Fields. A *number field* is any finite extension of $\mathbb{Q}$. The following theorem, along with the tower law (Theorem 5.8) tells us that number fields are precisely those fields formed by adjoining finitely many algebraic numbers. We first need to generalize our definition of an algebraic number slightly.

Definition 5.9. Given fields $K \subseteq L$, we say $\alpha \in L$ is *algebraic* over K if α is the root of a monic polynomial over K.

We have the following.

Theorem 5.10. *If $K \subseteq L$ are fields, then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K]$ is finite. In this case, $\deg \alpha = [K(\alpha) : K]$ and $K(\alpha) = K[\alpha]$.*

Proof. Suppose first that $\alpha \in L$ is algebraic over K of degree n. We claim that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a K-basis for $K(\alpha)$. For linear independence, note that if

$$\sum_{i=0}^{n-1} a_i \alpha^i = 0$$

then α is a root of $p(X) = \sum a_i X^i$ with $\deg p = n - 1 < \deg m_\alpha$. So it must be the case that p is identically zero. Let V denote the K-span of $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Observe that if

$$m_\alpha(X) = c_0 + c_1 X + \cdots + c_n X^n$$

for $c_i \in K$ then,

$$\alpha^n = -(c_0\alpha + \cdots + c_{n-1}\alpha^{n-1}),$$

and so inductively any power of α is in V, and so for $p \in K[X]$ and $p(\alpha) \in K(\alpha)$ we have $p(\alpha) \in V$. This gives $V = K[\alpha]$. Next, observe that since m_α is irreducible, then it must be that m_α and p are relatively prime in $K[X]$. So, there existsw $f, g \in K[X]$ so that

$$f(X)m_\alpha(X) + g(X)p(X) = 1.$$

Evaluating at α gives $g(\alpha)p(\alpha) = 1$ and so $1/p(\alpha) \in K[\alpha]$. Hence, $K[\alpha] = K(\alpha)$ as desired.

Conversely, suppose that $[K(\alpha) : K] = n$ is finite. Then, $1, \alpha, \ldots, \alpha^n$ are linearly dependent, so $\exists c_i \in K$ not all zero so that

$$\sum_{i=1}^{n} c_i \alpha^i = 0$$

making α algebraic over K. □

We denote the set of all algebraic numbers as $\bar{\mathbb{Q}}$ and the set of algebraic integers as $\bar{\mathbb{Z}}$. We have the following.

Theorem 5.11. *The set of algebraic numbers $\bar{\mathbb{Q}}$ forms a field.*

Proof. Observe that for any $\alpha, \beta \in \bar{\mathbb{Q}}$ with $\beta \neq 0$, we have that $\alpha \pm \beta$, $\alpha\beta$ and α/β are in $\mathbb{Q}(\alpha, \beta)$. So by Theorem 5.10 it suffices to show that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is finite. This follows directly from the tower law, since

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

and since β is algebraic over $\mathbb{Q}$ it must be algebraic over $\mathbb{Q}(\alpha)$. □

5.1.3. Rings of Integers. The *ring of integers* of a number field K is defined to be the set of all algebraic integers in K; that is

$$\mathcal{O}_K := K \cap \bar{\mathbb{Z}}.$$

It will turn out that $\mathcal{O}_K$ is analogous in some ways to $\mathbb{Z}$. Our main goal of this chapter will be to develop this analogy. First, we need to convince ourselves that $\mathcal{O}_K$ is in fact a ring. It will suffice to show the following.

Theorem 5.12. *The set of algebraic integers $\bar{\mathbb{Z}}$ forms a ring.*

It will be useful throughout this chapter to be able to talk about rings of integers as $\mathbb{Z}$-modules. Let's first develop this area a bit.

Modules, intuitively, are just vector spaces over rings. Formally, we have the following.

Definition 5.13. Given a commutative ring R, an R-module M is an abelian group with scalar multiplication rm for $r \in R$ and $m \in M$ satisfying the following properties

(1) $(r + s)m = rm + sm$,
(2) $r(m + n) = rm + rn$,
(3) $r(sm) = (rs)m$,
(4) $1m = m$

for all $r, s \in R$ and $m, n \in M$. Observe that when R Is a field, M is an R-vector space.

A module M is called *free* if it contains a basis B in the usual sense. That is, the elements of M are precisely those of the form

$$\sum r_i b_i$$

for $r_i \in R$ and $b_i \in B$ (i.e. the R-span of B equals M) and that

$$\sum c_i b_i = 0$$

if and only if $c_i = 0$ for all i (that is, B is R-linearly independent). The *rank* of M is the size of the basis B.

We have the following observation.

Lemma 5.14. *If R is an integral domain and M is a finitely generated free R-module of rank r, then M is torsion-free. That is, for every nonzero $m \in M$ and $r \in R$ we have $mr \neq 0$.*

Proof. Suppose that M has basis $\{b_1, \dots, b_n\}$. Then for any $m \in M$ we can write

$$m = c_1 b_1 + \cdots + c_n b_n$$

for $c_i \in R$. Now, take any nonzero element $r \in R$. Then we have

$$rm = (rc_1)b_1 + \cdots + (rc_n)b_n.$$

Since $m \neq 0$ and $\{b_i\}$ is R-linearly independent, then $c_i \neq 0$ for some $i \in \{1, \dots, n\}$. Since R is a domain, then $rc_i \neq 0$ which gives $rm \neq 0$ again by linear independence of $\{b_i\}$. □

The following structure theorem is typically covered in an abstract algebra course, so we omit the proof here.

Theorem 5.15 (Structure Theorem for Finitely Generated Modules over PIDs)**.** *Let R be a PID and M a finitely generated R-module. Then,*

$$M \cong R^r \oplus R/(\delta_1) \oplus \cdots \oplus R/(\delta_m)$$

where $\delta_i \in M$ satisfy $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_m$. In particular, if M is free then we have

$$M \cong R^r.$$

In this course, our modules will almost always be defined over $\mathbb{Z}$. Note that in this case, the structure theorem above is just the fundamental theorem on finitely generated abelian groups.

We need one more result on modules, which we state without proof.

Lemma 5.16. *Let $N \subseteq M$ be modules over a PID. If M is a finitely generated free R module of rank m, then N is also a finitely generated free R module of rank $n \leq m$.*

The following $\mathbb{Z}$-module will help us prove that $\bar{\mathbb{Z}}$ is in fact a ring.

Lemma 5.17. *A complex number α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module. Furthermore, if $\deg \alpha = n$ then $\mathbb{Z}[\alpha]$ has $\mathbb{Z}$-basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.*

We omit this proof, and note that it follows identically to the proof of Theorem 5.10. We are now prepared to prove Theorem 5.12.

Proof of 5.12. Take any $\alpha, \beta \in \bar{\mathbb{Z}}$ and suppose that $\deg \alpha = n$ and $\deg \beta = m$. We need to show that $\alpha \pm \beta$ and $\alpha\beta$ are in $\bar{\mathbb{Z}}$. By Lemma 5.17 we know that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules with bases $\{1, \alpha, \dots, \alpha^{n-1}\}$ and $\{1, \beta, \dots, \beta^{m-1}\}$ respectively. It is not difficult to see that $\mathbb{Z}[\alpha, \beta]$ has basis contained in

$$\{\alpha^i \beta^j\}$$

where we take $i \in \{0, \dots, n-1\}$ and $j \in \{0, \dots, m-1\}$. So $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module and so by Lemma 5.16 $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha \pm \beta]$ are finitely generated $\mathbb{Z}$-modules as well. So, the result follows by Lemma 5.17. □

5.1.4. Conjugates.

Let α be an algebraic number. By the fundamental theorem of algebra, we can write

$$m_\alpha(X) = (X - \alpha^{(1)})(X - \alpha^{(2)}) \cdots (X - \alpha^{(n)})$$

for some $\alpha^{(i)} \in \mathbb{C}$. We call the elements $\alpha^{(i)}$ the *conjugates* of α. These elements will help us define some key functions and invariants of a number field K which will be useful in studying its ring of integers. First we note the following.

Lemma 5.18. *The conjugates of any algebraic integer are distinct.*

Proof. This follows because m_α is irreducible over $\mathbb{Q}$ and so must have distinct roots over $\mathbb{C}$, but let's prove this from scratch. Suppose for a contradiction that $\alpha^{(i)} = \alpha^{(j)}$ for some $i \neq j$. Then we can write

$$m_\alpha(X) = (X - \alpha^{(i)})^2 g(X)$$

for some $g(X) \in \mathbb{C}[X]$. Taking the formal derivative gives

$$m'_\alpha(X) = 2(X - \alpha^{(i)})g(X) + (X - \alpha^{(i)})^2 g'(X).$$

So, we have $m'_\alpha(\alpha^{(i)}) = 0$. That is, $\alpha^{(i)}$ is a root of both m_α and m'_α. But since m_α is irreducible, it must be that $\gcd(m_\alpha, m) = 1$ and so by the Euclidean Algorithm in $\mathbb{Q}[X]$ there exist $q, t \in \mathbb{Q}[X]$ so that

$$q(X)m_\alpha(X) + t(X)m'_\alpha(X) = 1.$$

But if evaluate both sides of this equation at $\alpha^{(i)}$ we get $0 = 1$, a contradiction. □

Remark 5.19. Note that it is not always the case that the conjugates of α are in $K = \mathbb{Q}(\alpha)$. For example, the conjugates of $\alpha = \sqrt[3]{2}$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$ where $\zeta = e^{2\pi i/3}$ is a primitive 3rd root of unity. Since K is real in the case, we see that the conjugates of α, which are complex, certainly are not in K. Number fields that contain the conjugates of every element are called *Galois* over $\mathbb{Q}$.

The following results will tell us that for a number field $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$, the conjugates exactly define the monomorphisms $\sigma : K \hookrightarrow \mathbb{C}$ that fix $\mathbb{Q}$ (that is, the injective field homomorphisms with $\sigma(q) = q$ for all $q \in \mathbb{Q}$).

Theorem 5.20. *Let α be an algebraic number with conjugates $\alpha^{(1)}, \dots, \alpha^{(n)}$ and let $K = \mathbb{Q}(\alpha)$. Then, there are exactly n distinct monomorphisms $\sigma_i : K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$ and are given by $\sigma_i(\alpha) = \alpha^{(i)}$. That is, for $p(\alpha) \in \mathbb{Q}(\alpha)$ where $p(X) \in \mathbb{Q}[X]$ we define $\sigma_i(p(\alpha)) = p(\alpha^{(i)})$.*

Proof. It can be checked directly that the maps $\sigma_i(\alpha) = \alpha^{(i)}$ are injective field homomorphisms, which are distinct by Lemma 5.18. Furthermore, they fix $\mathbb{Q}$ by construction. Conversely, suppose that $\sigma : K \hookrightarrow \mathbb{C}$ is a monomorphism fixing $\mathbb{Q}$. Then,

$$m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0,$$

and so $\sigma(\alpha)$ is a conjugate of α. □

In fact, automatically this will define all monomorphisms on any given number field, due to the following theorem.

Theorem 5.21 (Primitive Element Theorem)**.** *If K is a finite extension of $\mathbb{Q}$, then there exists an element θ so that $K = \mathbb{Q}(\theta)$.*

However, we can usually get by without having to find a primitive element of K, so we omit the proof of this theorem and refer the reader to Theorem 2.2 of [**ST16**] for the details. Instead, we will use the following result to find the monomorphisms on number fields of the form $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Theorem 5.22. *Let $K \subseteq L$ be number fields. Then every embedding $K \hookrightarrow \mathbb{C}$ that fixes $\mathbb{Q}$ extends to exactly $[L : K]$ embeddings $L \hookrightarrow \mathbb{C}$ that fix $\mathbb{Q}$.*

Proof. We induct on $[L : K]$. The case $[L : K] = 1$ is clear, so suppose that $[L : K] > 1$. Then, there exists an element $\alpha \in L$ with $\alpha \notin K$. By the tower law and Theorem 5.10, since L is algebraic over $\mathbb{Q}$ it is also algebraic over K, and so there is an irreducible polynomial $f \in K[X]$ with $f(\alpha) = 0$. Write

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_0,$$

where $a_i \in K$ and $d \geq 2$. Take any embedding $\sigma : K \hookrightarrow \mathbb{C}$ and let $g := \sigma \cdot f$, where

$$(\sigma \cdot f)(X) := X^d + \sigma(a_1) X^{d-1} + \cdots + \sigma(a_0).$$

It can be shown that since f is irreducible, so is g, and so g has distinct roots $\beta^{(1)}, \ldots, \beta^{(d)}$ in $\mathbb{C}$. Define the maps $\tilde{\sigma}_i : K(\alpha) \hookrightarrow \mathbb{C}$ by sending

$$\tilde{\sigma}_i(\alpha) = \beta^{(i)} \text{ and } \tilde{\sigma}_i(k) = \sigma(k)$$

for all $k \in K$. It can be verified that $\tilde{\sigma}_i$ is a monomorphism, and by construction $\tilde{\sigma}_i$ extends K. By the inductive hypothesis, each of the $d = [K(\alpha) : K]$ embeddings $\tilde{\sigma}_i$ extends to exactly $[L : K(\alpha)]$ embeddings, and so by the tower law there are $[L : K(\alpha)][K(\alpha) : K] = [L : K]$ embeddings extending σ as desired. □

Example 5.23. Let's find all monomorphisms of $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ into $\mathbb{C}$ that fix $\mathbb{Q}$. Since $\sqrt{2}$ has conjugates $\pm\sqrt{2}$ the embeddings

$$\sigma_i : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$$

are given by $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Observe that the proof of Theorem 5.22 tells us precisely how to extend these embeddings. Since $\sqrt{3}$ has minimal polynomial $f(X) = X^2 - 3$ over $\mathbb{Q}(\sqrt{2})$ we get that $\sigma_i \cdot f = f$ and so the embeddings $\tilde{\sigma}_{ij}$ extending σ_i are given by

$$\tilde{\sigma}_{i1}(\sqrt{3}) = \sqrt{3} \text{ and } \tilde{\sigma}_{i1}(\sqrt{2}) = \sigma_i(\sqrt{2})$$

and

$$\tilde{\sigma}_{i2}(\sqrt{3}) = -\sqrt{3} \text{ and } \tilde{\sigma}_{i2}(\sqrt{2}) = \sigma_i(\sqrt{2}).$$

So the embeddings of K into $\mathbb{C}$, of which there should be exactly $4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ are defined by

$$\begin{gathered}
\tilde{\sigma}_{11} : \sqrt{2} \mapsto \sqrt{2} \text{ and } \sqrt{3} \mapsto \sqrt{3} \\
\tilde{\sigma}_{12} : \sqrt{2} \mapsto \sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3} \\
\tilde{\sigma}_{21} : \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto \sqrt{3} \\
\tilde{\sigma}_{22} : \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}
\end{gathered}$$

5.1.5. The Norm and Trace.

The norm and trace will be functions mapping from a number field K to the rational numbers, so that the restriction to the ring of integers $\mathcal{O}_K$ maps to the integers. These functions will often let us translate questions about arithmetic in $\mathcal{O}_K$ to arithmetic in $\mathbb{Z}$.

Definition 5.24. Let K be an algebraic number field, and $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings $K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$. Then, the *norm* of α in K is given by

$$N_K(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha)$$

and the *trace* of α in K is given by

$$\mathrm{Tr}_K(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha).$$

Lemma 5.25. *For any $\alpha \in K$ we have $N_K(\alpha), \mathrm{Tr}_K(\alpha) \in \mathbb{Q}$. Furthermore, if $\alpha \in \mathcal{O}_K$ then we have $N_K(\alpha), \mathrm{Tr}_K(\alpha) \in \mathbb{Z}$.*

Proof. Suppose that α has conjugates $\alpha^{(1)}, \ldots, \alpha^{(m)}$ labeled so that

$$\sigma_i(\alpha) = \sigma^{(i)}.$$

Recall from Theorem 5.22 we can relabel our σ_j so that

$$\sigma_i(\alpha) = \sigma_{m+i}(\alpha) = \cdots = \sigma_{(d-1)m+i}$$

where $d = n/m$ and for all $i = 1, \ldots, m$. Next, since

$$m_\alpha(X) = (X - \alpha^{(1)})(X - \alpha^{(2)}) \cdots (X - \alpha^{(n)})$$

we can write

$$m_\alpha(X) = X^m - \left(\sum_{i=1}^{m} \alpha^{(i)}\right) X^{m-1} + \cdots \pm \left(\prod_{i=1}^{m} \alpha^{(i)}\right).$$

Since $m_\alpha(X) \in \mathbb{Q}[X]$ we have $N_{\mathbb{Q}(\alpha)}(\alpha), \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Q}$. Furthermore, if $\alpha \in \bar{\mathbb{Z}}$ then $m_\alpha(X) \in \mathbb{Z}[X]$ and so $N_{\mathbb{Q}(\alpha)}(\alpha), \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha)$. The result follows by Exercise 6. □

In the exercises, you will also show that the norm gives a characterization of units in $\mathcal{O}_K$ and how it gives a sufficient condition for an element in $\mathcal{O}_K$ to be prime.

5.1.6. Discriminants.

For a number field K of degree n over $\mathbb{Q}$ and subset $A = \{\alpha_1, \ldots, \alpha_n\}$ of K, the *discriminant* of the set A is the value

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Observe that $\Delta(\alpha_1, \ldots, \alpha_n) = 0$ precisely when the α_i form a $\mathbb{Q}$-basis for K. Furthermore, if $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two $\mathbb{Q}$-bases for K with

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i$$

then we have

$$\Delta(\beta_1, \ldots, \beta_n) = (\det(c_{ik}))^2 \Delta(\alpha_1, \ldots, \alpha_n). \tag{5.1}$$

Theorem 5.26. *For any subset $\{\alpha_1, \dots, \alpha_n\}$ of a number field K, we have*

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(\operatorname{Tr}_K(\alpha_i\alpha_j))^2.$$

Proof. We have

$$\begin{aligned}\Delta(\alpha_1, \dots, \alpha_n) &= \det(\sigma_i(\alpha_j))^2\\ &= \det(\sigma_i(\alpha_j))\det(\sigma_i(\alpha_j))\\ &= \det(\sigma_j(\alpha_i))\det(\sigma_i(\alpha_j))\\ &= \det((\sigma_j(\alpha_i))(\sigma_i(\alpha_j))\\ &= \det(\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j))\\ &= \det(\operatorname{Tr}_K(\alpha_i\alpha_j)),\end{aligned}$$

as desired. □

This, along with Lemma 5.25 gives the following Corollary.

Corollary 5.27. For a subset $\{\alpha_1, \dots, \alpha_n\}$ of a number field K, $\Delta(\alpha_1, \dots, \alpha_n)$ is in $\mathbb{Q}$. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ then $\Delta(\alpha_1, \dots, \alpha_n)$ is in $\mathbb{Z}$. Furthermore, if all of the conjugates of the α_i are real, then $\Delta(\alpha_1, \dots, \alpha_n) \geq 0$.

5.1.7. Orders and Integral Bases. The following will allow us to define the discriminant as an invariant of K, and furthermore will help us understand $\mathcal{O}_K$ as a $\mathbb{Z}$-module. We first need the following observation.

Lemma 5.28. *If $\alpha \in K$ then there exists a nonzero integer c so that $c\alpha \in \mathcal{O}_K$.*

Proof. Write $m_\alpha(X) = X^n + a_1X^{n-1} + \cdots a_0$. Since $a_i \in \mathbb{Q}$ there is a nonzero integer $c \in \mathbb{Z}$ so that $ca_i \in \mathbb{Z}$ for all i. Observe that $c\alpha$ is a root of

$$f(X) = X^n + ca_1X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

so we have $c\alpha \in \mathcal{O}_K$. □

Theorem 5.29. *For a number field K, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.*

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for K. By Lemma 5.17 we know that there exist $c_i \in \mathbb{Z}$ with $c_i\alpha_i \in \mathcal{O}_K$. Letting $c = c_1 \cdots c_n$ we have $c\alpha_i \in \mathcal{O}_K$ for all i. It is not difficult to also check that $\{c\alpha_1, \dots, c\alpha_n\}$ is a basis for K, so by replacing α_i with $c\alpha_i$ we may assume that $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathcal{O}_K$. Next, let

$$d := \Delta(\alpha_1, \dots, \alpha_n).$$

Recall that $d \neq 0$, and let M denote the free $\mathbb{Z}$-module with basis $\{\alpha_1/d, \dots, \alpha_n/d\}$. We first claim that $\mathcal{O}_K \subseteq M$. To see this, take any $\alpha \in \mathcal{O}_K$ and write

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$$

with $x_i \in \mathbb{Q}$. If we let $\sigma_1, \dots, \sigma_n$ denote the distinct embeddings $K \hookrightarrow \mathbb{C}$ then we obtain a system of equations that can be organized as follows

$$\begin{pmatrix}\sigma_1(\alpha)\\ \vdots\\ \sigma_n(\alpha)\end{pmatrix} = \begin{pmatrix}\sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n)\\ \vdots & \ddots & \vdots\\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n)\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$$

By Cramer's rule, we have that

$$x_i = \det(A_i)/\det(\sigma_i(\alpha_j)),$$

where A_i is a matrix consisting of $\sigma_i(\alpha_j)$'s and $\sigma_i(\alpha)$'s. Since $\mathcal{O}_K$ is a ring and the conjugate of any algebraic integer is also an algebraic integer, we get $\det(A) \in \mathcal{O}_K$. Furthermore, we have

$$dx_i = \sqrt{d} \cdot \det(A)$$

So $dx_i \in \bar{\mathbb{Z}} \cap \mathbb{Q}$ which gives $dx_i \in \mathbb{Z}$ as desired. Hence, $\mathcal{O}_K$ is contained in a free $\mathbb{Z}$-module of rank n and so by Lemma 5.16 $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $\leq n$. Finally, we show that $\mathcal{O}_K$ has rank at least n. By the primitive element theorem, we can write $K = \mathbb{Q}(\theta)$ for some $\theta \in K$. By Lemma 5.28 we may assume that $\theta \in \mathcal{O}_K$. Recall that Lemma 5.17 tells us $\mathbb{Z}[\theta]$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and by definition $\mathbb{Z}[\theta] \subseteq \mathcal{O}_K$. □

Definition 5.30. An order $\mathcal{O}$ in a number field K is any free $\mathbb{Z}$-module with rank $n = [K : \mathbb{Q}]$ that is also a ring with unity.

For example, $\mathcal{O} = \mathbb{Z}[\sqrt{5}]$ is an order in $K = \mathbb{Q}(\sqrt{5})$. However, $\mathcal{O} \neq \mathcal{O}_K$ because for example $\alpha = \frac{1+\sqrt{5}}{2}$ has minimal polynomial $X^2 - X - 1$ and so $\alpha \in \mathcal{O}_K$ but not in $\mathcal{O}$.

Theorem 5.31. *The ring of integers of any number field is the maximal order. That is, if $\mathcal{O}$ is an order in K, then we have $\mathcal{O} \subseteq \mathcal{O}_K$.*

Proof. Take any $\alpha \in \mathcal{O}$. Then $\mathbb{Z}[\alpha] \subseteq \mathcal{O}$. Since $\mathcal{O}$ is a finitely generated free $\mathbb{Z}$-module, then by Lemma 5.16 so is $\mathbb{Z}[\alpha]$. So, if α has degree d then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\alpha]$ and so we must have $\alpha^d = \sum_{i=0}^{d-1} c_i \alpha^i$ for some $c_i \in \mathbb{Z}$ and so $\alpha \in \mathcal{O}_K$. □

This Theorem gives rise to the following definition.

Definition 5.32. The *index* of an order $\mathcal{O}$ in $\mathcal{O}_K$ is the size of the quotient group

$$(\mathcal{O}_K : \mathcal{O}) := |\mathcal{O}_K/\mathcal{O}|.$$

Note that, since $\mathcal{O}$ is an order, $(\mathcal{O}_K : \mathcal{O})$ is finite.

Next, we see how the discriminant can be used to measure the "size" of an order.

Theorem 5.33. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Z}$-basis for an order $\mathcal{O}$ in a number field K. Then $\{\beta_1, \ldots, \beta_n\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ if and only if the change of basis matrix C is in $\mathrm{GL}_n(\mathbb{Z})$; that is, there exists a matrix D so that $CD = I$. Furthermore, we have*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\beta_1, \ldots, \beta_n).$$

Proof. Write

$$\beta_i = \sum_{k=1}^{n} c_{ik}\alpha_k \text{ and } \alpha_i = \sum_{k=1}^{n} d_{ik}\beta_k$$

for $c_{ik}, d_{ik} \in \mathbb{Z}$. This gives

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \text{ and } \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = D \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

where $C = (c_{ik})$ and $D = (d_{ik})$ are in $\mathbf{Mat}_n(\mathbb{Z})$. So

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = CD \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix},$$

but since $\{\beta_1, \dots, \beta_n\}$ are $\mathbb{Q}$-linearly independent, we must have $CD = I$. Taking determinants gives $\det(C)\det(D) = 1$. But since $\det(C), \det(D) \in \mathbb{Z}$ we have $\det(C) = \pm 1$ and so by Equation (5.1) we get $\Delta(\alpha_1, \dots, \alpha_n) = \Delta(\beta_1, \dots, \beta_n)$. □

This gives rise to the following definition.

Definition 5.34. The *discrimimant* $\Delta_{\mathcal{O}}$ of an order $\mathcal{O}$ is the discriminant of any $\mathbb{Z}$-basis of $\mathcal{O}$. We call the discrimimant of the ring of integers $\mathcal{O}_K$ the discrimimant of K, and typically use the notation Δ_K to mean $\Delta_{\mathcal{O}_K}$.

Note that, since $\mathcal{O}_K$ has rank $[K : \mathbb{Q}]$, any $\mathbb{Z}$-basis for $\mathcal{O}_K$ is also a $\mathbb{Q}$-basis for K.

Definition 5.35. A $\mathbb{Q}$-basis $\{\alpha_1, \dots, \alpha_n\}$ is called an *integral basis* for a number field K if it is also a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

5.2. Finding Rings of Integers

We will see later in this chapter that the ring of integers $\mathcal{O}_K$ of a number field has several nice arithmetic properties. In this section, we show how the following result gives one strategy to find $\mathcal{O}_K$.

Theorem 5.36. *Let $\mathcal{O}$ be an order in K. Then,*

$$\Delta_{\mathcal{O}} = \Delta_K(\mathcal{O}_K : \mathcal{O})^2.$$

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and $\{\beta_1, \dots, \beta_n\}$ a $\mathbb{Z}$-basis for $\mathcal{O}$. By Theorem 5.31 we know that $\{\beta_1, \dots, \beta_n\} \subseteq \mathcal{O}_K$ and so we can write

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

for some $C \in \mathbf{Mat}_n(\mathbb{Z})$. Next, we write C in Smith Normal Form. That is, using row and column operations, we can construct matrices $X, Y \in \mathrm{GL}_n(\mathbb{Z})$ so that $XCY = \mathrm{diag}(d_1, \dots, d_n)$ where $d_i \in \mathbb{Z}$. So, we have

$$X \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \mathrm{diag}(d_1, \dots, d_n) Y^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Let

$$\begin{pmatrix} \beta_1' \\ \vdots \\ \beta_n' \end{pmatrix} = X \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \text{ and } \begin{pmatrix} \alpha_1' \\ \vdots \\ \alpha_n' \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Since $X, Y^{-1} \in \mathrm{GL}_n(\mathbb{Z})$ then by Theorem 5.33 we know that $\{\beta_1', \dots, \beta_n'\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ and $\{\alpha_1', \dots, \alpha_n'\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and by construction we have $\beta_i' = d_i \alpha_i'$. So,

$$\Delta_{\mathcal{O}} = \det(\sigma_i(\beta_j'))^2 = \det(d_i \sigma_i(\alpha_j'))^2 = \Delta_{\mathcal{O}_K}(d_1 \cdots d_n)^2.$$

By the structure theorem for modules over PIDs, we have the isomorphism

$$\varphi : \mathcal{O}_K \xrightarrow{\cong} \mathbb{Z}^{\oplus n}, a_1\alpha_1 + \cdots + a_n\alpha_n \mapsto (a_1, \dots, a_n).$$

So, we see that $\varphi(\mathcal{O}) \cong d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_n\mathbb{Z}$, which gives

$$|\mathcal{O}_K/\mathcal{O}| = |\mathbb{Z}^{\oplus n}/(d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_n\mathbb{Z})| = d_1 \cdots d_n$$

as desired. □

Note that if $\Delta_{\mathcal{O}}$ contains no square factor, we must have $(\mathcal{O}_K : \mathcal{O}) = 1$, immediately giving $\mathcal{O}_K = \mathcal{O}$. So if we can find an order in K with square-free discriminant, we automatically must have found the ring of integers. However, we don't always get so lucky. The following results show how we might still use the theorem above.

Proposition 5.37. Let $\mathcal{O}$ be an order in a number field K with $I = (\mathcal{O}_K : \mathcal{O})$. Then we have

$$\mathcal{O}_K \subseteq \frac{1}{I}\mathcal{O}.$$

Proof. As in the proof of 5.36, there exists a basis $\{\alpha_1, \dots, \alpha_n\}$ for $\mathcal{O}_K$ so that $\{d_1\alpha_1, \dots, d_n\alpha_n\}$ is a basis for $\mathcal{O}$. Now, for any $\alpha \in \mathcal{O}_K$ we have

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$$

for $a_i \in \mathbb{Z}$ and since $I = d_1 \cdots d_n$ we get

$$\alpha = \frac{1}{I}((a_1 d_2 \cdots d_n)d_1\alpha + \cdots + (a_1 d_1 \cdots d_{n-1})d_n\alpha) \in \frac{1}{I}\mathcal{O}.$$

□

Proposition 5.38. Suppose that $\mathcal{O}$ is an order in K with basis $\{\beta_1, \dots, \beta_n\}$. Then, for every prime p dividing the index $(\mathcal{O}_K : \mathcal{O})$, there exists a nonzero element $\alpha \in \mathcal{O}_K$ of the form

$$\alpha = \frac{1}{p}(r_1\alpha_1 + \cdots r_n\alpha_n)$$

where $r_i \in \mathbb{Z}$ with $0 \le r_i < p$.

Proof. Suppose that $\mathcal{O}_K \neq \mathcal{O}$ so that there exists a prime p dividing $(\mathcal{O}_K : \mathcal{O})$. By Proposition 5.37 we have

$$\mathcal{O}_K \subseteq \frac{1}{I}\mathcal{O}.$$

Take $\alpha \in \mathcal{O}_K$ with $\alpha \notin \mathcal{O}$. Then we can write

$$\alpha = \frac{1}{I}(b_1\beta_1 + \cdots + b_n\beta_n)$$

for some $b_i \in \mathbb{Z}$. Write $I = pd$ for a prime p and $d \in \mathbb{Z}$. Then we get

$$d\alpha = \frac{1}{p}(b_1\beta_1 + \cdots + b_n\beta_n)$$

Divide p into each b_i to write

$$b_i = pq_i + r_i$$

where $0 \leq r_i < p$. Since $\alpha \notin \mathcal{O}$ then we have $r_i \neq 0$ for some $i \in \{1, \ldots, n\}$. We get

$$d\alpha = \frac{1}{p}(r_1\beta_1 + \cdots + r_n\beta_n) + \alpha',$$

where $\alpha' = q_1\beta_1 + \cdots + q_n\beta_n \in \mathcal{O} \subseteq \mathcal{O}_K$. So, $d\alpha - \alpha' \in \mathcal{O}_K$ as desired. □

Example 5.39. Let $K = \mathbb{Q}(\sqrt[3]{5})$. We claim that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{5}]$. To see this, let $\theta = \sqrt[3]{5}$ and note that θ has conjugates $\theta, \zeta\theta, \zeta^2\theta$ where $\zeta = e^{2\pi i/3}$ is a primitive 3rd root of unity. Letting $\mathcal{O} = \mathbb{Z}[\theta]$ we have

$$\begin{aligned}\Delta_{\mathcal{O}} &= \det \begin{pmatrix} 1 & \theta & \theta^2 \\ 1 & \zeta\theta & \zeta^2\theta^2 \\ 1 & \zeta^2\theta & \zeta\theta^2 \end{pmatrix}^2 \\ &= \theta^6 \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix}^2 \\ &= 5^2(3\zeta^2 - 3\zeta)^2 \\ &= 5^2 \cdot 3^2(\zeta^2 - \zeta)^2 \\ &= 5^2 \cdot 3^2 \cdot \zeta + \zeta^2 - 2\zeta^3 \\ &= -3^3 \cdot 5^2.\end{aligned}$$

Note that $1 + \zeta + \zeta^2 = \frac{\zeta^3 - 1}{\zeta - 1}$ and since $\zeta^3 = 1$ we get $\zeta + \zeta^2 = -1$. So, by Theorem 5.36 we have

$$-3^3 \cdot 5^2 = \Delta_K(\mathcal{O}_K : \mathcal{O})^2.$$

For a contradiction, suppose that $3 \mid (\mathcal{O}_K : \mathcal{O})$. Then by Proposition 5.38 there exists an element $\alpha \in \mathcal{O}_K$ of the form

$$\alpha = \frac{1}{3}(r_1 + r_2\theta + r_3\theta^2).$$

with $0 \leq r_i < 3$. Asking technology to help you take the norm gives

$$N_K(\alpha) = \frac{1}{27}(r_1^3 - 15r_1r_2r_3 + 5r_2^3 + 25r_3^3)$$

We can check all possibilities for $r_i \in \{0, 1, 2\}$ to see that $N_K(\alpha) \notin \mathbb{Z}$ and so $\alpha \notin \mathcal{O}_K$. If $p = 5$ divides the index $(\mathcal{O}_K : \mathcal{O})$ then again by Proposition **??** there's a nonzero element $\beta \in \mathcal{O}_K$ of the form

$$\beta = \frac{1}{5}(r_1 + r_2\theta + r_3\theta^2)$$

with $0 \leq r_i < 5$. Taking the trace gives $\mathrm{Tr}_K(\beta) = r_1/5$ and so we must have $r_1 = 0$. Similar to above, we can compute

$$N_K(\beta)\frac{1}{125}(5r^2 + 25r_3^3)$$

and check by hand that there is no choice of $r_i \in \{0, \dots, 4\}$ making $N_K(\beta) \in \mathbb{Z}$ unless $\beta = 0$. So we must have $(\mathcal{O}_K : \mathcal{O}) = 1$ giving $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Remark 5.40. Note that number fields K with ring of integers of the form $\mathbb{Z}[\theta]$ for some $\theta \in K$ are called *monogenic.* We'll see in a future section that the cyclotomic fields $\mathbb{Q}(\zeta)$ are monogenic, where ζ is a root of unity. Characterizing monogenic fields and finding explicit information about their generators is a topic of current interest (see for example [**GSS19**] and [**Akh22**]).

5.3. Unique Factorization of Ideals in $\mathcal{O}_K$

The ring of integers $\mathcal{O}_K$ is a number field K is meant to generalize the integers $\mathbb{Z}$ inside of the rational numbers $\mathbb{Q}$. Unfortunately, this analogy does not immediately extend our fundamental theorem. That is, not every ring of integers has the property that *elements* factor uniquely into primes. In this section, we show that if we instead pass to ideas, we can recover such a theorem. First, we review some ring theory background.

5.3.1. Irreducible and Prime Elements.

. Let R be a ring. Recall that an element $u \in R$ is called a *unit* if it has a multiplicative inverse in R.

Definition 5.41. A nonzero nonunit $p \in R$ is said to be *prime* if it satisfies the following property:

$$\text{if } p \mid ab \text{ then } p \mid a \text{ or } p \mid b,$$

for any $a, b \in R$. A nonzero element $a \in R$ is said to be *irreducible* if whenever $a = xy$, either x or y is a unit in R.

It is not always the case that irreducibles are prime.

Example 5.42. Observe that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$. To see this, note that we can wrte

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

If $2 \mid (1 \pm \sqrt{-5})$ then by Exercise 6 we would have

$$N_K(2) \mid N_K(1 \pm \sqrt{-5}) \Rightarrow 4 \mid 6,$$

where $K = \mathbb{Q}(\sqrt{-5})$, a contradiction. So 2 is not prime. Now, if 2 were reducible we could write

$$2 = xy$$

for $x, y \in \mathbb{Z}[\sqrt{-5}]$ nonunits. Again by Exercise 6 this implies that $N(x), N(y) \neq \pm 1$. So we have

$$N_K(2) = N_K(x)N_K(y) \Rightarrow N_K(x) = \pm 2.$$

Note that we can write $x = a + b\sqrt{-5}$ and so the above implies that

$$a^2 + 5b^2 = \pm 2.$$

But there are no integer solutions a, b to the above equation and so $x \notin \mathbb{Z}[\sqrt{-5}]$. So 2 must be irreducible.

If our ring R is an integral domain, the converse does hold.

Lemma 5.43. *If R is an integral domain, then every prime is irreducible.*

Proof. Suppose that p is prime, and write $p = xy$. Without loss of generality, say that $p \mid x$. Then we can write $x = ap$ for some $a \in R$. So we get

$$p = apy \Rightarrow p(1 - ay) = 0$$

and since R is an integral domain and $p \neq 0$ we get $1 - ay = 0$. Hence, $ay = 1$ and so a is a unit. □

In Exercise 10 you'll show that factorization into irreducibles (and hence factorization into primes) is not guaranteed in a ring of integers.

5.3.2. Prime Ideals. Recall that an ideal $\mathfrak{a}$ is a subset of a ring R that's an additive group with the property that for every $r \in R$ we have $r\mathfrak{a} \subseteq \mathfrak{a}$.

Definition 5.44. A proper ideal $\mathfrak{a}$ in a ring R is called *maximal* if for all ideals $\mathfrak{b} \subseteq R$ with $\mathfrak{a} \subseteq \mathfrak{b}$ either $\mathfrak{b} = \mathfrak{a}$ of $\mathfrak{b} = R$.

Definition 5.45. An ideal $\mathfrak{p}$ in a ring R is called *prime* if for all ideals $\mathfrak{b}, \mathfrak{c}$ in R with $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{p}$, we have $\mathfrak{b} \subseteq \mathfrak{p}$ or $\mathfrak{c} \subseteq \mathfrak{p}$.

Note that this definition generalizes the notion of prime element, since for principle ideals (a) and (b) in a ring R we have $(b) \subseteq (a)$ if and only if $a \mid b$. The following alternate definition of prime ideals will often be useful.

Definition 5.46. A proper ideal $\mathfrak{a}$ in a ring R is called *prime* if for all elements $b, c \in R$ with $bc \in \mathfrak{a}$ either $b \in \mathfrak{a}$ or $c \in \mathfrak{a}$.

Lemma 5.47. *Definition 5.45 and 5.46 are equivalent.*

Proof. Suppose that $\mathfrak{p}$ is prime as given in Definition 5.45, and suppose $b, c \in R$ with $bc \in \mathfrak{p}$. Then $(b)(c) \subseteq \mathfrak{p}$ and so either $(b) \subseteq \mathfrak{p}$ or $(c) \subseteq \mathfrak{p}$ and so b or c is an element of $\mathfrak{p}$. Conversely, suppose that $\mathfrak{p}$ is prime as given in Definition 5.46 and let $\mathfrak{a}, \mathfrak{b}$ be ideals in R with $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{p}$. Suppose that $\mathfrak{b} \not\subseteq \mathfrak{p}$. Then, there exists an element $b \in \mathfrak{b}$ with $b \not\in \mathfrak{p}$. Now, for any $c \in \mathfrak{c}$ we have $bc \in \mathfrak{b}\mathfrak{c} \subseteq \mathfrak{p}$ and so we must have $c \in \mathfrak{p}$. This gives $\mathfrak{c} \subseteq \mathfrak{p}$. □

Lemma 5.48. *In a ring R, every maximal ideal is prime.*

Proof. Let $\mathfrak{a}$ be a maximal ideal in R, and take any $b, c \in R$ with $bc \in \mathfrak{a}$. Suppose that $b \not\in \mathfrak{a}$. Then $\mathfrak{a} + (b)$ is an ideal strictly containing $\mathfrak{a}$, and so by maximality we must have $\mathfrak{a} + (b) = R$. So, there exists some $a \in \mathfrak{a}$ and $r \in R$ with $a + rb = 1$. So, $c = ac + rbc \in \mathfrak{a}$. □

5.3.3. Primes Factorization of Ideals in $\mathcal{O}_K$. While the converse of Lemma 5.48 does not hold in general (see Exercise 11, for example) this does hold in $\mathcal{O}_K$.

Lemma 5.49. *Let K be a number field. Then every prime ideal in $\mathcal{O}_K$ is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$. Then for any $\alpha \in \mathfrak{p}$ we have $N_K(\alpha) \in \mathfrak{p}$. So,

$$\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_K/(N_K(\alpha)).$$

Since $(N_K(\alpha)) = N_K(\alpha) \cdot \mathcal{O}_K$ then we have $|\mathcal{O}_K/(N_K(\alpha))|$ is finite. The result will then follow by Exercise 12. □

To prove our generalization of the fundamental theorem of arithmetic for rings of integers, it will be useful to think of the ideals in $\mathcal{O}_K$ as elements of a group. Unfortunately there is not a good notion of inverses for ideals, so we will have to expand the elements we consider.

Definition 5.50. A *fractional ideal in K* is an $\mathcal{O}_K$-module $\mathfrak{a} \subseteq K$ so that the set

$$d\mathfrak{a} = \{da \mid a \in \mathfrak{a}\}$$

is an ideal in $\mathcal{O}_K$ for some nonzero element $d \in \mathcal{O}_K$. We call d a *common denominator* of $\mathfrak{a}$, and denote the set of fractional ideals in $\mathcal{O}_K$ by $\mathrm{Id}(K)$.

For example, the fractional ideals in $\mathbb{Z}$ are precisely $q\mathbb{Z}$ for $q \in \mathbb{Q}$. In fact, if $\mathcal{O}_K$ is any principal ideal domain, the fractional ideals are precisely given by $k\mathcal{O}_K$ for $k \in K$. In general, any fractional ideal $\mathfrak{a}$ with common denominator d can be written in the form $\mathfrak{a} = d^{-1}\mathfrak{b}$ for an ideal $\mathfrak{b}$ in $\mathcal{O}_K$.

Recall, given ideals $\mathfrak{a}, \mathfrak{b}$ in a ring R, their product

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

is also an ideal. We use this to define a group structure on $\mathrm{Id}(K)$.

Theorem 5.51. *For a number field K, $\mathrm{Id}(K)$ forms a group with products defined as follows: for $\mathfrak{a}, \mathfrak{b} \in \mathrm{Id}(K)$, write $\mathfrak{a} = c^{-1}\mathfrak{c}$ and $\mathfrak{b} = d^{-1}\mathfrak{d}$ for $c, d \in K_{\neq 0}$ and $\mathfrak{c}, \mathfrak{d}$ ideals in $\mathcal{O}_K$. Then,*

$$\mathfrak{a}\mathfrak{b} := (cd)^{-1}\mathfrak{c}\mathfrak{d}.$$

Furthermore, inverses are given by

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

Note that $\mathfrak{a}^{-1}$ includes more than just common denominators, since we are allowing elements x to be in K, instead of just in $\mathcal{O}_K$.

Proof. It follows from definition that $\mathrm{Id}(K)$ is closed under products and that $\mathrm{Id}(K)$ has identity $\mathcal{O}_K = (1)$. For any $\mathfrak{a} \in \mathrm{Id}(K)$, it can be checked that $\mathfrak{a}^{-1}$ is an $\mathcal{O}_K$-module, and if we take any nonzero $d \in \mathfrak{a}$ then by definition

$$d\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$$

So d is a common denominator for the $\mathcal{O}_K$ module $\mathfrak{a}^{-1}$, giving $\mathfrak{a}^{-1} \in \mathrm{Id}(K)$. So, what's left to show is that

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$$

for any $\mathfrak{a} \in \mathrm{Id}(K)$. One set inclusion follows from definition: if we take any nonzero $\alpha \in \mathfrak{a}\mathfrak{a}^{-1}$ then $\alpha \in d\mathfrak{a}^{-1}$ for some nonzero $d \in \mathfrak{a}$ and as above $d\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ so that $\alpha \in \mathcal{O}_K$. The other set inclusion is a bit more delicate, so to save some time (and my sanity) I'm going to skip this and instead refer the reader to Section 5.2 of [**ST16**]. □

We are now prepared to prove our generalization of the fundamental theorem of arithmetic for rings of integers.

Theorem 5.52. *Every nonzero ideal in $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.*

Proof. Let S be the set of ideals that are not the product of prime ideals, and for a contradiction suppose that S is not empty. We can choose a maximal ideal $\mathfrak{a}$ in S, since the ring $\mathcal{O}_K$ is *Noetherian* (that is, every nonempty set of ideals has a maximal element; this follows from $\mathcal{O}_K$ being a finitely generated free $\mathbb{Z}$-module, but we'll omit the details here). Since $\mathfrak{a}$ isn't a product of prime ideals, it's not prime itself, and so by Lemma 5.48 $\mathfrak{a}$ is not maximal in $\mathcal{O}_K$. So, there exists a maximal (and hence prime) ideal $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathcal{O}_K$. It can be shown that

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^1 \subseteq \mathcal{O}_K$$

(this step is nontrivial, and again uses $\mathcal{O}_K$ being Noetherian, but it's a bit lengthy to do carefully so let's skip it). Since $\mathfrak{a}$ is maximal in S, we have that $\mathfrak{a}\mathfrak{p}^{-1} \notin S$ and so we can write

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \Rightarrow \mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

for prime ideals $\mathfrak{p}_i$ in $\mathcal{O}_K$, contradicting $\mathfrak{a} \in S$. So, every ideal is a product of prime ideals. For uniqueness, suppose that we have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \tag{5.2}$$

for prime ideals $\mathfrak{p}_i, \mathfrak{q}_j$ Then $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$ and since $\mathfrak{p}_1$ is prime we have $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$ for some i. But since prime ideals are maximal in $\mathcal{O}_K$, which we showed in Lemma 5.49, then we must have $\mathfrak{p}_1 = \mathfrak{q}_i$. Without loss of generality, suppose that $i = 1$. Multiplying both sides of Equation (5.2) by $\mathfrak{p}_1^{-1}$ gives

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Repeating this process r times, where without loss of generality $r \leq s$, we get

$$\mathcal{O}_K = \mathfrak{q}_{r+1} \cdots \mathfrak{q}_s.$$

But since $\mathfrak{q}_s$ is a prime ideal, it must be a proper subset of $\mathcal{O}_K$ and so

$$\mathfrak{q}_{r+1} \cdots \mathfrak{q}_s \subseteq \mathfrak{q}_s \subseteq \mathcal{O}_K$$

which gives $\mathcal{O}_K \neq \mathfrak{q}_{r+1} \cdots \mathfrak{q}_s$, a contradiction unless $r = s$. □

5.4. The Class Group

The following Theorem will motivate our definition of the class group.

Theorem 5.53. *Elements in $\mathcal{O}_K$ factor uniquely into irreducibles if and only if every ideal of $\mathcal{O}_K$ is principal.*

Remark 5.54. Note that unique factorization means that we can write any $a \in \mathcal{O}_K$ as $a = up_1 \cdots p_r$ for a unit u and irreducibles p_i, and furthermore this representation is unique up to permutation and choice of unit. A domain in which elements factor uniquely into irreducibles as above is often called a *unique factorization domain*, or UFD for short.

To prove this result, we need to define one more object.

5.4.1. The Norm of an Ideal.

Given a number field K and an ideal $\mathfrak{a}$ in $\mathcal{O}_K$, the *norm* of the ideal $\mathfrak{a}$ is defined as the size of the quotient group.

$$N_K(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$$

Observe that any ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is a $\mathbb{Z}$-module by definition. Furthermore, for any $a \in \mathfrak{a}$ we have $a\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$ and so $\mathfrak{a}$ is a finitely generated free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. So, we can define the discriminant of $\mathfrak{a}$ to be

$$\Delta(\mathfrak{a}) := \Delta(\alpha_1, \ldots, \alpha_n),$$

where $\{\alpha_1, \ldots, \alpha_n\}$ is any $\mathbb{Z}$-basis for $\mathfrak{a}$. Note here that while $\mathfrak{a}$ is a free $\mathbb{Z}$-module of maximal rank that is closed under products, it is only an order when $\mathfrak{a} = \mathcal{O}_K$ is the trivial ring, since otherwise $\mathfrak{a}$ does not contain 1. We have the following.

Proposition 5.55. Given an ideal $\mathfrak{a}$ in $\mathcal{O}_K$,

$$N_K(\mathfrak{a}) = |\Delta(\mathfrak{a})/\Delta_K|^{1/2}.$$

Proof. As in the proof of Theorem 5.36, since $\mathfrak{a}$ is a finitely generated $\mathbb{Z}$-submodule of $\mathcal{O}_K$ then there exists a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathcal{O}_K$ so that $\{d_1\alpha_1, \ldots, d_n\alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$. So, if σ_i are the distinct embeddings $K \hookrightarrow \mathbb{C}$ then we have

$$\Delta(\mathfrak{a}) = \det(\sigma_i(d_j\alpha_j)) = (d_1 \cdots d_n)^2 \Delta_K.$$

The result follows by taking square roots, since $N_K(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = d_1 \cdots d_n$. □

Proposition 5.56. If $\mathfrak{a} = (a)$ is a principal ideal, then $N_K(\mathfrak{a}) = |N(a)|$.

Proof. Suppose that $\mathcal{O}_K$ has $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. Then, the ideal (a) has $\mathbb{Z}$-basis $\{a\alpha_1, \ldots, a\alpha_n\}$ and so by Proposition 5.55 we have

$$\begin{aligned} N((a)) &= |\Delta(a\alpha_1, \ldots, a\alpha_n)/\Delta(\alpha_1, \ldots, \alpha_n)|^{1/2} \\ &= |\sigma_1(a) \cdots \sigma_n(a)| \\ &= |N_K(a)|, \end{aligned}$$

where σ_i denote the distinct embeddings $K \hookrightarrow \mathbb{C}$. □

We have the following properties.

Theorem 5.57. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals in $\mathcal{O}_K$. Then,*

a $N_K(\mathfrak{a}\mathfrak{b}) = N_K(\mathfrak{a})N_K(\mathfrak{b})$*;*

b $N_K(\mathfrak{a})$ *is an element of* $\mathfrak{a}$*;*

c If $N_K(\mathfrak{a})$ *is prime, then so is* $\mathfrak{a}$*;*

d If $\mathfrak{a}$ *is prime, then there is a distinct rational prime* p *with* $p \in \mathfrak{a}$ *and* $N_K(\mathfrak{a}) = p^m$ *for an integer* m *with* $m \leq [K : \mathbb{Q}]$.

Proof. We refer the reader to Section 5.3 of [**ST16**] for the details of part (a), since it is a bit lengthy. Next, since $N(\mathfrak{a})$ is the size of the quotient group $\mathcal{O}_K/\mathfrak{a}$ then for any $x \in \mathcal{O}_K$ we have $N(\mathfrak{a})x \in \mathfrak{a}$. Setting $x = 1$ gives part (b). For (c), note that if we write $\mathfrak{a}$ in its prime factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$$

for prime ideals $\mathfrak{p}_i$, then we have $N_K(\mathfrak{a}) = N_K(\mathfrak{p}_1) \cdots N_K(\mathfrak{p}_t)$. Since the $\mathfrak{p}_i$ are prime, we have $\mathfrak{p}_i \neq \mathcal{O}_K$ and so $N_K(\mathfrak{p}_i) \neq 1$ for any i. Hence, $N_K(\mathfrak{a})$ is not prime. Finally, suppose that $\mathfrak{a}$ is prime. Write $N_K(\mathfrak{a}) = p_1 \cdots p_t$ for rational primes p_i. By part (b) we have $(N_K(\mathfrak{a})) \subseteq \mathfrak{a}$ and so $(p_1) \cdots (p_t) \subseteq \mathfrak{a}$. Since $\mathfrak{a}$ is prime this means $(p_i) \subseteq \mathfrak{a}$ for some i. So,

$$\begin{aligned} &\mathcal{O}_K/\mathfrak{a} \subseteq \mathcal{O}_K/(p_i) \\ \Rightarrow\ &N_K(\mathfrak{a}) \mid N_K((p_i)) = |N_K(p_i)| = p_i^n, \end{aligned}$$

where $n = [K : \mathbb{Q}]$, noting that the final equality follows because $p_i \in \mathbb{Q}$. Observe furthermore that p_i is distinct. If it were the case that $p, q \in (a)$ for distinct primes p and q then we would have

$$1 = cp + dq \in (a),$$

for some integers c, d since $\gcd(p, q) = 1$. But then $1 \in \mathfrak{a}$ giving $\mathfrak{a} = \mathcal{O}_K$, which contradicts $\mathfrak{a}$ being prime. □

We are now prepared to the main result of this section.

Proof of Theorem 5.53. Suppose that every ideal in $\mathcal{O}_K$ is principal (in fact, this direction will hold for any principal ideal domain; the only extra step would be to show that PIDs are Noetherian). Let S be the set of ideals in $\mathcal{O}_K$ of the form (x) where x does not factor uniquely into irreducibles in $\mathcal{O}_K$. Since x is not irreducible, we can write $x = yz$ for some nonunits $y, z \in \mathcal{O}_K$. So, $(x) \subseteq (y)$ and similarly $(x) \subseteq (z)$. Note that (x) is a proper subset of (y) and (z) by Exercise 15, and so $(y), (z) \notin S$. So we can write y and z as a product of irreducibles, contradicting the fact that $(x) \in S$. So $S = \varnothing$ as desired. To see that factorization is unique, it suffices to show that irreducibles are prime (and proceed as in the proof of the Fundamental Theorem of Arithmetic). Let x be irreducible. Note that if $(x) \subseteq (y)$ then $x \in (y)$ and so $x = yz$. But since x is irreducible, either y or z is a unit; that is either $(x) = (y)$ or $(y) = \mathcal{O}_K$. So, (x) is maximal. Now, suppose that $x \mid ab$. If $x \nmid a$ then (x) is a proper subset of (x, a). Since (x) is maximal, this gives $(x, a) = \mathcal{O}_K$. That is, there exist $q, r \in \mathcal{O}$ so that $xq + ar = 1$. Multiplying by b gives $xqb + abr = b$ and since $x \mid ab$ this gives $x \mid b$.

Conversely, suppose that $\mathcal{O}_K$ has unique factorization of elements into irreducibles. First, we show that in this case, irreducibles are prime. To see this, let $p \in \mathcal{O}_K$ be irreducible, and suppose that $p \mid ab$. Write $pc = ab$ for $c \in \mathcal{O}_K$ and factor a, b, c uniquely into irreducibles as follows

$$\begin{aligned} a &= up_1 \cdots p_n \\ b &= vq_1 \cdots q_m \\ c &= wr_1 \cdots r_s. \end{aligned}$$

for units u, v, w Then we have

$$p(wr_1 \cdots r_s) = (up_1 \cdots p_n)(vq_1 \cdots q_m).$$

By unique factorization, we know that p must be associate to one of the p_i or q_j's. Without loss of generality, suppose that $p = tp_1$ for a unit $t \in \mathcal{O}_K^\times$. Then $p \mid a$ as desired. Next, since we know that ideals factor uniquely into prime ideals, it will suffice to show that every prime ideal is principal. So, take a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$.

By Theorem 5.57 (2), we know that $N := N_K(\mathfrak{p})$ is an element of $\mathfrak{p}$. Write N in its unique factorization as

$$N = \pi_1 \cdots \pi_s$$

for irreducibles π_i. Then, $\pi_1 \cdots \pi_s \in \mathfrak{p}$, and since $\mathfrak{p}$ is prime this gives $\pi_i \in \mathfrak{p}$ for some i, and so $(\pi_i) \subseteq \mathfrak{p}$. By above, we know that π_i is prime, and so by Exercise 16 we get that (π_i) is a prime ideal. Since prime ideals are maximal in $\mathcal{O}_K$ we have $(\pi_i) = \mathfrak{p}$ as desired. □

Remark 5.58. Note that we've showed a bit more. We have the following.

(1) If $\mathcal{O}_K$ is a UFD, then irreducible elements are prime.

(2) When $\mathcal{O}_K$ is a UFD, prime factorization of elements corresponds to prime factorization of the corresponding principal ideals.

(3) If $\mathcal{O}_K$ is not a UFD, and $\pi \in \mathcal{O}_K$ is irreducible but not prime, then the prime factorization of the ideal (π) contains a nonprincipal ideal.

The class group will then help us understand how "badly" a ring of integers fails unique factorization. We have the following.

Definition 5.59. Let $\mathcal{P}(K)$ denote the group of all principal fractional ideals; that is, fractional ideals of the form $k\mathcal{O}_K$ for some $k \in K$. Then, the *class group* of K is the quotient group

$$\mathcal{H}(K) := \mathrm{Id}(K)/\mathcal{P}(K).$$

The size of $\mathcal{H}(K)$ is called the *class number* of K, and is often denoted h_K.

The following result follows directly as a corollary to Theorem 5.53.

Theorem 5.60. *Elements in $\mathcal{O}_K$ factor uniquely into irreducibles if and only if $h_K = 1$.*

We will see in the next chapter that even when $h_K \neq 1$, if the class group isn't "too large" we can use unique factorization into ideals to recover our strategy for solving Diophantine equations. First, we show that h_K is in fact always finite. To do so, it will be useful to give a geometric interpretation of $\mathcal{O}_K$. These methods will also give us a strategy to compute some class numbers.

5.5. Some Geometry of Numbers

In this section, we show how to view the ring of integers as a lattice in $\mathbb{R}^n$. The perspective of viewing certain number theoretic objects as figures in $\mathbb{R}^n$ is used to study a wide range of problems. In this section, we'll take a brief detour to give one such example outside of algebraic number theory. Readers interested in learning more about this technique can consult Cassels' text ([**Cas97**]) and Pete Clark's lecture notes ([**?**])

5.5.1. Lattices.

Definition 5.61. Let $B = \{b_1, \dots, b_n\}$ be a linearly independent subset of $\mathbb{R}^n$. The *lattice* Λ generated by the set B is the free $\mathbb{Z}$-module generated by $\{e_1, \dots, e_n\}$. The *fundamental domain* of Λ is the set $T \subseteq \mathbb{R}^n$ given by

$$T = \{\sum a_i b_i \mid 0 \leq a_i < 1\}.$$

We call this domain "fundamental" because every element x in $\mathbb{R}^n$ can be written in the form $x = a + \ell$ where $a \in T$ and $\ell \in \Lambda$. In this way, the fundamental domain tiles $\mathbb{R}^n$ by boxes whose corners are in the lattice Λ. Note that the fundamental domain of a lattice depends on choice of basis B. To define an invariant of our lattice, we look at its size.=

Definition 5.62. Let $\{b_1, \dots, b_n\}$ be a basis for a lattice Λ. Then, the *determinant* of Λ (sometimes called the *covolume*) is the value

$$d(\Lambda) = |\det(b_1, \dots, b_n)|.$$

Observe that $d(\Lambda)$ gives the volume of any fundamental domain of Λ.

Note that $d(\Lambda)$ does not depend on choice of basis, since the change of basis matrix between any two bases of a free $\mathbb{Z}$-module of rank n is in $\mathrm{GL}_m(\mathbb{Z})$, and hence has determinant ± 1 (as discussed in Theorem 5.33). Furthermore, since the determinant of a collection of vectors gives the volume of their corresponding parallelepiped, the determinant of a lattice measures the volume of any fundamental domain.

5.5.2. Minkowski's Convex Body Theorem.

We recall the following definitions.

Definition 5.63. Let X be a subset of $\mathbb{R}^n$. Then X is *convex* if for every $x, y \in X$ we have

$$\lambda x + (1 - \lambda)y$$

is also in X, for every $0 \leq \lambda \leq 1$. We call X *centrally symmetric* if for all $x \in X$ we have $-x \in X$.

The following Theorem is one of the key tools in geometry of numbers. To save some time we skip the proof, and instead refer the reader to Chapter 7 of [**ST16**].

Theorem 5.64 (Minkowski's Convex Body Theorem)**.** *Let Λ be a lattice in $\mathbb{R}^n$. If X is a convex centrally symmetric subset of $\mathbb{R}^n$ and*

$$vol(X) > 2^n \det(\Lambda),$$

then X contains a non-zero lattice point of Λ.

In the next section, we'll give an embedding of $\mathcal{O}_K$ into the $\mathbb{R}^n$ which will map ideals to lattices. This perspective, along with the theorem above, will help us study the size of the class group. First, we show how Minkowski's convex body theorem can be used to give an alternate proof of Lagrange's four square's theorem to that seen in the previous chapter.

5.5.3. Another Proof of Lagrange's Four Square Theorem. We give an alternate prof of Theorem 4.24. Note that if we can write integers $n = a^2 + b^2 + c^2 + d^2$ and $m = A^2 + B^2 + C^2 + D^2$ as sums of four squares, then we can write

$$mn = (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2.$$

So, it suffices to show that any prime is a sum of four squares. Since we have

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

we may assume that p is an odd prime. Observe by the pigeonhole principle there exists integers u, v so that

$$u^2 + v^2 + 1 \equiv (\operatorname{mod} p).$$

Let Λ be the lattice in $\mathbb{R}^4$ generated

$$(p, 0, 0, 0)$$

$$(0, p, 0, 0)$$

$$(u, v, 1, 0)$$

$$(-v, u, 0, 1).$$

Observe that $\det(\Lambda) = p^2$. Furthermore for any $(x_1, x_2, x_3, x_4) \in \Lambda$ it can be checked that

$$ux_1 + vx_2 \equiv x_3 (\operatorname{mod} p),$$

$$ux_2 - vx_1 \equiv x_4 (\operatorname{mod} p)$$

which gives

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= x_1^2 + x_2^2 + (ux_1 + vx_2)^2 + (ux_2 - vx_1)^2 \\ &= (u^2 + v^2 + 1)(x_1^2 + x_2^2) \\ &\equiv 0 (\operatorname{mod} p). \end{aligned}$$

Now, let $X = B_r(0)$ be a ball in $\mathbb{R}^4$ of radius r centered at the origin with $r = \sqrt{2p}$. Then,

$$\operatorname{vol}(X) = (1/2)\pi^2 (2p)^2 > 2^4 \det(\Lambda).$$

So by Minkowski's Convex Body Theorem, there exists a nonzero point (a, b, c, d) in Λ and in X. Since (a, b, c, d) is in Λ then by above we have

$$a^2 + b^2 + c^2 + d^2 \equiv 0 (\operatorname{mod} p),$$

and since $(a, b, c, d) \in X$, which is a ball of radius $r = \sqrt{2p}$ then we have

$$0 < a^2 + b^2 + c^2 + d^2 < 2p$$

which gives $a^2 + b^2 + c^2 + d^2 = p$ as desired. □

5.6. Ideals as Lattices

Let K be a number field of degree n. Note that if $\sigma : K \hookrightarrow \mathbb{C}$ is any embedding fixing $\mathbb{Q}$, then so is $\bar{\sigma}$, where

$$\bar{\sigma}(\alpha) := \overline{\sigma(\alpha)}$$

for any $\alpha \in K$ (note that the bar notation above means to take the complex conjugate). Since $\bar{\sigma} = \sigma$ if and only if $\sigma(K) \subseteq \mathbb{R}$, then the complex embeddings must come in conjugate pairs and $n = r + 2s$, where r denotes the number of real embeddings and $2s$ the number of complex embeddings. Label the embeddings so that $\sigma_1, \ldots, \sigma_r$ are real (that is $\sigma_i(K) \subseteq \mathbb{R}$ for $i = 1, \ldots, r$) and so that $\sigma_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \ldots, \bar{\sigma}_{r+s}$ are complex. Then, for each element $\alpha \in K$ we can define a map $\Psi : K \to \mathbb{R}^n$ by

$$\Psi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \Re(\sigma_{r+1}(\alpha)), \Im(\sigma_{r+1}(\alpha)), \ldots, \Re(\sigma_{r+s}(\alpha)), \Im(\sigma_{r+s}(\alpha))),$$

where $\Re(z)$ and $\Im(z)$ denote the real and imaginary parts of a complex number z, respectively. We have the following.

Theorem 5.65. *If $\mathfrak{a}$ is any ideal in $\mathcal{O}_K$, then $\Lambda_{\mathfrak{a}} := \Psi(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$ with*

$$\det(\Lambda_{\mathfrak{a}}) = 2^{-s}\sqrt{|\Delta(\mathfrak{a})|},$$

where s is the number of complex conjugate pair embeddings $K \hookrightarrow \mathbb{C}$.

Proof. Recall that any ideal $\mathfrak{a}$ is a free $\mathbb{Z}$-module with rank $n = [K : \mathbb{Q}]$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be any $\mathbb{Z}$-basis for $\mathfrak{a}$. Note that Ψ is $\mathbb{Z}$-linear, and so $\Psi(\mathfrak{a})$ is generated by $\{\Psi(\alpha_1), \ldots, \Psi(\alpha_n)\}$. Next, consider the matrix

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \cdots & \Re(\sigma_{r+i}(\alpha_1) & \Im(\sigma_{r+i}(\alpha_1)) & \cdots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \cdots & \Re(\sigma_{r+i}(\alpha_n) & \Im(\sigma_{r+i}(\alpha_n)) & \cdots \end{pmatrix}.$$

Let

$$C_i := \begin{pmatrix} \mathbb{R}(\sigma_{r+i}(\alpha_1)) \\ \vdots \\ \Re(\sigma_{r_i}(\alpha_n)) \end{pmatrix} \text{ and } C_{i+1} = \begin{pmatrix} \Im(\sigma_{r+i}(\alpha_1) \\ \vdots \\ \Im(\sigma_{r+i}(\alpha_n) \end{pmatrix}).$$

Then, if we replace C_i with $C_i + iC_{i+1}$ and then afterwards replace C_{i+1} with $-2iC_{i+1} + C_1$, we obtain the matrix

$$B = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \cdots & \sigma_{r+i}(\alpha_1) & \bar{\sigma}_{r+i}(\alpha_1) & \cdots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \cdots & \sigma_{r+i}(\alpha_n) & \bar{\sigma}_{r+i}(\alpha_n) & \cdots \end{pmatrix}$$

with $\det(B) = (2i)^s \det(A)$. Hence,

$$|((2i)^s \det(A))^2| = |\det(B)^2| = |\Delta(\mathfrak{a})| \Rightarrow |\det(A)| = 2^{-s}\sqrt{|\Delta(\mathfrak{a})|}.$$

Furthermore, since $\Delta(\mathfrak{a}) \neq 0$ then we know that the set $\{\Psi(\alpha_1), \ldots, \Psi(\alpha_n)\}$ is $\mathbb{R}$-linearly independent, making $\Lambda_{\mathfrak{a}} := \Psi(\mathfrak{a})$ a lattice with covolume as desired. □

We now apply Minkowski's Convex Body Theorem. The result below will be the key fact we'll need in the next section.

Theorem 5.66. *If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$, then there's a nonzero $\alpha \in \mathfrak{a}$ with*

$$|N_K(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{a})|},$$

where s is the number of complex conjugate pair embeddings $K \hookrightarrow \mathbb{C}$.

Proof. Let $[K : \mathbb{Q}] = n$ and $n = r + 2s$ where r denotes the number of real embeddings, and s the number of complex conjugate pair embeddings $K \hookrightarrow \mathbb{C}$. For $\varepsilon > 0$, let $c_1, \ldots, c_r$ and $d_1, \ldots, d_s$ be real numbers so that

$$\left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{a})|} + \varepsilon = c_1 \cdots c_r d_1 \cdots d_s.$$

Define the set $X \subseteq \mathbb{R}^n$ by

$$X = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| < c_i \text{ and } |x_{r+j}^2 + x_{r+j+1}^2| < d_j\},$$

where $i \in \{1, \ldots, r\}$ and $j \in \{1, \dot{;}s\}$. Observe that

$$\operatorname{vol}(X) = 2^r \pi^s c_1 \cdots c_r d_1 \cdots d_s.$$

So,

$$\begin{aligned} \operatorname{vol}(X) &> 2^r \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{a})|} \\ &= 2^{r+s} \sqrt{|\Delta(\mathfrak{a})|} \\ &= 2^n \det(\Lambda_{\mathfrak{a}}). \end{aligned}$$

So, by Minkowki's convex body theorem, there's a nonzero element $(x_1, \ldots, x_n) \in X$ that's also contained in the lattice $\Lambda_{\mathfrak{a}}$. Since $(x_1, \ldots, x_n) \in \Lambda_{\mathfrak{a}}$, then there's an element $\alpha \in \mathfrak{a}$ with

$$\sigma_1(\alpha) = x_1, \ldots, \sigma_r(\alpha) = x_r$$

$$\sigma_{r+i}(\alpha) = x_{r+i} + ix_{r+i+1}, \text{ for } i = 1, 3, \ldots, 2s - 1,$$

where $\sigma_1, \ldots, \sigma_r$ are the real embeddings and $\sigma_{r+1}, \sigma_{r+2s}$ are the distinct complex embeddings $K \hookrightarrow \mathbb{C}$. And since $(x_1, \ldots, x_n) \in X$ we have

$$|\sigma_i(\alpha)| = c_i$$

for all $i \in \{1, \ldots, n\}$. So,

$$|N_K(\alpha)| = |\sigma_1(\alpha) \cdots \sigma_n(\alpha)| < c_1 \cdots c_n = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{a})|} + \varepsilon.$$

Now, let A_ε be the set of all α satisfying

$$|N_K(\alpha)| < \sqrt{|\Delta(\mathfrak{a})|} + \varepsilon.$$

Since lattices are discrete (a fact we have not shown, but isn't too difficult), and the image $\Psi(A_\varepsilon)$ is bounded then A_ε must be finite. Since each $A_\varepsilon \neq \varnothing$ then there must exist an element

$$\alpha \in \bigcap_\varepsilon A_\varepsilon.$$

That is, $|N_K(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{a})|}$ as desired. □

5.7. Finiteness of the Class Group

The following Corollary will be the last step we need to prove that the class group of any number field is finite.

Corollary 5.67. For any $[\mathfrak{a}] \in \mathrm{Cl}(K)$ there's an ideal $\mathfrak{c}$ in $\mathcal{O}_K$ with $[\mathfrak{a}] = [\mathfrak{c}]$ in $\mathrm{Cl}(K)$ and

$$N_K(\mathfrak{c}) \leq (2/\pi)^s \sqrt{|\Delta_K|}.$$

Proof. Take any fractional ideal $\mathfrak{a}$ in $\mathrm{Id}(K)$ and let d be a common divisor of $\mathfrak{a}^{-1}$ so that $\mathfrak{b} = d\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. By Theorem 5.66 there's an element $\alpha \in \mathfrak{b}$ so that

$$|N_K(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{\Delta(\mathfrak{b})}$$

and by Theorem 5.55 we rewrite the right hand side to get

$$|N_K(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}N_K(\mathfrak{b}).$$

Since $\alpha \in \mathfrak{b}$ then $(\alpha) \subseteq \mathfrak{b}$. So by Exercise 18 there's an ideal $\mathfrak{c}$ with $\mathfrak{c}\mathfrak{b} = (\alpha)$. By Theorem 5.57 we have $N_K(\mathfrak{c})N_K(\mathfrak{b}) = |N_K(\alpha)|$ and so from above we get

$$N_K(\mathfrak{c}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

It can then be checked that $[\mathfrak{c}] = [\mathfrak{a}]$ in $\mathrm{Cl}(K)$. □

The finiteness of the class group then follows directly from the following observation.

Proposition 5.68. There are only finitely many ideals with a fixed norm.

We leave this proof as an exercise.

Example 5.69. Let $K = \mathbb{Q}(\sqrt{-5})$. We'll show that $h_K = 2$ using the results above.

By Exercise 9 we have that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, which we know does not have unique factorization by Exercise 10, so $h_K > 1$. Note that the embeddings $K \hookrightarrow \mathbb{C}$ are given by

$$\sigma_1 : \sqrt{-5} \mapsto \sqrt{-5}, \text{ and } \sigma_2 : \sqrt{-5} \mapsto -\sqrt{-5}.$$

So, $\sigma_2 = \bar{\sigma}_1$ are a pair of complex conjugate embeddings, giving $r = 0$ and $s = 1$. We compute $\Delta_K = -20$ and so we have

$$\left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|} = \frac{2}{\pi}\sqrt{20} < 2.85.$$

By Corollary 5.67 every ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is equivalent to an ideal $\mathfrak{c}$ with norm 1 or 2. If $N_K(\mathfrak{c}) = 1$, then we would have $\mathfrak{c} = \mathcal{O}_K$, which gives $[\mathfrak{a}]$ equal to the equivalence class of principal fractional ideals. Now, if $N_K(\mathfrak{c}) = 2$ then by Theorem 5.57(b) we have that $2 \in \mathfrak{c}$. By Exercise 18 this tells us that $(2) = \mathfrak{c}\mathfrak{d}$ for some ideal $\mathfrak{d}$ in $\mathcal{O}_K$. But observe that

$$(2) = (2, 1 + \sqrt{-5})^2$$

and furthermore since $N_K((2, 1+\sqrt{-5})) = 2$, then $(2, 1+\sqrt{-5})$ is prime with norm 2. Hence, the only ideal with norm 2 in $\mathcal{O}_K$ is $(2, 1 + \sqrt{-5})$. So, every fractional ideal in $\mathcal{O}_K$ is either a principal fractional ideal, or equivalent to $(2, 1+\sqrt{-5})$ which gives $h_K = 2$.

5.8. Existence of Extensions with Unique Factorization

While $\mathcal{O}_K$ may not always have unique factorization, the fact that the class group of K is always finite will tell us the situation isn't as bad as we might think. First, we need the following lemma.

Lemma 5.70. *Let K be a number field. Then there exists a finite extension L of K so that for every ideal $\mathfrak{a}$ in $\mathcal{O}_K$ we have that $\mathfrak{a}\mathcal{O}_L$ is a principal ideal in $\mathcal{O}_L$.*

Proof. We give a sketch of this proof, and skip some of the details for the sake of time. Since $\mathrm{Cl}(K)$ is finite, we can write $\mathrm{Cl}(K) = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_h]\}$ where $h = h_K$ and we can choose $\mathfrak{a}_i$ to be ideals in $\mathcal{O}_K$ (rather than fractional ideals). Note that for each $\mathfrak{a}_i$ we have $\mathfrak{a}_i^h = (\alpha_i)$ for $\alpha_i \in \mathcal{O}_K$. Let

$$L = K(\alpha_1^{1/h}, \ldots, \alpha_h^{1/h}).$$

It can be shown that for each i we have that $\mathfrak{a}_i L$ is principal. Since every ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is equivalent to one of the $\mathfrak{a}_i$, and $\mathfrak{a}_i\mathcal{O}_L$ is principal by above, with a bit of work it follows that $\mathfrak{a}\mathcal{O}_K$ is also principal. □

We have the following.

Theorem 5.71. *For a number field K, there exists a finite extension L of K so that for every nonzero nonunit $a \in \mathcal{O}_K$ can be written uniquely (up to units and permutation) in the form*

$$a = p_1 \cdots p_r,$$

for nonunits (but not necessarily irreducible) p_i in $\mathcal{O}_L$.

Proof. Let L be as in Lemma 5.70, and take any $a \in \mathcal{O}_K$. Then, we can factor the ideal (a) in $\mathcal{O}_K$ as

$$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_t,$$

for prime ideal $\mathfrak{p}_i$ in $\mathcal{O}_K$. By the previous lemma, we know that $\mathfrak{p}_i\mathcal{O}_L = p_i\mathcal{O}_L$ and so we get

$$(a)\mathcal{O}_L = p_1 \cdots p_t\mathcal{O}_L.$$

By Exercise 15 this implies that $a = up_1 \cdots p_t$ for a unit $u \in \mathcal{O}_L^\times$. Uniqueness of the p_i (up to units) follows from unique factorization of the ideal (a). □

Exercises

1. Show that the minimal polynomial $m_\alpha(X)$ of an algebraic number α is unique. *(Hint: use the division algorithm in $\mathbb{Q}[X]$)*
2. This problem will finish the our computation of the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{5}$ from Example 5.4. Show that $f(X) = X^4 - 14X^2 + 9$ does not have a quadratic factor. (*Hint: suppose that $f(X) = (X^2+aX+b)(X^2+cX+d)$. Use the fact that $f(X) = f(-X)$ and compare coefficients to show that no such integers a, b, c, d could exist).*
3. Show that the following complex numbers are algebraic. Determine which are algebraic integers. (Bonus: also find their minimal polynomials).
   (a) $(1+i)/\sqrt{2}$
   (b) $i + \sqrt{2}$
   (c) $e^{2\pi i/3} + 2$
   (d) $\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}$
4. Show that the set of algebraic numbers $\bar{\mathbb{Q}}$ is countable. Conclude that there exists infinitely many transcendental numbers.
5. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Find all monomorphisms $K \hookrightarrow \mathbb{C}$ that fix $\mathbb{Q}$.
6. Let K be a number field with $[K : \mathbb{Q}] = n$. Prove the following.
   (a) For any $p, q \in \mathbb{Q}$ and $\alpha, \beta \in K$
   $$\begin{aligned} N_K(p\,\alpha\beta) &= p^n N_K(\alpha) N_K(\beta), \text{ and} \\ \operatorname{Tr}_K(p\alpha + q\beta) &= p \operatorname{Tr}_K(\alpha) + q \operatorname{Tr}_K(\beta). \end{aligned}$$
   (b) If $\alpha \in K$ with $[K : \mathbb{Q}] = n$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$ then
   $$\begin{aligned} N_K(\alpha) &= d^n N_{\mathbb{Q}(\alpha)}(\alpha), \text{ and} \\ \operatorname{Tr}_K(\alpha) &= d \operatorname{Tr}_{\mathbb{Q}(\alpha)}(\alpha), \end{aligned}$$
   where $d = n/m$.
   (c) An element $u \in \mathcal{O}_K$ is a unit (that is, u has a multiplicative inverse) if and only if $N_K(u) = \pm 1$.
   (d) If $p \in \mathcal{O}_K$ is prime, then $N_K(p)$ is a "rational prime" (that is, $N_K(p)$ is a prime in $\mathbb{Z}$; we typically will add the adjective "rational" when we want to emphasize our element is a prime in $\mathbb{Z}$ instead of in $\mathcal{O}_K$).
7. Show that $\Delta(\alpha_1, \ldots, \alpha_n) = 0$ if and only if the α_i are linearly dependent.
8. Find the ring of integers for the following number fields.
   (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
   (b) $\mathbb{Q}(\sqrt{2}, i)$
   (c) $\mathbb{Q}(\sqrt[3]{2})$
   (d) $\mathbb{Q}(\sqrt[4]{2})$
9. Let $K = \mathbb{Q}(\sqrt{D})$ for a square-free integer D. Show that
   $$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D \not\equiv 1 (\operatorname{mod} 4) \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & \text{if } D \equiv 1 (\operatorname{mod} 4). \end{cases}$$

(Hint: observe that in the quadratic case, α is an algebraic integer if and only if $N_K(\alpha)$ and $\mathrm{Tr}_K(\alpha)$ are both integers).

10. Show that $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives two distinct factorizations of 6 into irreducibles in the ring $\mathbb{Z}[\sqrt{-5}]$.
11. Show that the ideal (X) is prime but not maximal in $\mathbb{Z}[X]$.
12. This problem will finish the proof of Lemma 5.49.
    (a) For a commutative ring R, show that an ideal $\mathfrak{a} \subseteq R$ is prime if and only if $R/\mathfrak{a}$ is an integral domain.
    (b) Show that any finite integral domain is a field.
    (c) Conclude that every prime ideal in $\mathcal{O}_K$ is maximal.
13. Let $R = \mathbb{Z}[\sqrt{-5}]$ and consider the ideals
$$\mathfrak{p} = (2, 1+\sqrt{-5})$$
$$\mathfrak{q} = (3, 1+\sqrt{-5})$$
$$\mathfrak{r} = (3, 1-\sqrt{-5}).$$
Show that these ideals are maximal (and hence prime). Furthermore, show that
$$\mathfrak{p}^2 = (2), \mathfrak{q}\mathfrak{r} = (3)$$
$$\mathfrak{p}\mathfrak{q} = (1+\sqrt{-5}), \mathfrak{p}\mathfrak{r} = (1-\sqrt{-5}).$$
14. Using the previous problem, show that the distinct factorizations into irreducibles from Problem 10 comes from two different groupings of the factorization into prime ideals $(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{r}$.
15. Show that for two principal ideals $(x), (y)$ in an integral domain R, if $(x) = (y)$ then $x = uy$ for a unit u.
16. Show that an element p in an integral domain R is prime if and only if the ideal (p) is prime.
17. Use Minkowski's Convex Body Theorem to show that every prime $p \equiv 1 (\bmod 4)$ is a sum of two integer squares by considering a lattice with elements of the form (x_1, x_2) where $x_2 \equiv ux_1 (\bmod p)$ and u is any integer with $u^2 \equiv 1 (\bmod p)$.
18. This problem will help finish the proof of Theorem 5.67. Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_K$ with $\mathfrak{a} \subseteq \mathfrak{b}$, then there exists an ideal $\mathfrak{c}$ so that $\mathfrak{c}\mathfrak{b} = \mathfrak{a}$. For this reason, we sometimes use the notation $\mathfrak{b} \mid \mathfrak{a}$ to mean $\mathfrak{a} \subseteq \mathfrak{b}$.
19. Prove Theorem 5.68; that is, show there are only finitely many ideals with a fixed norm. Conclude that the class group of any number field is finite. *(Hint: use unique factorization in $\mathcal{O}_K$ and Theorem 5.57).*

Diophantine Analysis Revisited

We end the semester by looking at how some of the tools we developed in the previous chapter can help us solve further Diophantine problems.

6.1. Further Mordell Equations

The following example shows how we can generalize the techniques from Examples 4.25 and 4.26 when the ring we factor over does not have unique factorization. This example is pulled from Keith Conrad's expository note [**Conb**].

Example 6.1. We show that the Mordell equation $Y^2 = X^3 - 5$ has no integer solutions. Suppose for a contradiction that there were integers x, y with $y^2 = x^3 - 5$. Factoring over $\mathbb{Z}[\sqrt{-5}]$ gives

$$x^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

It can be shown (by taking norms) that $y + \sqrt{-5}$ and $y - \sqrt{-5}$ have no common divisors other than units. But, as we saw in Exercise 10, the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, so we cannot conclude that $y \pm \sqrt{-5}$ are perfect cubes. Instead, we pass to ideals. Let $K = \mathbb{Q}(\sqrt{-5})$ and recall by Exercise 9 that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then we have equality of ideals in $\mathcal{O}_K$

$$(x)^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

Write

$$(y + \sqrt{-5}) = \mathfrak{p}_1 \cdots \mathfrak{p}_t \text{ and } (y - \sqrt{-5}) = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

for prime ideals $\mathfrak{p}_i, \mathfrak{q}_j$ in $\mathcal{O}_K$, which we recall are unique up to permutation and units. We claim that none of the $\mathfrak{p}_i$ are equal to any of the $\mathfrak{q}_j$. If they were, say $\mathfrak{p} = \mathfrak{p}_i = \mathfrak{q}_j$ for some i, j then we'd have

$$(y + \sqrt{-5}) = \mathfrak{p}\mathfrak{a} \text{ and } (y + \sqrt{-5}) = \mathfrak{p}\mathfrak{b}$$

for some ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}_K$ and so

$$y + \sqrt{-5} \in (y + \sqrt{-5}) = \mathfrak{p}\mathfrak{a} \subseteq \mathfrak{p}\mathfrak{a}\mathfrak{b}$$
$$y - \sqrt{-5} \in (y - \sqrt{-5}) = \mathfrak{p}\mathfrak{b} \subseteq \mathfrak{p}\mathfrak{a}\mathfrak{b}$$

which gives $2\sqrt{-5} \in \mathfrak{p}\mathfrak{a}\mathfrak{b}$. Taking norms, we have that

$$N_K(\mathfrak{p}) \mid |N_K(2\sqrt{-5})| = 20.$$

But since $(y + \sqrt{-5}) = \mathfrak{p}\mathfrak{a}$ then we also have

$$N_K(\mathfrak{p}) \mid |N(y + \sqrt{-5})| = y^2 + 5.$$

Looking at the equation $x^3 = y^2 + 5$ modulo 4, it can be shown that y must be even and so $N_K(\mathfrak{p})$ is odd, giving $N_K(\mathfrak{p}) = 5$ and by above this gives

$$5 = N_K(\mathfrak{p}) \mid (y^2 + 5) \Rightarrow 5 \mid y.$$

Since $x^3 = y^2 + 5$ we have $5 \mid x$ as well, but then

$$5 = x^3 - y^2 \equiv 0 (\operatorname{mod} 25)$$

a contradiction. So the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ do not share a common prime ideal factor. Since ideals factor uniquely in $\mathcal{O}_K$, and their product is equal $(x)^3$ we must have

$$(y + \sqrt{-5}) = \mathfrak{a}^3 \text{ and } (y - \sqrt{-5}) = \mathfrak{b}^3$$

for ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}_K$. Since $\mathfrak{a}^3$ is principal, we know that the order of $\mathfrak{a}$ divides 3 in $\mathrm{Cl}(K)$. But by Example 5.69 we know that $h_K = 2$ and so we must have the order of $\mathfrak{a}$ equal to 1 in $\mathrm{Cl}(K)$. That is, $\mathfrak{a}$ (and similarly $\mathfrak{b}$) is principal. So we can write

$$(y + \sqrt{-5}) = (\alpha)^3 = (\alpha^3), \text{ and } (y - \sqrt{-5}) = (\beta)^3 = (\beta^3)$$

for elements $\alpha, \beta \in \mathcal{O}_K$ and so by Exercise 15 we have

$$y + \sqrt{-5} = u\alpha^3, \text{ and } y - \sqrt{-5} = v\beta^3$$

for units $u, v \in \mathcal{O}_K^\times$. In Exercise 5 you'll show that $\mathcal{O}_K^\times = \{\pm 1\}$ and so we can replace α, β with $-\alpha, -\beta$ if needed to write

$$y + \sqrt{-5} = \alpha^3, \text{ and } y - \sqrt{-5} = \beta^3$$

for $\alpha, \beta \in \mathcal{O}_K$. We can now proceed as before. Write

$$y + \sqrt{-5} = (a + b\sqrt{-5})^3.$$

Comparing coefficients of $\sqrt{-5}$ gives

$$3a^2b - 5b^3 = 1 \Rightarrow b(3a^2 - 5b^2) = 1$$

and so $b = \pm 1$. But we see there is no integer solution a to the equation above.

6.2. A Special Case of Fermat's Last Theorem

Recall Fermat's last theorem, which we introduced at the end of Chapter 4, claims that there are no nontrivial integer solutions to the equation $X^n + Y^n = Z^n$ for $n \geq 3$. Note that it suffices to prove this theorem only for prime exponents n. Our goal in this section will be to prove the following special case of Fermat's last theorem.

Theorem 6.2. *If p is an odd regular prime (defined below), then the equation*

$$X^p + Y^p = Z^p \tag{6.1}$$

has no solutions (x, y, z) with $p \nmid xyz$.

With some extra work, the condition that $p \nmid xyz$ can be removed. For details about this case, see Keith Conrad's expository note [**Conc**]. The proof of Theorem 6.2 will start similarly to our strategy for solving Mordell equations. Observe that if (x, y, z) is a solution to the Fermat equation (6.1) then we can factor over the *cyclotomic field* $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a pth root of unity, to write

$$z^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y).$$

As before, our main step will be using the class group of K to show that the terms $x + \zeta_p^i y$ are pth powers. First, we look in more details at cyclotomic fields.

6.2.1. Cyclotomic Fields.

Given an integer n, a *cyclotomic field* is a number field of the form $K = \mathbb{Q}(\zeta)$ where ζ is a primitive nth root of unity. Sometimes we will refer to K as the nth cyclotomic field. Recall that the nth cyclotomic polynomial is defined by

$$\Phi_n(X) = \prod(X - \zeta),$$

where the product is taken over all primitive nth roots of unity. It is a field theory exercise (which we will skip here) that the cyclotomic polynomials are irreducible, and so

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

For our purposes, we will only need to consider cyclotomic fields coming from pth roots of unity ζ_p for a prime p. In this case,

$$\mathbb{Q}(\zeta_p) : \mathbb{Q}) = p - 1$$

and

$$\Phi_p(X) = \prod_{i=1}^{p-1}(X - \zeta^i)$$

where ζ is any fixed primitive pth root of unity. This tells us that the conjugates of ζ are precisely ζ^i for $i \in \{1, \ldots, p-1\}$. We will need the following lemmas.

Lemma 6.3. *For any cyclotomic field $K = \mathbb{Q}(\zeta)$ we have $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Proof. (Let's get through our special case of FLT first, and come back to this if time). □

Lemma 6.4. *The units of $\mathbb{Z}[\zeta]$ are of the form $r\zeta^k$ where $r \in \mathbb{R}$ and $k \in \mathbb{Z}$.*

Proof. (Ditto). □

6.2.2. Regular Primes. A prime p is said to be *regular* if p does not divide the class number h_K, where $K = \mathbb{Q}(\zeta)$ is the pth cyclotomic field. Our best known result on regular primes relates them to the Bernouilli numbers (which we do not discuss here). It is conjectured there are infinitely many regular primes, with asymptotic density about 60%, although both of these conjectures are still open. If these are true, Fermat's last theorem is then true by somewhat elementary means about 60% of the time. No one knows exactly the proof that Fermat was imagining when he wrote his conjecture in the margins of his book. To me, it seems possible that he was imagining some sketch of the proof we give below, but did not realize unique factorization failed in cyclotomic fields. We'll see, similar to the Mordell equation we solved above, that this issue can be fixed when the class number is "well behaved" (that is, when p is regular, which again we expect is true about 60% of the time). After this, the proof follows similarly to the elementary examples we saw in Chapter 4.

6.2.3. Proof of Theorem 6.2. For time, we sketch the beginning of this argument. Note first that since p is odd then

$$X^p + Y^p = Z^p$$

has a solution if and only if

$$X^p + Y^p = -Z^p$$

does. So we instead work with the second equation. Supposing that (x, y, z) is an integer solution, we factor over the pth cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_p$, to get

$$-z^p = \prod_{i=0}^{p-1}(x + \zeta^i y).$$

As in our Mordell equation example, this gives an equation of ideals

$$(z)^p = \prod_{i=0}^{p-1}(x + \zeta^i y).$$

We first claim that the ideals $(x + \zeta^i y)$ have no prime ideal factors in common. For a contradiction, suppose $\mathfrak{p} \mid (x + \zeta^i y)$ and $\mathfrak{p} \mid (x + \zeta^j y)$ for a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ and $i < j$. Then, $x + \zeta^i y, x + \zeta^j y$ are elements of $\mathfrak{p}$ and so

$$x + \zeta^i y - (x + \zeta^j y) = y\zeta^i(1 - \zeta^k)$$

is also an element of $\mathfrak{p}$, where $k = j - i$. Observe that

$$1 - \zeta^\ell = (1 - \zeta)(1 + \zeta + \cdots + \zeta^{\ell-1})$$

for any j. So $1 - \zeta$ divides $1 - \zeta^k$ and if we choose t so that $kt \equiv 1 (\bmod p)$ then $1 - \zeta^k$ divides $1 - \zeta^{kt} = 1 - \zeta$. So by Exercise 3 we have that $1 - \zeta^k = u(1 - \zeta)$ for a unit $u \in \mathcal{O}_K^\times$. Since ζ^k is also a unit, this gives

$$y(1 - \zeta) \in \mathfrak{p}.$$

Since $\mathfrak{p}$ is prime we have either $y \in \mathfrak{p}$ or $1 - \zeta \in \mathfrak{p}$. Observe that we may assume x, y and z are pairwise relatively prime. If $y \in \mathfrak{p}$ and by assumption $x - \zeta^i y \in \mathfrak{p}$ then by above we also get $z^p \in p$. But since $\gcd(y, z^p) = 1$ this gives $1 \in \mathfrak{p}$, a contradiction.

Now, if $1-\zeta \in \mathfrak{p}$ then $N_K(1-\zeta)$ divides $N(z) = z^{p-1}$. In Exercise 4 you'll show that $N_K(1-\zeta) = p$ which gives $p \mid z$, a contradiction. Hence, the ideals $(x+\zeta^i y)$ must not have any common prime ideal in their unique factorizations. Since ideals in $\mathcal{O}_K$ factor uniquely, this gives that

$$(x+y\zeta) = \mathfrak{a}^p$$

for some ideal $\mathfrak{a}$ in $\mathcal{O}_K$. But, this tells us that $\mathfrak{a}^p$ is principal, and so the order of $\mathfrak{a}$ in $\mathrm{Cl}(K)$ divides p. Since $p \nmid h_K$, $\mathfrak{a}$ must be principal to start with, and so

$$(x+y\zeta) = (\delta)^p \Rightarrow x+y\zeta = u\delta^p,$$

for $\delta \in \mathcal{O}_K$ and where u is a unit in $\mathcal{O}_K$. Note that this is precisely the step we would have ended up at if $\mathbb{Z}[\zeta]$ were a UFD! The rest of this argument uses some congruence considerations, more complicated but similar in style to what we saw in Chapter 4. For time, we'll skip the rest of this argument, and instead refer the reader to Keith Conrad's expository note [**Conc**].

Exercises

1. Let $K = \mathbb{Q}(\sqrt{-5})$. Show that $\mathcal{O}_K^\times = \{\pm 1\}$, where $\mathcal{O}_K^\times$ denotes the units of $\mathcal{O}_K$.
2. Let p be an odd prime, and $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive pth root of unity. Show that
$$N_K(\zeta_p^s) = 1 \text{ for all } s \in \mathbb{Z}, \text{ and}$$
$$\mathrm{Tr}_K(\zeta_p^s) = \begin{cases} -1 & \text{if } s \not\equiv 0 (\operatorname{mod} p) \\ p-1 & \text{if } s \equiv 0 (\operatorname{mod} p). \end{cases}$$
3. Let a, b be elements of a commutative ring R. If $a \mid b$ and $b \mid a$ show that $a = ub$ for a unit $u \in R^\times$.
4. Show that $N_K(1-\zeta) = p$, where $K = \mathbb{Q}(\zeta)$ and ζ is a primitive pth root of unity.

Bibliography

[AGP94] W. R. Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722. MR 1283874

[Akh22] Shabnam Akhtari, *Quartic index form equations and monogenizations of quartic orders*.

[Apo76] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976. MR 0434929

[AZ18] Martin Aigner and Günter M. Ziegler, *Proofs from The Book*, sixth ed., Springer, Berlin, 2018, See corrected reprint of the 1998 original [MR1723092], Including illustrations by Karl H. Hofmann. MR 3823190

[Bac90] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. MR 1023756

[BG15] Michael A. Bennett and Amir Ghadermarzi, *Mordell's equation: a classical approach*, LMS J. Comput. Math. **18** (2015), no. 1, 633–646. MR 3406453

[BHV01] Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122, With an appendix by M. Mignotte. MR 1863855

[Bru93] J. W. Bruce, *A really trivial proof of the Lucas-Lehmer test*, Amer. Math. Monthly **100** (1993), no. 4, 370–371. MR 1209464

[Car14] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **15** (1913/14), no. 1-4, 49–70. MR 1502459

[Cas97] J. W. S. Cassels, *An introduction to the geometry of numbers*, Classics in Mathematics, Springer-Verlag, Berlin, 1997, Corrected reprint of the 1971 edition.

[Cla18] Pete Clark, *Number Theory: A Contemporary Introduction*, http://alpha.math.uga.edu/~pete/4400FULL2018.pdf, 2018, [Online; accessed 22-August-2022].

[Cona] Keith Conrad, *Carmichael Numbers and Korselt's Criterion*, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf, [Online; accessed 27-September-2022].

[Conb] ———, *EXAMPLES OF MORDELL'S EQUATION, II*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn2.pdf, [Online; accessed 29-November-2022].

[Conc] ———, *Fermat's Last Theorem for Regular Primes*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/fltreg.pdf, [Online; accessed 04-December-2022].

[Cond] ———, *Square Patterns and Infinitely Many Primes*, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/squaresandinfmanyprimes.pdf, [Online; accessed 30-August-2022].

[Cone] ———, *The Infinitude of the Primes*, https://kconrad.math.uconn.edu/math3240s20/handouts/infinitudeofprimes.pdf, [Online; accessed 30-August-2022].

[Conf] ———, *The Miller-Rabin Test*, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf, [Online; accessed 29-September-2022].

[Gam06] Adam Gamzon, *The Hasse-Minkowski Theorem*, https://opencommons.uconn.edu/srhonors_theses/17, 2006, [Online; accessed 9-October-2022].

[GSS19] T. Alden Gassert, Hanson Smith, and Katherine E. Stange, *A family of monogenic S_4 quartic fields arising from elliptic curves*, J. Number Theory **197** (2019), 361–382. MR 3906505

[HPS14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An introduction to mathematical cryptography*, second ed., Undergraduate Texts in Mathematics, Springer, New York, 2014. MR 3289167

[IS12] Patrick Ingram and Joseph H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 243–271. MR 2867920

[Ros88] Michael I. Rosen, *A proof of the Lucas-Lehmer test*, Amer. Math. Monthly **95** (1988), no. 9, 855–856. MR 967346

[Ros00] Kenneth H. Rosen, *Elementary number theory and its applications*, fourth ed., Addison-Wesley, Reading, MA, 2000. MR 1739433

[Sch96] Wolfgang M Schmidt, *Diophantine approximation*, Springer Science & Business Media, 1996.

[Ser73] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French. MR 0344216

[Sil88] Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237. MR 961918

[Sil13] ———, *Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture*, J. Number Theory **133** (2013), no. 9, 2948–2963. MR 3057058

[ST16] Ian Stewart and David Tall, *Algebraic number theory and Fermat's last theorem*, fourth ed., CRC Press, Boca Raton, FL, 2016. MR 3443702

[Tao] Terry Tao, *The Lucas-Lehmer Test for Mersenne primes*, https://terrytao.wordpress.com/2008/10/02/the-lucas-lehmer-test-for-mersenne-primes/, [Online; accessed 02-October-2022].