PMATH 340 Course Notes

Elementary Number Theory

Haochen Wu

University of Waterloo
Winter 2021

Contents

1 MATH 135 Review **1**
1.1 Divisibility . . . 1
1.2 Primes . . . 1
1.3 Division Algorithm . . . 2
1.4 GCDs . . . 2
1.5 Coprime . . . 2
1.6 The Fundamental Theorem of Arithmetic . . . 3
1.7 Modulos . . . 3
1.8 Congurence Class . . . 5
1.9 Linear Diophantine Equation . . . 6
1.10 Zero Divisors . . . 6
1.11 Chinese Remainder Theorem . . . 7

2 Quadratic Residues **9**
2.1 Euler's Criterion . . . 9
2.2 Properties of Legendre Symbol . . . 9
2.3 Gauss's Lemma . . . 10
2.4 Properties of Legendre Symbol Continued . . . 10
2.5 The Law of Quadratic Reciprocity . . . 10
2.6 The General Quadratic . . . 11

3 Introduction to Multiplicative Functions **13**
3.1 Multiplicative Functions . . . 13
3.2 Perfect Numbers . . . 14
3.3 Mobius μ-function . . . 15
3.3.1 Inversion . . . 15

4 Continued Fractions **17**
4.1 Motivation . . . 17
4.2 Decimals of Rationals . . . 17
4.3 Continued Fractions . . . 18
4.4 Convergents . . . 19
4.5 Infinite Continued Fractions . . . 20
4.6 Rational Approximation . . . 22
4.7 Quadratic Irrationals . . . 23
4.8 Eventually Periodic Continued Fractions . . . 23
4.9 Periodic Continued Fractions . . . 25
4.10 Continued Fraction of $\sqrt{d}$ . . . 26
4.11 Pell's Equations . . . 26

5 Some Random Stuff **29**
5.1 Pythagorean Triples . . . 29

5.2 $n = 4$ case of FLT 30
5.3 Which Numbers are a Sum of Two Squares? 31

Chapter 1 MATH 135 Review

Sets that we will work with

- Natural Numbers: $\mathbb{N} = \{1, 2, 3, 4, ...\}$. Note that $0 \notin \mathbb{N}$
- Integers: $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$
- Rationals: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$
- Reals: $\mathbb{R}$

1.1 Divisibility

Definition 1.1. Let $a, b \in \mathbb{Z}$. We say that a **divides** b**,** a **is a divisor of** b, written $a \mid b$, if there exists an integer c such that $ac = b$. Otherwise, we write $a \nmid b$

Proposition 1.2. Let $a, b, c, x, y \in \mathbb{Z}$:

- If $a \mid b$ and $b \mid c$, then $a \mid c$
- If $c \mid a$ and $c \mid b$, then $c \mid ax + by$
- If $c \mid a$ and $c \nmid b$, then $c \nmid a \pm b$
- If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$
- If $a \mid b$ and $b \mid a$, then $a = \pm b$
- If $a \mid b$ then $\pm a \mid \pm b$
- $1 \mid a$
- $a \mid 0$
- $0 \mid a$ if and only if $a = 0$

1.2 Primes

Definition 1.3. Let $p \geq 2$ be a natural number. We say that p is a **prime** if the only positive divisors of p are 1 and p. Otherwise, p is a composite.

Lemma 1.4. Let $n \geq 2$ be a natural number. Then n has a prime divisor

Theorem 1.5. Euclid: There are infinitely many prime numbers

1.3 Division Algorithm

Proposition 1.6. Let $a, b \in \mathbb{Z}$ with $a > 0$. There exists unique integers q, r such that

- $b = aq + r$, and
- $0 \leq r < a$

1.4 GCDs

Definition 1.7. Let $a, b \in \mathbb{Z}$, not both 0. The **greatest common divisor** of a and b, written $\gcd(a, b)$ is the unique integer d that satisfies the following two conditions:

- $d \mid a$ and $d \mid b$
- Whenever c is a common divisor of a and b, we have that $c \leq d$

We also define $\gcd(0, 0) = 0$

Proposition 1.8. For all integers a, b, q, we have that

$$\gcd(a, b) = \gcd(b, a - bq)$$

In particular, in the case where $b = aq + r$ in the Division Algorithm, we have

$$\gcd(a, b) = \gcd(b, r)$$

Definition 1.9. Let $a, b \in \mathbb{Z}$. For integers c that can be written in the form $ax + by$ for some $x, y \in \mathbb{Z}$. We call $ax + by$ an **integer combination** of a, b.

Theorem 1.10. Bezout's Lemma: Let $a, b \in \mathbb{Z}$, not both 0. Let d be the smallest positive integer combination of a and b, then

- d divides every integer combination of a, b
- $d = \gcd(a, b)$

1.5 Coprime

Definition 1.11. Let $a, b \in \mathbb{Z}$. We say that a, b are **coprime** if $\gcd(a, b) = 1$

Corollary 1.12. Corollary of **Bezout's Lemma**. Let $a, b \in \mathbb{Z}$. If $ax + by = 1$ has a solution, then $\gcd(a, b) = 1$

Proposition 1.13. Let $a, b, c \in \mathbb{Z}$ with a, b coprime. If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Proposition 1.14. Let $a, b, c \in \mathbb{Z}$ with a, b coprime. If $a \mid bc$, then $a \mid c$.

Theorem 1.15. Euclid's Lemma: Let p be a prime. Let $a, b \in \mathbb{Z}$. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Corollary 1.16. Corollary of **Euclid's Lemma**: Let p be a prime. Let $a_1, \cdots, a_n \in \mathbb{Z}$. If $p \mid (a_1 \times \cdots \times a_n)$ then there is an integer $1 \leq i \leq n$ such that $p \mid a_i$

1.6 The Fundamental Theorem of Arithmetic

Theorem 1.17. The Fundamental Theorem of Arithmetic, aka **Unique Factorization Theorem**:

Let $n \in \mathbb{N}$ with $n \geq 2$. There exists primes $p_1, \cdots, p_k$ such that $n = p_1 \cdots p_k$. Up to the ordering of the product, these primes are unique.

Proposition 1.18. Let $n \in \mathbb{N}$ with $n \geq 2$. Suppose that $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of n (with p_i all distinct primes). The positive divisors of n are exactly those numbers of the form $p_1^{b_1} \cdots p_k^{b_k}$ with $0 \leq b_i \leq a_i$ for all i.

1.7 Modulos

Definition 1.19. Let $a, b \in \mathbb{Z}$ and $n \geq 2$. We say that a **is congruent to b mod(ulo)** n, written $a \equiv b \mod n$, if $n \mid (a - b)$

Proposition 1.20. Congurence $\mod n$ is an equivalent relation. That is, congruence $\mod n$ is:

- reflexive: for any integer a, we have that $a \equiv a \mod n$.
- symmetric: if $a \equiv b \mod n$, then $b \equiv a \mod n$
- transitive: if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$

Remark: Saying that $a \equiv b \mod n$ is equivalent to saying that a is obtained from b by adding a multiple of n: there exists $k \in \mathbb{Z}$ such that $a = b + kn$.

Remark: Saying that $a \mid b$ is equivalent to saying that $b \equiv 0 \mod a$ (or $0 \equiv b \mod a$)

Remark:

- Given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, we can divide a by n: there exists unique $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $a = qn + r$.
- In other words, there exists a unique number r in the integer interval $[0, n-1]$ such that $a \equiv r \mod n$
- In other words, $\mod n$, every integer in congruent to exactly one of $0, 1, 2, \cdots, n-1$. The process of finding r is called reducing a modulo n

Proposition 1.21. Let $a, b, c, d \in \mathbb{Z}$, and let $n \in \mathbb{N}$. Assume $a \equiv b \mod n$ and $c \equiv d \mod n$. Then:

- $a + c \equiv b + d \mod n$
- $ac \equiv bd \mod n$

Corollary 1.22. If $a \equiv b \mod n$, then for any $k \in \mathbb{N}$, we have that $a^k \equiv b^k \mod n$

Proposition 1.23. If $ac \equiv bc \mod n$ and $\gcd(c, n) = 1$, then $a \equiv b \mod n$

Proposition 1.24. Let $N \in \mathbb{Z}$. Then $11 \mid N$ if and only in the alternating sum of the digits of N is divisible by 11.

Proposition 1.25. Let $N \in \mathbb{Z}$. Then $7 \mid N$ if and only if the alternating sum of length 3 blocks of N, starting from the right, is divisible by 7.

Proposition 1.26. Let $N \in \mathbb{Z}$ and $N = 10x + y$ with $0 \leq y \leq 9$. That is, let y be the final digit of N, and let x be the number obtained by deleting the ones digit of N. Then, $7 \mid N$ if and only if $7 \mid x - 2y$

Remark: Gievn $a, b \in \mathbb{Z}$, we have that if $a = b$, then for any $n \in \mathbb{N}$, we must have $a \equiv b \mod n$. This can be useful when showing some equations have no integer solutions.

1.8 Congurence Class

Definition 1.27. Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. The **congruence class of** a **modulo** n, written $[a]$ or $[a]_n$, is the set

$$\{x \in \mathbb{Z} : x \equiv a \mod n\} = \{a + qn : q \in \mathbb{Z}\}$$

An integer in $[a]$ is called a **representative** of $[a]$. We often omit n.

Proposition 1.28. Fix $n \in \mathbb{N}$. All our congruences classes are with respect to n. Then $[a] = [b]$ if and only if $a \equiv b \mod n$.

So, there are exactly n different congruence classes when working with $\mod n$

Every integer is in exactly one of $[0], [1], \cdots, [n-1]$. That is, $[0] \cup [1] \cup \cdots \cup [n-1] = \mathbb{Z}$, and $[a] \cap [b] = \emptyset$ for all $0 \leq a, b, \leq n-1$ when $a \neq b$

Definition 1.29. Let $n \in \mathbb{N}$. The **integers** $\mod n$, denoted $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}_n$, is the set of all congruence class $\mod n$. That is,

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$$

Definition 1.30. Let $n \in \mathbb{N}$. We define the following operations on $\mathbb{Z}_n$:

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

These operations are **well-defined**. That is, if $[a] = [b]$ and $[c] = [d]$, then $[a] + [c] = [b] + [d]$ and $[a][c] = [b][d]$

Definition 1.31. We say that $[a]$ is a **zero divisor** of $\mathbb{Z}_n$ if there exists some $[b] \neq [0]$ in $\mathbb{Z}_n$ so that $[a][b] = [0]$.

Definition 1.32. Let $n \in \mathbb{N}$. We say that $[a]$ is a **unit** of $\mathbb{Z}_n$ (or that $[a]$ is **invertible** in $\mathbb{Z}_n$) if there exists $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$

Equivalently, $[a]$ is a unique of $\mathbb{Z}_n$ if the equation $ax \equiv 1 \mod n$ has a solution.

We call $[b]$ the inverse of $[a]$, and write $[b] = [a]^{-1}$

1.9 Linear Diophantine Equation

Theorem 1.33. Let $a, b, c \in \mathbb{Z}$, and let $d = \gcd(a, b)$. Consider the equation $ax + by = c$. We are interested in integer solutions x, y to this equation.

- The equation has a solution if and only if $d \mid c$
- if (x_0, y_0) is a solution to the equation, then the complete solution is given by

$$(x, y) = (x_0 + \frac{b}{d}n, y - \frac{a}{d}n)$$

as n ranges over all integers

Theorem 1.34. Consider the equation $ax \equiv c \mod n$. Let $d = \gcd(a, n)$.

- The equation has a solution if and only if $d \mid c$
- If x_0 is one solution to $ax \equiv c \mod n$, then every solution is congruent to exactly one of

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \cdots, x_0 + (d-1)\frac{n}{d}$$

- Equivalently, if $[x_0]$ is one solution to $[a][x] = [c]$ in $\mathbb{Z}_n$, then the complete solution is

$$[x_0], [x_0 + \frac{n}{d}], \cdots, [x_0 + (d-1)\frac{n}{d}]$$

1.10 Zero Divisors

Corollary 1.35. Let $a \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Then $[a]$ is a unit of $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.

Proposition 1.36. $[a]$ is a zero divisor of $\mathbb{Z}_n$ if and only if $\gcd(a, n) > 1$

Corollary 1.37. Let $n \in \mathbb{N}$:

- If n is a prime, then every element of $\mathbb{Z}_n$ except for $[0]$ is a unit.
- If n is a composite, then $\mathbb{Z}_n$ has a non-trivial zero divisor.

Definition 1.38. The set of all units of $\mathbb{Z}_n$ is denoted by $\mathbb{Z}_n^*$

Definition 1.39. For $n \in \mathbb{Z}_n$, we define $\phi(n)$ to be the number of integers $1 \leq k < n$ so that $\gcd(k, n) = 1$. The function ϕ is called the **Euler Phi Function**, or **Euler's Totient**

Function.

Proposition 1.40. Let $[a], [b] \in \mathbb{Z}_n^*$, then $[a][b] \in \mathbb{Z}_n^*$

Theorem 1.41. Euler's Theorem: Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$ so that $\gcd(a, n) = 1$. Then, $a^{\phi(n)} \equiv 1 \mod n$.

Equivalently, let $n \in \mathbb{N}$, and let $[a] \in \mathbb{Z}_n^*$, then $[a]^{\phi(n)} = [1]$.

Theorem 1.42. Fermat's Little Theorem (FℓT): Let p be a prime, and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$

1.11 Chinese Remainder Theorem

Proposition 1.43. Splitting the Modulus: Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Let $a, b \in \mathbb{Z}$. Then $a \equiv b \mod mn$ if and only if $a \equiv b \mod m$ and $a \equiv b \mod n$

Theorem 1.44. Chinese Remainder Theorem (Sunzi):

Let $m_1, m_2 \in \mathbb{N}$ be coprime. Let $a_1, a_2 \in \mathbb{Z}$. The system of simultaneous congruences

$$x \equiv a_1 \mod m_1$$

$$x \equiv a_2 \mod m_2$$

has a solution. Furthermore, any two solutions are congruent to each other modulo $m_1 m_2$

Theorem 1.45. Generalized Chinese Remainder Theorem:

Let $m_1, m_2, \cdots, m_k \in \mathbb{N}$ with $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Let $a_1, \cdots, a_k \in \mathbb{Z}$. The system of simultaneous congruences

$$x \equiv a_1 \mod m_1$$

$$\vdots$$

$$x \equiv a_k \mod m_k$$

has a solution, and this solution is unique modulo $m_1 \times \cdots \times m_k$

To solve such system, we may

1. Let $M = m_1 \times \cdots \times m_k$. For $1 \leq i \leq k$, let $M_i = \frac{M}{m_i}$

2. For $1 \leq i \leq k$, let c_i be a solution to $M_i x \equiv 1 \mod m_i$
3. Let $A = a_1 M_1 c_1 + \cdots + a_k M_k c_k$
4. Then A is a solution to the system

Chapter 2 Quadratic Residues

Definition 2.1. Let $m \in \mathbb{N}$, and let $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. We say that a is a **quadratic residue modulo** m if the equation $x^2 \equiv a \mod m$ has an (integer) solution. Otherwise, we say that a is a **quadratic nonresidue modulo** m

Now, let p be an odd prime, and let $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$.

Proposition 2.2. The congruence $x^2 \equiv a \mod p$ has either no solutions, or has exactly two incongruent solutions $\mod p$

Proposition 2.3. There are exactly $\frac{p-1}{2}$ incongruent quadratic residues $\mod p$ and exactly $\frac{p-1}{2}$ incongruent quadratic nonresidues $\mod p$

Definition 2.4. Let p be an odd prime. Let $a \in \mathbb{Z}$ with $p \nmid a$ (equivalent to $\gcd(a, p) = 1$). Then, the **Legendre Symbol** of a modulo p, denoted $\left(\frac{a}{p}\right)$ is defined as:

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

2.1 Euler's Criterion

Theorem 2.5. Euler's Criterion:

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

Theorem 2.6. Wilson's Theorem: If p is a prime, then $(p-1)! \equiv -1 \mod p$

Actually, the converse is true as well.

2.2 Properties of Legendre Symbol

Proposition 2.7. Let p be an odd prime. Let $a, b \in \mathbb{Z}$ such that $p \nmid a$ and $p \nmid b$. Then

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

By this proposition, we know that, if $a \in \mathbb{Z}$ and $p \nmid a$, we can write $a = \pm 2^{a_0} p_1^{a_1} \cdots p_k^{a_k}$, where p_i are distinct odd primes, also distinct from p, and the a_i are positive integers, then we know

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{a_0}\left(\frac{p_1}{p}\right)^{a_1}\cdots\left(\frac{p_k}{p}\right)^{a_k}$$

In other words, we want to calculate $\left(\frac{\pm 1}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{q}{p}\right)$ where q is an odd prime distinct from p.

First off, $\left(\frac{1}{p}\right) = 1$

Theorem 2.8. Let p be an odd prime. Then,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

2.3 Gauss's Lemma

Lemma 2.9. Gauss's Lemma: Let p be an odd prime, and let $a \in \mathbb{Z}$ such that $p \nmid a$. Let n be the number of remainders larger than $\frac{p}{2}$ when each of $a, 2a, \cdots, (\frac{p-1}{2})a$ are divided by p. Then,

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

2.4 Properties of Legendre Symbol Continued

Theorem 2.10. Let p be an odd prime. Then,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \mod 8 \\ -1 & \text{if } p \equiv 3, 5 \mod 8 \end{cases}$$

2.5 The Law of Quadratic Reciprocity

We now turn the problem of calculate $\left(\frac{p}{q}\right)$ where p and q are odd primes.

Theorem 2.11. The Law of Quadratic Reciprocity, By Gauss: Let p and q be distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$
$$= \begin{cases} -1 & \text{if } p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 4 \\ 1 & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \end{cases}$$

Lemma 2.12. Let p be an odd prime. Let $a \in \mathbb{Z}$ be odd with $p \nmid a$. Let

$$N = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor$$

The

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

2.6 The General Quadratic

Now, consider the general case: $ax^2 + bx + c \equiv 0 \mod p$ where p is an odd prime, $p \nmid a$.

Let $y = 2ax + b$ and $d = b^2 - 4ac$. Note that given any value of y, the equation $2ax \equiv b - y \mod p$ has a unique solution for x. In other words, change of variables is invertible.

Theorem 2.13. $ax^2 + bx + c \equiv 0 \mod p$ has a solution x if and only if $y^2 \equiv d \mod p$ has a solution y.

Corollary 2.14. $ax^2 + bx + c \equiv 0 \mod p$ has a solution if and only if $\left(\frac{b^2 - 4ac}{p}\right) = 1$

Theorem 2.15. Let p be an odd prime, $p \nmid a$. The equation $x^2 \equiv a \mod p$ has a solution if and only if for any $k \in \mathbb{N}$, the equation $x^2 \equiv a \mod p^k$ has a solution.

In the case of having a solution, the equation $x^2 \equiv a \mod p^k$ has exactly two incongruent solutions.

Proposition 2.16. Let p, q be distinct odd primes, and let $a \in \mathbb{Z}$ such that $p \nmid a$ and $q \nmid a$.

Then, $x^2 \equiv a \mod pq$ has a solution if and only if $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a}{q}\right) = 1$.

In the case of having a solution, there are exactly 4 incongruent solutions modulo pq.

Lemma 2.17. If $p \mid a$, then the equation $x^2 \equiv a \mod p$ has exactly one incongruent solution.

Proposition 2.18. Let $N = p_1^{b_1} \times \cdots \times p_k^{b_k}$ where the p_i's are odd and distinct primes and the b_i's are positive integers. Let $a \in \mathbb{Z}$ be such that $p_i \nmid a$ for all i. The congruence

$$x^2 \equiv a \mod N$$

has a solution if and only if each $\left(\frac{a}{p_i}\right) = 1$.

In the case of having a solution, there are exactly 2^k incongruent solutions modulo N.

If $p = 2$... then (Let $a \in \mathbb{Z}$, $2 \nmid a$):

- The congruences $x^2 \equiv a \mod 2$ has exactly one incongruent solution $\mod 2$. This is because we have $b \equiv -b \mod 2$ for all $b \in \mathbb{Z}$.
- If $x^2 \equiv a \mod 4$ has a solution, it has exactly two incongruent solutions $\mod 4$.
- Now let $k \geq 3$. The congurence $x^2 \equiv a \mod 2^k$ has a solution if and only if $a \equiv 1 \mod 8$. In the case it has a solution, there are exactly four incongruent solutions $\mod 2^k$
- There is a pattern to these four solutions. For example, the four solutions to $x^2 \equiv 1 \mod 2048$ is $1, 1023, 1025, 2047$

Chapter 3 Introduction to Multiplicative Functions

3.1 Multiplicative Functions

Definition 3.1. A function $f : \mathbb{N} \to \mathbb{C}$ is said to be **multiplicative** if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$

In this course, most/all of our functions will actually be $f : \mathbb{N} \to \mathbb{Z}$

Note that any multiplicative function satisfies $f(1) = f(1)f(1)$, so $f(1)$ must be either 0 or 1. If there is some k such that $f(k) \neq 0$, then we must have $f(1) = 1$ since $f(k) = f(k)f(1)$.

Suppose f is multiplicative and $n = p_1^{a_1} \cdots p_k^{a_k}$. Then $f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k})$. In other words, multiplicative functions are exactly those functions that are determined by their values at prime powers.

So,to give a multiplicative function, for each prime p and natural number n, you have to define $f(p^n)$. You also have to define $f(1)$ to be either 0 or 1, and it has to be 1 unless the function is identically 0.

Theorem 3.2. Suppose that $f(n)$ is multiplicative. Then, the function

$$g(n) = \sum_{d|n, d>0} f(d)$$

is also multiplicative

Definition 3.3. For $n \in \mathbb{N}$, let $\nu(n)$ denote the number of positive divisors of n

Proposition 3.4. $\nu(n)$ is multiplicative.

Proposition 3.5. Let p be prime, and let $k \in \mathbb{N}$. Then $\nu(p^k) = k + 1$

Proposition 3.6. Let $n \in \mathbb{N}$, then

$$(\sum_{d|n, d>0} \nu(d))^2 = \sum_{d|n, d>0} \nu(d)^3$$

It is a famous identity that

$$[\frac{(k+1)(k+2)}{2}]^2 = 1^3 + 2^3 + \cdots + (k+1)^3$$

Proposition 3.7. Let $n \in \mathbb{N}$. Then $\nu(n)$ is odd if and only if n is a perfect square.

Theorem 3.8. $\phi(n)$ is multiplicative

Proposition 3.9. Let p be a prime, and k be a positive integer. Then

$$\phi(p^k) = p^{k-1}(p-1)$$

$\prod_{p|n}$ means the product over all distinct prime divisors of n

Proposition 3.10. For all $n \in \mathbb{N}, n \geq 2$, we have

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

Let $f(n) = \sum_{d|n} \phi(d)$. We know that $f(n)$ is multiplicative.

Theorem 3.11. Gauss:

$$\sum_{d|n} \phi(d) = n$$

Let $n \in \mathbb{N}$. We define $\sigma(n) = \sum_{d|n, d>0} d$. We have that $\sigma(n)$ is equal to the sum of positive divisors of n. Also, $\sigma(n)$ is multiplicative.

Proposition 3.12. Given a prime p, and $k \in \mathbb{N}$. We have that

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$$

3.2 Perfect Numbers

Definition 3.13. Given $n \in \mathbb{N}$, we say that n is **perfect** if n equals the sum of it's positive and strict divisors. That is, n is perfect if $\sigma(n) = 2n$

Definition 3.14. A prime number which is one less than a power of 2 is called a **Mersenne prime**.

That is, a Mersenne prime is a prime number of the form $2^n - 1$.

Theorem 3.15. Let $n \in \mathbb{N}$. We have that n is an even perfect number if and only if there exists a prime of the form $2^\alpha - 1$ such that $n = 2^{\alpha-1}(2^\alpha - 1)$

3.3 Mobius μ-function

Definition 3.16. Given $n \in \mathbb{N}$, we define

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{there exists some prime } p \text{ so that } p^2 \mid n \\ (-1)^r & n = p_1 p_2 \cdots p_r \text{ with } p_1, p_2, ..., p_r \text{ distinct primes} \end{cases}$$

The function μ is called the **Mobius μ-function**.

Proposition 3.17. μ is multiplicative

Proposition 3.18. Let $n \in \mathbb{N}$. Then

$$\sum_{d|n, d>0} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

From now on, when we write $\sum_{d|n}$, we actually mean $\sum_{d|n, d>0}$

3.3.1 Inversion

Suppose we have functions f, g (f, g are not necessarily multiplicative) such that $f(n) = \sum_{d|n} g(d)$. Can we express $g(n)$ in terms of various values of f?

Theorem 3.19. Mobius Inversion Theorem: Let f, g be two functions (whose domains are $\mathbb{N}$). Then

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

if and only if

$$g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d) \quad (= \sum_{d|n} \mu(d) f(\frac{n}{d}))$$

We know that:

- We can always write $f(n)$ as a sum/difference of $g(d)$ as d ranges over all divisors of n
- We also know how to do this.

Corollary 3.20. Mobius Inversion Theorem tells us that:

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

Lemma 3.21. Given any functions F, G, the following equation (of nested sums) holds

$$\sum_{d|n} F(\frac{n}{d}) \sum_{c|d} G(c) = \sum_{c|n} G(c) \sum_{d|\frac{n}{c}} F(d)$$

Chapter 4 Continued Fractions

4.1 Motivation

We are used to describing real number using decimal representations - powers of 10. For example, when we write 23.668, we really mean

$$10^1 \times 2 + 10^0 \times 3 + 10^{-1} \times 6 + 10^{-2} \times 6 + 10^{-3} \times 8$$

Pros:

- It has been used for a long time
- It's easy to compare sizes (just compare the leftmost unequal digit)

Cons:

- Not all rational numbers are treated equally. For example, $\frac{8}{5} = 1.6, \frac{8}{3} = 2.6666\cdots, \frac{8}{7} = 1.\overline{142857}$
- Why do we use 10?
- Decimal expansions are not unique

So, we are going to give a new system of representing real numbers using sequences of integers. Along the way, we will answer some cool questions like "What is the best rational approximation of an irrational number?"

4.2 Decimals of Rationals

Example 4.1. We first show an example on how to find the decimal expansion of a rational number.

Take $\frac{57}{25}$. We have that $57 = 25(2) + 7$, so $\frac{57}{25} = 2 + \frac{7}{25}$.

Then, write $\frac{7}{25} = \frac{1}{10} \times \frac{70}{25} = \frac{1}{10}(2 + \frac{20}{25})$.

Then, we have $\frac{20}{25} = \frac{1}{10} \times \frac{200}{25} = \frac{1}{10} \times 8$.

So,

$$\begin{aligned}
\frac{57}{25} &= 2 + \frac{1}{10}(2 + \frac{20}{25}) \\
&= 2 + \frac{1}{10}(2 + \frac{1}{10} \times 8) \\
&= 2 + \frac{2}{10} + \frac{8}{100} \\
&= 10^0 \times 2 + 10^{-1} \times 2 + 10^{-2} \times 8 \\
&= 2.28
\end{aligned}$$

Next, consider $\frac{41}{333}$. We can write $\frac{41}{333} = \frac{1}{10} \times \frac{410}{333} = \frac{1}{10}(1 + \frac{77}{333})$.

Then, we write $\frac{77}{333} = \frac{1}{10} \times \frac{770}{333} = \frac{1}{10}(2 + \frac{104}{333})$.

Then, we write $\frac{104}{333} = \frac{1}{10} \times \frac{1040}{333} = \frac{1}{10}(3 + \frac{41}{333})$

So $\frac{41}{333} = \frac{1}{10}(1 + \frac{77}{333}) = \frac{1}{10}(1 + \frac{1}{10}(2 + \frac{104}{333})) = \frac{1}{10}(1 + \frac{1}{10}(2 + \frac{1}{10}(3 + \frac{41}{333})))$

So, $\frac{41}{333} = \frac{1}{10} + \frac{2}{100} + \frac{3}{1000} + \frac{1}{1000}\frac{41}{333}$

It follows that $\frac{41}{333} = 0.\overline{123}$

Definition 4.2. Let $\beta \in \mathbb{R}, 0 < \beta < 1$, with $\beta = \sum_{n=1}^{\infty} \frac{a^n}{10^n}$, with each $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

We say that this decimal representation is **eventually periodic** if there exists $\tau \in \mathbb{N}$ and $N \in \mathbb{N}$ such that $a_{n+\tau} = a_n$ whenever $n \geq N$. The smallest such τ is called the **period**.

Theorem 4.3. Let $\beta = \sum_{n=1}^{\infty} \frac{a^n}{10^n}$. Then $\beta \in \mathbb{Q}$ if and only if this decimal representation is eventually periodic.

4.3 Continued Fractions

Example 4.4. Consider the fraction $\frac{62}{13}$. Let's do some divisions:

$$\begin{aligned} 62 &= 13(4) + 10 \\ 13 &= 10(1) + 3 \\ 10 &= 3(3) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

So,

$$\begin{aligned} \frac{62}{13} &= 4 + \frac{10}{13} \\ &= 4 + \frac{1}{(\frac{13}{10})} \\ &= 4 + \frac{1}{1 + \frac{3}{10}} \\ &= 4 + \frac{1}{1 + \frac{1}{(\frac{10}{3})}} \\ &= 4 + \frac{1}{1 + \frac{1}{3 + \frac{1}{3}}} \end{aligned}$$

This expression is called the continued fraction expansion of $\frac{62}{13}$

Definition 4.5. An expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

with $a_1, a_2, \cdots a_n$ positive real numbers, is called a **finite continued fraction**, and is denoted by $[a_0, a_1, \cdots, a_n]$. It is called a **finite continued simple fraction** if, in addition, each a_i is an integer.

Note that a continued fraction representation of 7 is $[7]$. Another continued fraction representation of 7 is $[6, 1]$ since $7 = 6 + \frac{1}{1}$

Note that $[a, b, c, d] = [a, b, c + \frac{1}{d}]$

Proposition 4.6. If $[a, b, c, d]$ is simple, then $a < [a, b, c, d] < a + 1$.

Likewise, we can say $a + \frac{1}{b+1} < [a, b, c, d] < a + \frac{1}{b}$

Proposition 4.7. Let $\alpha \in \mathbb{R}$. Then $\alpha \in \mathbb{Q}$ if and only if α can be expressed as a finite simple continued fraction.

4.4 Convergents

Definition 4.8. Let $\alpha = [a_0, a_1, \cdots, a_n]$ be a simple continued fraction.

For $0 \leq i \leq n$, we define the i-th **convergent** of α, written as C_i, to be

$$[a_0, a_1, \cdots, a_i]$$

Example 4.9. Let $\alpha = \frac{237}{101}$. It turns out that $\alpha = [2, 2, 1, 7, 1, 3]$. So,

$$\begin{array}{ll} C_0 = \frac{2}{1} & C_1 = \frac{5}{2} \\ C_2 = \frac{7}{3} & C_3 = \frac{54}{23} \\ C_4 = \frac{61}{26} & C_5 = \frac{237}{101} = \alpha \end{array}$$

By calculating $\alpha - C_i$, we may notice that

1. $|\alpha - C_i| \to 0$

2. $C_0 < C_2 < C_4$
3. $C_1 > C_3 > C_5$

This is true in general.

Proposition 4.10. Let $\alpha = [a_0, a_1, \cdots, a_n]$ be a finite continued fraction. Define the following recursive sequences $p_0, p_1, \cdots, p_n$ and $q_0, q_1, \cdots, q_n$ by

$$\begin{array}{lll} p_0 = a_0 & p_1 = a_0a_1 + 1 & p_i = a_ip_{i-1} + p_{i-2} \text{ for } 2 \leq i \leq n \\ q_0 = 1 & q_1 = a_1 & q_i = a_iq_{i-1} + q_{i-2} \text{ for } 2 \leq i \leq n \end{array}$$

Then, $C_i = \frac{p_i}{q_i}$ for all $0 \leq i \leq n$

Lemma 4.11. For all $1 \leq i \leq n$, we have that $p_iq_{i-1} - p_{i-1}q_i = (-1)^{i-1}$

Corollary 4.12. $\gcd(p_i, q_i) = 1$ for all $0 \leq i \leq n$

Proposition 4.13. The followings are true:

1. $C_i - C_{i-1} = \frac{(-1)^{i-1}}{q_iq_{i-1}}$ for all $1 \leq i \leq n$
2. $C_i - C_{i-2} = \frac{(-1)^i a_i}{q_iq_{i-2}}$ for all $2 \leq i \leq n$

Proposition 4.14. The increasing/decreasing property:

1. $C_0 < C_2 < C_4 < \cdots$
2. $C_1 > C_3 > C_5 > \cdots$
3. $C_{2j} < C_{2j+1}$ for all i, j

4.5 Infinite Continued Fractions

In calculus, we define the value of an infinite sum to be a limit of the partial sums. For example, when we write down $0.\overline{5}$, we mean

$$\sum_{n=1}^{\infty} \frac{5}{10^n}$$

by which we really mean

$$\lim_{N\to\infty} \sum_{n=1}^{\infty} \frac{5}{10^n}$$

We are going to define infinite continued fractions similarly.

Lemma 4.15. Let $[a_0, a_1, \cdots, a_n]$ be a finite simple continued fraction. Then $q_i \geq i$ for all i.

Theorem 4.16. Let $a_0, a_1, a_2, ...$ be a sequence of integers, with $a_i > 0$ whenever $i > 0$. For each $i \geq 0$, if we define $C_i = [a_0, a_1, \cdots, a_i]$. Then,

$$\lim_{i \to \infty} C_i$$

exists. This limit α is called the value of the infinite simple continued fraction $[a_0, a_1, \cdots]$, and we call C_i the i-th convergent of this infinite continued fraction

This is kind of the analogue of the result that says: given any sequence $b_0, b)1, b_2, \cdots \in \{0, 1, ..., 9\}$ we have that $\lim_{n\to\infty} \sum_{i=0}^{n} \frac{b^i}{10^i}$ exists.

Example 4.17. Let $\alpha = [2, 5, 2, 5, 2, 5, ...] = [\overline{2, 5}]$. Then $\alpha = [2, 5, \alpha]$. So,

$$\alpha = 2 + \frac{1}{5 + \frac{1}{\alpha}}$$

which gives $\alpha = 1 + \sqrt{\frac{7}{5}}$

Given $\alpha \in \mathbb{R}$, we can write α as an infinite continued fraction. To do so, we first let $a_0 = \lfloor \alpha \rfloor$. Then,

$$\alpha = a_0 + (\alpha - a_0) = a_0 + \frac{1}{\frac{1}{\alpha - a_0}} = a_0 + \frac{1}{a_1}$$

where we define $\alpha_1 = \frac{1}{\alpha - a_0}$. From here, we let $a_1 = \lfloor \alpha_1 \rfloor$, and then let $a_2 = \frac{1}{\alpha_1 - a_1}$, and so on:

$$a_i = \lfloor \alpha_i \rfloor \text{ for } i \geq 0$$
$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} \text{ for } i \geq 0$$

Theorem 4.18. Let $a \in \mathbb{R}$. Then α may be represented as an infinite (simple) continued fraction if and only if $\alpha \in \mathbb{R} - \mathbb{Q}$.

Remark: There are rational numbers that have both a finite decimal expansion and an infinite decimal expansion (for example, $1 = 0.\bar{9}$). This is not true for continued fractions.

If we can use precise expression in the above iterative process (for example, use $\sqrt{3}$ along with the process and do not substitute with its decimal approximations), we might be able to discover the pattern in continued fractions and see how the pattern repeats.

Proposition 4.19. Suppose that $[a_0, a_1, a_2, \cdots] = [b_0, b_1, b_2, \cdots]$. Then $a_i = b_i$ for all $i \geq 0$.

Remark: Note that $[c_0, c_1, c_2, \cdots] = c_0 + \frac{1}{[c_1, c_2, c_3, \cdots]}$

4.6 Rational Approximation

Theorem 4.20. Let $\gamma \in \mathbb{R} - \mathbb{Q}$. Given any $\epsilon > 0$, there exists $\frac{a}{b} \in \mathbb{Q}$ such that $|\gamma - \frac{a}{b}| < \epsilon$

That being said, our only goal with rational approximations is not so make $|\gamma - \frac{a}{b}|$ as small as possible. We also want to make b not too large.

Proposition 4.21. Let $\gamma \in \mathbb{R} - \mathbb{Q}$. Let $\frac{p_i}{q_i}$ be a convergent of γ. For all $a, b \in \mathbb{Z}$ with $0 < b < q_{i+1}$, we have that

$$|q_i\gamma - p_i| \leq |b\gamma - a|$$

Corollary 4.22. Let $\gamma \in \mathbb{R} - \mathbb{Q}$. Let $\frac{p_i}{q_i}$ be a convergent of γ. Let $a, b \in \mathbb{Z}$ with $1 \leq b \leq q_i$. Then,

$$|\gamma - \frac{p_i}{q_i}| \leq |\gamma - \frac{a}{b}|$$

Remark: This is not a good rational approximation for free. To calculate convergents, we needed an already known approximation of a irrational number.

Theorem 4.23. Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $b > 0$. Let $\alpha \in \mathbb{R} - \mathbb{Q}$ such that $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$. Then, $\frac{a}{b}$ is a convergent of α

Remark: Given a convergent $C_i = \frac{p_i}{q_i}$ of α, it is not necessarily the case that $|\alpha - C_i| < \frac{1}{2q_i^2}$

Remark: it can be shown that $|\alpha - C_i| < \frac{1}{q_i^2}$ for every i. In fact, it essentially has been. Previously, we showed that $|\alpha - C_i| < \frac{1}{q_i q_{i+1}}$. Since $q_{i+1}q_i > q_i^2$, the result is true.

Theorem 4.24. Hurwitz, ∼1890: Let $\gamma \in \mathbb{R} - \mathbb{Q}$.

1. There exists infinitely distinct rational numbers $\frac{a}{b}$ such that $|\gamma - \frac{a}{b}| < \frac{1}{\sqrt{5}b^2}$
2. $\sqrt{5}$ is "best possible". That is, if $C > \sqrt{5}$, then there exists only finitely many $\frac{a}{b}$ such that $|\frac{1+\sqrt{5}}{2} - \frac{a}{b}| < \frac{1}{Cb^2}$

Theorem 4.25. Roth, 1952: Let $\gamma \in \mathbb{R} - \mathbb{Q}$. Let $k > 2$. There exists only finitely many rational numbers $\frac{a}{b}$ such that $|\gamma - \frac{a}{b}| < \frac{1}{b^k}$

4.7 Quadratic Irrationals

Definition 4.26. Let $\alpha \in \mathbb{R} - \mathbb{Q}$. We say that α is a **quadratic irrational** number if α is the root of a quadratic polynomial with integer coefficients. That is, α is a **quadratic irrational** if there exists $A, B, C \in \mathbb{Z}, A \neq 0$ such that $A\alpha^2 + B\alpha + C = 0$

Proposition 4.27. Let $\alpha \in \mathbb{R}-\mathbb{Q}$. α is a quadratic irrational number if and only if $\alpha = \frac{a+\sqrt{b}}{c}$ for some $a, b, c \in \mathbb{Z}$ with $b > 0$ and b not a perfect square, and $c \neq 0$

Lemma 4.28. Let α be a quadratic irrational number. Let $a, b, c, d \in \mathbb{Z}$ with c, d not both zero. Then, $\frac{a\alpha+b}{c\alpha+d}$ is either a rational number or a quadratic irrational number.

Definition 4.29. Let $\alpha = [a_0, a_1, a_2, ...]$ be an infinite continued fraction. We say that α is **eventually periodic** if there exists $N, \tau \in \mathbb{N}$ such that $a_{n+\tau} = a_n$ whenever $n \geq N$. The smallest such τ is called the period. In this case, we write

$$\alpha = [a_0, a_1, \cdots, a_{N-1}, \overline{a_N, a_{N+1}, ..., a_{N+\tau-1}}]$$

Theorem 4.30. Let $\alpha = [a_0, a_1, \cdots, a_{N-1}, \overline{a_N, a_{N+1}, ..., a_{N+\tau-1}}]$ be an eventually periodic simple continued fraction. Then, α is a quadratic irrational.

4.8 Eventually Periodic Continued Fractions

Theorem 4.31. Let $\alpha \in \mathbb{R}$. Then α is a quadratic irrational if and only if the continued fraction expression of α is eventually periodic.

Lemma 4.32. Let α be a quadratic irrational. Then we may write $\alpha = \frac{P+\sqrt{d}}{Q}$ where $P, d, Q \in \mathbb{Z}$, d is a positive integer that isn't a perfect square, $Q \neq 0$, and $Q \mid (d - P^2)$

Proposition 4.33. Let $\alpha = \frac{P_0+\sqrt{d}}{Q_0}$ with P_0, Q_0, d integers, $Q_0 \neq 0$, d positive and not a perfect square, with $Q_0 \mid d - P_0^2$. Define sequences $(\alpha_n)_{n=0}^{\infty}, (a_n)_{n=0}^{\infty}, (P_n)_{n=0}^{\infty}, (Q_n)_{n=0}^{\infty}$ as follows:

$$\begin{aligned} \alpha_n &= \tfrac{P_n+\sqrt{d}}{Q_n} && \text{for } n \geq 0 \\ a_n &= \lfloor \alpha_n \rfloor && \text{for } n \geq 0 \\ P_{n+1} &= a_n Q_n - P_n && \text{for } n \geq 0 \\ Q_{n+1} &= \tfrac{d-P_{n+1}^2}{Q_n} && \text{for } n \geq 0 \end{aligned}$$

Then $\alpha = [a_0, a_1, a_2, ...]$.

Definition 4.34. Let $\alpha = \frac{a+\sqrt{d}}{c}$ be an irrational quadratic number. The conjugate of α, denoted $\overline{\alpha}$, is defined to be $\overline{\alpha} = \frac{a-\sqrt{d}}{c}$.

Note that this is not the same as complex conjugation. α is the root of a quadratic polynomial. $\overline{\alpha}$ is the other root.

Lemma 4.35. Let α_1, α_2 be two quadratic irrationals. Then the following hold:

1. $\overline{\alpha_1 \pm \alpha_2} = \overline{\alpha_1} \pm \overline{\alpha_2}$
2. $\overline{\alpha_1 \times \alpha_2} = \overline{\alpha_1} \times \overline{\alpha_2}$
3. $\overline{(\frac{\alpha_1}{\alpha_2})} = \frac{(\overline{\alpha_1})}{(\overline{\alpha_2})}$
4. $\overline{r\alpha_1} = r\overline{\alpha_1}$ for $r \in \mathbb{Q}$

Theorem 4.36. Let α be a quadratic irrational. When written as an infinite simple continued fraction, α is eventually periodic.

Example 4.37. Let $\alpha = \sqrt{7} = \frac{0+\sqrt{7}}{1}$. It's already in the desired form since $1 \mid 7 - 0^2$. Using the rules $\alpha_n = \frac{P_n+\sqrt{d}}{Q_n}$, $a_n = \lfloor \alpha_n \rfloor$, $P_{n+1} = a_n Q_n - P_n$, and $Q_{n+1} = \frac{d-P_{n+1}^2}{Q_n}$. We can obtain the following table

i	P_i	Q_i	α_i	a_i
0	0	1	$\frac{0+\sqrt{7}}{1}$	2
1	2	3	$\frac{2+\sqrt{7}}{3}$	1
2	1	2	$\frac{1+\sqrt{7}}{2}$	1
3	1	3	$\frac{1+\sqrt{7}}{3}$	1
4	2	1	$\frac{2+\sqrt{7}}{1}$	4
5	2	3	can stop here	

Everything repeats from here. So, we have that

$$\alpha = [2, 1, 1, 1, 4, 1, 1, 1, 4, \cdots] = [2, \overline{1, 1, 1, 4}]$$

We can also discard the use of P_i and Q_i.

Example 4.38. Let $\alpha = \frac{7+\sqrt{6}}{2}$. Write α as an eventually periodic continued fraction. We use the rules $a_n = \lfloor \alpha_n \rfloor$ and $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$ with $\alpha_0 = \alpha$. We can obtain the following table

i	α_i	a_i
0	$\frac{7+2\sqrt{6}}{2}$	4
1	$\frac{2+2\sqrt{6}}{5}$	1
2	$\frac{3+2\sqrt{6}}{3}$	2
3	$\frac{3+2\sqrt{6}}{5}$	1
4	$\frac{1+\sqrt{6}}{2}$	1
5	$\frac{2+2\sqrt{6}}{2}$	can stop here

We conclude that $\alpha = [4, \overline{1, 2, 1, 1}]$. We know the process has to repeat, but no idea how long this takes. (Know the period can be at most $\approx (2\sqrt{d}) \times d = 2d^{3/2}$, but no idea when the period starts)

Example 4.39. Let $\alpha = [1, 2, 3, 4, \overline{1, 2, 1, 3, 2}]$. Write α in the form $\frac{A+\sqrt{d}}{B}$ with A, B, d integers.

To do this, we let $\beta = [\overline{1, 2, 1, 3, 2}]$. Then $\beta = [1, 2, 1, 3, 2, \beta]$.

For the continued fraction $[1, 2, 1, 3, 2]$, we obtain $p_0 = 1, p_1 = 3, p_2 = 4, p_3 = 15, p_4 = 34, q_0 = 1, q_1 = 2, q_2 = 3, q_3 = 11, q_4 = 25$. From here, we obtain that $\beta = \frac{34\beta+15}{25\beta+11}$. Solving for $\beta = \frac{23+\sqrt{2029}}{50}$

So, $\alpha = [1, 2, 3, 4, \beta]$. Similar to before, we obtain that $\alpha = \frac{43\beta+10}{30\beta+7}$. Simplifying this gives that $\alpha = \frac{21377-\sqrt{2029}}{14890}$

4.9 Periodic Continued Fractions

Theorem 4.40. Let α be a quadratic irrational. Then the CF expression of α is periodic if and only if $\alpha > 1$ and $-1 < \overline{\alpha} < 0$. Such numbers are called **reduced**.

4.10 Continued Fraction of $\sqrt{d}$

Let $d \in \mathbb{N}$ not be a perfect square. What can we say about the continued fraction expression of $\sqrt{d}$? Here are some examples:

$$\begin{aligned}\sqrt{2} &= [1, \overline{2}]\\ \sqrt{28} &= [5, \overline{3, 2, 3, 10}]\\ \sqrt{61} &= [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]\\ \sqrt{73} &= [8, \overline{1, 1, 5, 5, 1, 1, 16}]\\ \sqrt{87} &= [9, \overline{3, 18}]\end{aligned}$$

We may notice that:

- The periodic part of the CF expression begins after the first terms
- The final term in the periodic part is twice the initial term a_0
- Palindrome

Theorem 4.41. Let $d \in \mathbb{N}$ with d not a perfect square. Let $\alpha = \sqrt{d}$. When α is written as a continued fraction, it takes the form $[a_0, \overline{a_1, ..., a_{\tau-1}, 2a_0}]$

Example 4.42. Let $n \in \mathbb{N}$. Let $\alpha = \sqrt{n^2+2}$. Write α as a continued fraction. Let's use the rules $\alpha_n = \frac{P_n+\sqrt{d}}{Q_n}, a_n = \lfloor \alpha_n \rfloor, P_{n+1} = a_n Q_n - P_n, Q_{n+1} = \frac{d-P_{n+1}^2}{Q_n}$. We can obtain the following table

i	P_i	Q_i	α_i	a_i
0	0	1	$\frac{0+\sqrt{n^2+2}}{1}$	n
1	n	$\frac{n^2+2-n^2}{1} = 2$	$\frac{n+\sqrt{n^2+2}}{2}$	n
2	$2n - n = n$	$\frac{n^2+2-n^2}{2} = 1$	$\frac{n+\sqrt{n^2+2}}{1}$	$2n$
3	n	2	$\frac{n+\sqrt{n^2+2}}{2}$	n

From which we obtain $\sqrt{n^2+2} = [n, \overline{n, 2n}]$

4.11 Pell's Equations

Definition 4.43. For fixed $d, n \in \mathbb{Z}$, **Pell's Equation** is the Diophantine Equation

$$x^2 - dy^2 = n$$

We are going to focus on the case $x^2 - dy^2 = 1$ where d is positive and square-free (i.e. not a perfect square). Note that:

1. if $d < 0, n < 0$, then $x^2 - dy^2 = n$ has no solution
2. if $d < 0, n > 0$, then $x^2 - dy^2 = n$ has finitely many solutions
3. in other words, the equation is most interesting when $d > 0$
4. if $d > 0$ is a square, then the equation has finitely many solution.

Theorem 4.44. Let $d \in \mathbb{N}$, not a perfect square, and let $n \in \mathbb{N}$ such that $0 < n < \sqrt{d}$. If (a, b) is a positive solution (i.e. $a > 0, b > 0$) of $x^2 - dy^2 = n$, then $\frac{a}{b}$ is a convergent of $\sqrt{d}$.

Actually, this result is still true if $n \in \mathbb{Z}$ and $0 < |n| < \sqrt{d}$.

Lemma 4.45. Let $d \in \mathbb{N}$ not be a square. Let $\alpha = \sqrt{d}$. Let $\frac{p_i}{q_i}$ be a convergent of α. Then

$$p_i^2 - dq_i^2 = (-1)^{i+1} Q_{i+1}$$

Lemma 4.46. Let P_i, Q_i, α_i, a_i be generated from $\sqrt{d}$, and let $P_i', Q_i', \alpha_i', a_i'$ be generated from $\lfloor \sqrt{d} \rfloor + \sqrt{d}$. Then, $P_i = P_i', Q_i = Q_i', \alpha_i = \alpha_i'$, and $a_i = a_i'$ for all $i \geq 1$. Furthermore, $Q_0 = Q_0'$

Lemma 4.47. Let d be a positive integer, not a square. Let τ be the period when $\alpha = \sqrt{d} = \frac{0+\sqrt{d}}{1}$ is written as an (eventually periodic) infinited simple continued fraction. Then:

1. For all $n \geq 0$, we have that $Q_n = 1$ if and only if $\tau \mid n$
2. For all $n \geq 0$, $Q_n \neq -1$

Theorem 4.48. Let $d \in \mathbb{N}$ with d not a perfect square. Let $\frac{p_i}{q_i}$ be the convergents of $\sqrt{d}$. Let τ be the period when $\sqrt{d}$ is written as an (eventually periodic) infinited simple continued fraction. Consider the equation $x^2 - dy^2 = 1$:

1. If τ is even, then the positive solutions are exactly those of the form $(p_{k\tau-1}, q_{k\tau-1})$ with $k \in \mathbb{N}$
2. If τ is odd, then the positive solutions are exactly those of the form $(p_{2k\tau-1}, q_{2k\tau-1})$ with $k \in \mathbb{N}$

Definition 4.49. Let (p, q) be the positive solution to $x^2 - dy^2 = 1$ with p, q as small as possible. This is the **fundamental solution**.

Theorem 4.50. Once we have the fundamental solution, we can find all other solutions as

follows: define $x_1 = p$ and $y_1 = q$. For $n \geq 2$, define (x_n, y_n) by imposing $x_n \in \mathbb{Z}, y_n \in \mathbb{Z}$ and

$$(x_1 + \sqrt{d}y_1)^n = x_n + y_n\sqrt{d}$$

The positive solutions to $x^2 - dy^2 = 1$ are exactly the pairs (x_n, y_n) with $n \in \mathbb{N}$

Chapter 5 Some Random Stuff

5.1 Pythagorean Triples

Definition 5.1. A **Pythagorean triple** is a triplet of positive integers (a, b, c) such that $a^2 + b^2 = c^2$

Example 5.2. $(3, 4, 5), (5, 12, 13), (6, 8, 10)$ are all Pythagorean triples. $(-3, 4, 5), (0, 4, 4)$ are not Pythagorean triples.

We are interested in describing all Pythagorean triples such that a, b, c have no shared common factor. Such triples are called **primitive**.

We are interested in integer solutions to the equation $X^2 + Y^2 = Z^2$. Except for the only solution with $Z = 0$, this is equivalent to looking for **rational** solutions to the equation $x^2 + y^2 = 1$ (Divide the original equation by Z^2, and define $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$). This is the equation of a unit circle in $\mathbb{R}^2$ centered at the origin.

So, the equation is how do we describe all rational points on the unit circle? We can use geometry. Fix a point $P = (-1, 0)$ on the circle. Consider the line through P with slope λ. Let Q_λ be the other intersection point of the line with the circle.

Proposition 5.3. If $\lambda \in \mathbb{Q}$, then $Q_\lambda \in \mathbb{Q}^2$

The equation of L_λ is $y = \lambda(x+1)$. To solve for Q_λ, we should solve $x^2 + \lambda^2(x+1)^2 = 1$. Expanding it gives us the quadratic equation

$$(1 + \lambda^2)x^2 + 2\lambda^2 x + (\lambda^2 - 1) = 0$$

To see the proposition is true, we can look at:

- The sum of the roots is $\frac{-2\lambda^2}{1+\lambda^2}$, which is rational. Since one root is rational, so is the other.
- Use the quadratic formula to obtain $x = \frac{-\lambda^2 \pm 1}{\lambda^2 + 1}$. We obtain $x = -1$ with the minus sign, and therefore $x_\lambda = \frac{1-\lambda^2}{1+\lambda^2}$ and $y_\lambda = \lambda(x_\lambda + 1) = \frac{2\lambda}{1+\lambda^2}$. From this we see that if $\lambda \in \mathbb{Q}$, then $Q_\lambda = (x_\lambda, y_\lambda) \in \mathbb{Q}^2$.

This "process" hits every rational point other than P: suppose R is a rational point distinct from P. Then the line through R and P has rational slope. Call this slope τ: then $R = Q_\tau$

Remark: To obtain R for $Q_\lambda = (\frac{1-\lambda^2}{1+\lambda^2}, \frac{2\lambda}{1+\lambda^2}) \in \mathbb{Q}^2$, we must substitute ∞ for λ.

For $\lambda \in \mathbb{Q}$, we have $Q_\lambda = (\frac{1-\lambda^2}{1+\lambda^2}, \frac{2\lambda}{1+\lambda^2})$. Now let $\lambda = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$.

Recall that we made the substitutions $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. Thus, we should write each term for Q_λ as a ratio of two integers. Doing this gives us

$$Q_\lambda = (\frac{b^2-a^2}{b^2+a^2}, \frac{2ba}{b^2+a^2})$$

Lemma 5.4. Let $a, b \in \mathbb{N}$. Then $\gcd(b^2-a^2, b^2+a^2) = 1 = \gcd(2ba, b^2+a^2)$ if and only if $\gcd(a,b) = 1$ and a, b are not both odd.

Theorem 5.5. The primitive Pythagorean Triples are exactly those numbers of the form $(b^2-a^2, 2ab, b^2+a^2)$ with $a, b \in \mathbb{N}, a < b, \gcd(a,b) = 1$, and a, b not both odd.

The circle $x^2 + y^2 = 1$ was a quadratic curve. What about the cubic curve $y^2 = x^3 + x$?

- In general, a line intersects the curve at 3 points (with proper counting, i.e. with consideration of a point at infinity)
- If P is rational, there is no reason that R or Q have to be rational.
- In fact, it is impossible to parameterize the rational points using a ratio of polynomials.
- However, if P and Q are both rational, then so is R. This gives rise to a group structure on the set of rational points.
- Studying the rational points on cubic curves is one of the main areas of research of modernmathematics. Another name for cubic curves is elliptic curves

5.2 $n = 4$ case of FLT

Theorem 5.6. Fermat's Last Theorem (Stated in 1630's, Proved in 1990's): Let $n \geq 3$. The equation $x^n + y^n = z^n$ has no positive integer solutions.

It suffices to prove it for the case $n = 4$ and for n being an odd prime. Much of number theory done during the 1700's and 1800's was in the effort to make progress towards proving this. Trying to prove FLT fell out of style in the 1900's. In the 1980's, it was shown that FLT was a corollary of a major open problem.

Theorem 5.7. $x^4 + y^4 = z^4$ has no positive integer solutions.

Remark: if (a, b, c) is a solution to $x^4+y^4 = z^4$, then (a, b, c^2) is a solution to $x^4+y^4 = z^2$. The contrapositive of this is that: if $x^4+y^4 = z^2$ has no positive integer solution, then neither does $x^4 + y^4 = z^4$.

5.3 Which Numbers are a Sum of Two Squares?

Proposition 5.8. Let $a, b \in \mathbb{N}$. If a, b are each a sum of two squares, then so is ab.

With this result, we can consider turn question into considering whether or not a given prime number is a sum of two squares. Trivially, 2 is, so we can focus on odd primes.

Theorem 5.9. (**Euler**): Let p be an odd prime. Then p may be written as a sum of two squares if and only if $p \equiv 1 \mod 4$.

Definition 5.10. The **Gaussian Integers**, denoted $\mathbb{Z}[i]$ is the set of all complex numbers whose real and imaginary parts are integers. That is,

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

A member of $\mathbb{Z}[i]$ is called a **Gaussian integer**.

Notice that $\mathbb{Z}[i]$ is closed under addition and multiplication. $\mathbb{Z}[i]$ is an example of a **ring**. Let $z \in \mathbb{Z}[i]$, we say that z is

- a **unit** if there exists $w \in \mathbb{Z}[i]$ such that $zw = 1$
- **reducible** (composite) if there exists $x, y \in \mathbb{Z}[i]$, neither a unit, such that $z = xy$
- **irreducible** (prime) if it is non-zero and not reducible.
- **zero** if $z = 0$

Definition 5.11. Let $w = a + bi$ with $a, b \in \mathbb{Z}$. The **norm** of w, written $N(w)$ is defined to be $a^2 + b^2 = |a + ib|^2$.

Proposition 5.12. Let $z, w \in \mathbb{Z}[i]$. Then

- $N(z) \in \mathbb{Z}$ and $N(z) \geq 0$
- $N(zw) = N(z)N(w)$
- $N(z) = 1$ if and only if z is a unit.

Proposition 5.13. Let $z, w \in \mathbb{Z}[i]$ with $z \neq 0$. There exists $q, r \in \mathbb{Z}[i]$ so that $w = qz + r$ and $N(r) < N(z)$.

Definition 5.14. Given $a, b \in \mathbb{Z}[i]$, we say that $a \mid b$ if there exists $c \in \mathbb{Z}[i]$ so that $ac = b$.

We could define gcd's in $\mathbb{Z}[i]$ (they are not unique, but they are unique up to a unit). Here is the $\mathbb{Z}[i]$'s analogue of Bezout's Lemma:

Theorem 5.15. Let $a, b \in \mathbb{Z}[i]$, not both 0. Let d be a Gaussian integer combination of a, b such that $N(d)$ is as small as possible while still being positive. Then d divides every Gaussian integer combination of a, b.

Theorem 5.16. Let $p, w, z \in \mathbb{Z}[i]$ with p irreducible. If $p \mid wz$, then $p \mid w$ or $p \mid z$.

Theorem 5.17. Let p be a prime such that $p \equiv 1 \mod 4$. Then p may be written as a sum of two squares.

It seems that lose uniqueness when we go into the land of $\mathbb{Z}[i]$. This is because we are used to working in $\mathbb{N}$. If we instead worked in $\mathbb{Z}$, we would also lose uniqueness since there are two units in $\mathbb{Z}(1, -1)$. The problem here is that there is no good analogue $X \subseteq \mathbb{Z}[i]$ of $N \subseteq Z$.

$\mathbb{Z}[i]$ has an analogue of unique factorization. It seems natural to ask questions about $\mathbb{Z}[\sqrt{d}]$. Studying things like the Division Algorithm and Unique Factorization in things like $\mathbb{Z}[i]$ is the begining of **Algebraic Number Theory**.

While $\mathbb{Z}[\sqrt{-1}]$ has only 4 units, if d is positive and square-free, then $\mathbb{Z}[\sqrt{d}]$ has infinitedly many units. This is related to Pell's equation.

Asking which numbers can be written in the form $a^2 + 5b^2$ might lead you to consider properties of $\mathbb{Z}[\sqrt{-5}]$. The ring $\mathbb{Z}[\sqrt{-5}]$ does not have a division algorithm, and hence does not have Euclid's Lemma (or any analogue of Unique Factorization). A weird identity in this ring is $2 \times 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

A celebrated achievedment of the 1950s, conjectured by Gauss: let $d < 0$, then $\mathbb{Z}[\sqrt{d}]$ has unique factorization if and only if

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$$

This is known as the **Stark Heegner Theorem**.

A famous identity, found in the 1850's, is

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999923...$$

That is, $e^{\pi\sqrt{163}}$ is really close to an integer. This is related to the previous point.