Number Theory

Jim Brown
(Notes by Shuai Wei)

September 17, 2023

Contents

Chapter 1

Open Problems

Many problems are easy to state but hard to prove.

(a) Given $n \in \mathbb{Z}_{\geqslant 2}$, is it always true that there exists $x, y, z \in \mathbb{N}$ such that $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$? Vaughan proved the number of $n \leqslant N$ for which the above equality is insolvable is $O\big(N \cdot \exp(-c(\log N)^{\frac{2}{3}})\big)$ for some positive constant c.

(b) Modern: Twin Primes. There are infinitely many pairs of primes (p, p') such that $p - p' = 2$. Zhang proved there are infinitely many pairs of prime numbers that differ by 70 million or less, i.e., $\lim_{n\to\infty} \inf(p_{n+1} - p_n) < N = 7 \times 10^7$, where p_n is the n^{th} prime. James Maynard prove it holds for $N = 252$. According to the Polymath project wiki, $N = 246$. Assume another conjecture, $N = 6$.

(c) Fermat's Last Theorem: $x^n + y^n = z^n$ has no positive interger solutions (x, y, z) for $n \in \mathbb{Z}_{>2}$. Almost all of modern algebra came from people trying to prove Fermat's Last Theorem. Fermat's Last Theorem is a corollary to a theorem that every ellipic curve is a modular form.

(d) Is it true the equation $x^n + y^n = z^n + w$ with $n \geqslant 5$?

Remark. All of these can be formulated as looking for solutions to equations $f(x_1, \ldots, x_n) = 0$ for $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and solutions in R^n for some integrating set R. These are called Diophantine equation-all the complicated machinery today was developed to solve them.

Chapter 2

Introduction

Convention 2.1. Assume all varaibles in this book are integers.

2.1 Prerequisites

Definition 2.2. (a) Assume $a \neq 0$. We say a *divides* b and write $a \mid b$ if there exists $c \in \mathbb{Z}$ such that $ac = b$.

(b) Assume $a \neq 0$ and $k \geqslant 0$. Write $a^k \mid\mid b$ "*exactly divides*" if $a^k \mid b$ but $a^{k+1} \nmid b$.

Fact 2.3. We have the following facts.

(a) $a \mid a$ for any $a \neq 0$.

(b) $a \mid 0$, for any $a \neq 0$.

(c) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(d) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.

(e) If $a \mid b$ and $b \mid a$, then $a = b$.

(f) If $a \mid b$ and $a > 0$ and $b > 0$, then $a \leqslant b$.

(g) If $m \neq 0$, then $ma \mid mb$.

Theorem 2.4 (Division Algorithm)**.** *Assume $a \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that $b = aq+r$ and $0 \leqslant r < a$. In particular, if $a \nmid b$, then $0 < r < a$.*

Proof. Let $q_0 = \arg\max_{q\in\mathbb{Z}}\{aq \mid aq \leqslant b\}$. Then $a(q_0 + 1) > b$, i.e., $a > b - aq_0$. Let $r_0 := b - aq_0$. Then $b = aq_0 + r_0$ with $0 \leqslant r_0 < a$. Suppose there exist another $r_1, q_1 \in \mathbb{Z}$ such that $b = aq_1 + r_1$ and $0 \leqslant r_1 < a$. Then $aq_0 + r_0 = aq_1 + r_1$, i.e., $a \mid (r_1 - r_0)$. Since $-a < r_1 - r_0 < a$, $r_1 = r_0$. Also, since $a \neq 0$, $q_0 = q_1$. □

Definition 2.5. Let $a \neq 0$.

(a) If $a \mid b$ and $a \mid c$, we say a is a *common divisor* of b and c.

(b) The largest common positive divisor of b and c is called the *greatest common divisor* of b and c, denoted by (b, c) or $\gcd(b, c)$.

(c) Analogously define $\gcd(b_1, \ldots, b_n)$.

Theorem 2.6.

$$\gcd(b, c) = \min\{bx + cy > 0 \mid x, y \in \mathbb{Z}\}.$$

Proof. Let $D = \{bu + cv > 0 \mid u, v \in \mathbb{Z}\}$, . Then $D \neq \emptyset$. Let $d := bx + cy$ for some $x, y \in \mathbb{Z}$ such that $d = \min D$. Suppose $d \nmid b$. Since $d > 0$, we can write $b = dq + r$ with $0 < r < d$. Then $r = b - dq = b - (bx + cy)q = b(1 - qx) + c(-yq) \in D$, contradicted by $0 < r < d = \min D$. So $d \mid b$. Similarly, $d \mid c$. Hence $d \leqslant g = \gcd(b, c)$. Note $gB = b$ and $gC = c$ for some $B, C \in \mathbb{Z}$. Then $d = (gB)x + (gC)y = g(Bx + Cy)$. So $g \mid d$. Since $g, d > 0$, we have $g \leqslant d$ and then $g = d$. $\square$

Corollary 2.7. If $am + bn = 1$, then

$$\gcd(a, b) = \gcd(a, n) = \gcd(m, b) = \gcd(m, n) = 1.$$

Theorem 2.8. *Let $m \in \mathbb{N}$, then $\gcd(mb, mc) = m \gcd(b, c)$.*

Proof. Let $d = \gcd(b, c)$. Then $d \mid b$ and $d \mid c$. Since $m \neq 0$, $md \mid mb$ and $md \mid mc$. So $\gcd(mb, mc) \geqslant md$. Suppose there exists $D > md$ such that $D \mid mb$ and $D \mid mc$. Then $D = mx$ for some $x \in \mathbb{N}$. Then $x \mid b$ and $x \mid c$. So $x \leqslant \gcd(b, c) = d$. Also, $D = mx > md$, i.e., $x > d$, a contradiction. $\square$

Corollary 2.9. If $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{\gcd(a,b)}{d}$ and so $d \mid \gcd(a, b)$.

Proof. $\gcd(a, b) = \gcd\left(d\left(\frac{a}{d}\right), d\left(\frac{b}{d}\right)\right) = d \cdot \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$. $\square$

Theorem 2.10. *If $\gcd(a, m) = 1 = \gcd(b, m)$, then $\gcd(ab, m) = 1$.*

Proof. There exist x_1, x_2 and $y_1, y_2 \in \mathbb{Z}$ such that $ax_1 + my_1 = 1$ and $bx_1 + my_2 = 1$. Then $ax_1 = 1 - my_1$, $bx_1 = 1 - my_2$ and $abx_1x_2 = 1 - my_1 - my_2 + m^2y_1y_2$, i.e., $abx_1x_2 + m(y_1 + y_2 - my_1y_2) = 1$. By Corollary 2.7, $\gcd(ab, m) = 1$. $\square$

Fact 2.11.

$$\gcd(a, b) = \gcd(b, a) = \gcd(-a, b) = \gcd(a, b + ax).$$

Theorem 2.12. *If $c \mid ab$ and $\gcd(b, c) = 1$, then $c \mid a$.*

Proof. Since there exist m, n such that $1 = bm + cn$, we have $a = abm + acn$. Since $c \mid ab$ and $c \mid ac$, we have $c \mid a$. $\square$

Theorem 2.13 (Euclidean Algorithm)**.** *Let $c \in \mathbb{N}$. Repeat applying the division algorithm, write*

$$\begin{aligned}
b &= cq_1 + r_1, 0 \leqslant r_1 < c, \\
c &= r_1q_2 + r_2, 0 \leqslant r_2 < r_1, \\
r_1 &= r_2q_3 + r_3, 0 \leqslant r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, 0 \leqslant r_n < r_{n-1}, \\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Then $r_n = \gcd(b, c)$.

Proof.

$$\begin{aligned}\gcd(b,c) &= \gcd(b-cq_1,c) = \gcd(r_1,c) = \gcd(r_1,c-r_1q_2) = \gcd(r_1,r_2)\\ &= \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n.\end{aligned}$$

□

Remark. This allows us to solve the linear Diophantine equation $bx + cy = \gcd(b,c) = r_n$, i.e.,

$$r_n = r_{n-2} - r_{n-1}q_n = (r_{n-4} - r_{n-3}q_{n-2})q_{n-1} - (r_{n-3} - r_{n-2}q_{n-1})q_n,$$

i.e., continue to let $r_j = r_{j-2} - q_jr_{j-1}$ for $j = n, \ldots, 3$ and $r_2 = c - r_1q_2$ and $r_1 = b - cq_1$.

Definition 2.14. (a) We say $b \in \mathbb{Z}$ is a *common multiple* of $a_1, \cdots, a_n$ if $a_i \mid b$ for $i = 1, \cdots, n$.

(b) The *least common multiple* is the smallest positive common multiples. Denote this by

$$[a_1, \ldots, a_n] = \mathrm{lcm}(a_1, \ldots, a_n).$$

Fact 2.15.

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

Definition 2.16. Let $n \in \mathbb{N}$. We say that a is *congruent* to b modulo n, and write $a \equiv b \pmod{n}$, when $m \mid (a-b)$. We say that a is *not congruent* to b modulo n, and write $a \not\equiv b \pmod{m}$, when $m \nmid (a-b)$.

Remark. $\equiv$ is an equivalence relation.

Theorem 2.17. *Let $n \in \mathbb{N}$. Then $ca \equiv cb \pmod{n}$ if and only if $a \equiv b \pmod{\frac{n}{\gcd(c,n)}}$. In particular, if $ca \equiv cb \pmod{n}$ and $\gcd(c,n) = 1$, then $a \equiv b \pmod{n}$.*

Proof. $\Longrightarrow$ Note there exists k such that $c(a-b) = nk$. Also ther exist $r, s \in \mathbb{Z}$ with $\gcd(r,s) = 1$ so that $n = dr$ and $c = ds$. Then $drk = nk = c(a-b) = ds(a-b)$, i.e., $rk = s(a-b)$. Since $\gcd(r,s) = 1$, $r \mid (a-b)$. So $(n/d) \mid a - b$.

$\Longleftarrow$ Since $c \cdot \frac{n}{\gcd(c,n)} = \mathrm{lcm}(c,n) \in \mathbb{N}$, $ca \equiv cb \pmod{\mathrm{lcm}(c,n)}$. So $ca \equiv cb \pmod{n}$. □

Theorem 2.18. *Let $n \in \mathbb{N}$. Then there exists x such that $ax \equiv 1 \pmod{n}$ if and only if $\gcd(a,n) = 1$. If x_1 and x_2 are any two such integers, then $x_1 \equiv x_2 \pmod{n}$.*

Proof. $\Longrightarrow$ Suppose $\gcd(a,n) > 1$, then $(ax,n) > 1$ for any x. But if one were to have $ax \equiv 1 \pmod{n}$, then write $ax = 1 + nq$ for some q, so $\gcd(ax,n) = \gcd(1+nq,n) = \gcd(1,n) = 1$, a contradiction.

$\Longleftarrow$ By Theorem 2.6. □

Definition 2.19. Let $n \in \mathbb{N}$.

(a) If $x \equiv y \pmod{n}$, then y is called a *residue* of x modulo n.

(b) We say that $\{x_1, \cdots, x_n\}$ is a *complete residue system* modulo n if for each y, there exists a unique x_i with $y \equiv x_i \pmod{m}$.

(c) The set of x with $x \equiv a \pmod{m}$ is called the *residue class*, or *congruence class*m of a modulo m.

Definition 2.20. We say $p \geqslant 2$ is *prime* if whenever $p \mid ab$, then $p \mid a$ or $p \mid b$.

Remark. Since $\mathbb{Z}$ is a Unique Factorization Domain, It is equivalent to say p is prime if the only divisors of p is ± 1 and $\pm p$.

Lemma 2.21. Every $n \geqslant 2$ is a product of prime.

Proof. Proof by induction. Base case: 2 is straightforward. Inductive step: Assume every integer $2 < n < N$ is a product of prime. If N is a prime, then we are done. If N is not a prime, then it has a proper divisor d, write $N = dn,\ 1 < d, n < N$. Apply inductive hypothesis to d and n, so they have prime factorization. Hence N has a prime factorization. This gives the result. □

Definition 2.22. Let $n \in \mathbb{Z} \smallsetminus \{\pm 1, 0\}$, write $n = (\pm 1)\prod_{i=1}^{m} p_i^{e_i}$, with $p_1 < \cdots < p_m$ primes and $e_1, \ldots, e_m \in \mathbb{N}$. This is the *canonical factorization* of n.

Theorem 2.23 (Fundamental Theorem of Arithemetic)**.** *The canonical factorization of $n \in \mathbb{Z}^{\geqslant 2}$ is unique.*

Proof. Proof by induction. Suppose we have a unique factorization for all integer $2 \leqslant n \leqslant N$. Suppose we have two canonical factorizations $N + 1 = \prod_{i=1}^{m} p_i^{e_i} = \prod_{j=1}^{k} q_i^{f_i}$. Since p_1 is prime and $p_1 \mid \prod_{j=1}^{k} q_j^{f_j}$, $p_1 \mid q_j$ for some $j \in \{1, \ldots, k\}$. Since p_1 and q_j are primes, we have $p_1 = q_j$. Then $p_1^{e_1 - 1}\prod_{i=2}^{m} p_i^{e_i} = q_j^{f_j - 1}\prod_{i=1, i\neq j}^{k} q_i^{f_i} \leqslant N$. Now apply the inductive hypothesis. □

Theorem 2.24 (Euclid)**.** *There are infinitely many primes.*

Proof. Assume there are only finitely many primes, say $p_1, \ldots, p_n$. Set $N = p_1 \cdots p_n + 1$. Since $N > 1$, N has prime factorization and then there exists a prime p such that $p \mid N$. Then $p = p_j$ for some $j \in \{1, \ldots, n\}$ and $p \mid (p_1 \cdots p_n)$. So $p \mid (N - p_1 \cdots p_n)$, i.e., $p \mid 1$, a contradiction. □

Theorem 2.25. *Let p_n be the n^{th} prime. Then $p_n < 2^{2^n}$.*

Proof. Proof by induction. Base case: $p_1 = 2 < 2^{2^1}$. Suppose this is true for all $n \leqslant N$. Since $p_i \nmid (p_1 \cdots p_N + 1)$ for $i = 1, \ldots, N$, we have $p_{N+j} \mid (p_1 \cdots p_N + 1)$ for some $j \geqslant 1$. So

$$\begin{aligned} p_{N+1} \leqslant p_{N+j} \leqslant p_1 \cdots p_N + 1 &< 2^{2^1} \cdots 2^{2^N} + 1 = 2^{\sum_{j=1}^{N} 2^j} + 1 = 2^{2\left(2^N - 1\right)} + 1 \\ &= 2^{2^{N+1} - 2} + 1 < 2^{2^{N+1} - 2} + 2^{2^{N+1} - 2} = 2^{2^{N+1} - 1} < 2^{2^{N+1}}. \end{aligned}$$ □

Definition 2.26. Let $x \in \mathbb{R}_{\geqslant 0}$. Define

$$\pi(x) = \#\{p \text{ prime} \mid p \leqslant x\}.$$

Theorem 2.27 (Prime Number Theorem)**.**

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

Proof. By Hadamard and de la Valle. □

Remark. Since it is asymptotic result, the log base can be any number that is greater than 1.

Corollary 2.28. $\pi(x) > \log(\log x)$, where the log base can be any $2 < \alpha < 4$.

Proof. Let $x \geqslant 2$. Choose n such that $2^{2^n} \leqslant x < 2^{2^{n+1}}$. Then by theorem 2.25, we have $\pi(x) \geqslant n$. Since our log is an increasing function, $\log x < \log 2^{2^{n+1}} = 2^{n+1} \log 2 = 2^n \log 4 < 2^n$. So $\log(\log x) < n \log 2 < n \leqslant \pi(x)$. □

Theorem 2.29. *There are arbitrary large gaps between consecutive primes.*

Proof. Let n be the gap size and consider the sequence $n! + 2, \dots, n! + n$. Since the i^{th} number in the sequence is divisible by $i + 1$ for $i = 1, \dots, n - 1$, we have a sequence of $n - 1$ consecutive composite numbers. So as $n \to \infty$, the gap between consecutive primes get arbitrary large. □

Lemma 2.30. If p is odd prime, then $p \equiv \pm 1 \pmod 4$, i.e., $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

Fact 2.31. If $p_1, p_2 \equiv 1 \pmod 4$, then $p_1 p_2 \equiv 1 \pmod 4$.

Theorem 2.32 (Euclid)**.** *There are infinitely many primes of the form* $4k + 3$.

Proof. Assume $p_1, \dots, p_n$ are all the prime of the form $p \equiv 3 \pmod 4$. Set $N = 4p_1 \cdots p_n - 1$. Then $N \equiv 3 \pmod 4$ and $p_i \nmid N$ for $i = 1, \dots, n$. So there must be a prime other than $p_1, \dots, p_n$ dividing N. Since N is odd, $2 \nmid N$. Suppose $N = q_1^{e_1} \cdots q_r^{e_r}$ for some $e_1, \cdots, e_r \in \mathbb{N}$ and primes $q_1, \cdots, q_r \equiv 1 \pmod 4$. By Fact 2.31, we have N has the form $N \equiv 1 \pmod 4$, a contradiction. Hence, N has at least one prime factor p of the form $4k + 3$. Since $p_i \nmid N$ for $i = 1, \dots, n$, we have $p \neq p_i$ for $i = 1, \dots, n$, a contradiction. □

Lemma 2.33 (Dirichet's theorem)**.** Let $\gcd(a, b) = 1$, then there are infinitely many primes of the form $ak + b$ for $k \in \mathbb{N}$.

Lemma 2.34. There exists $n \geqslant 1$ and $f \in \mathbb{Z}[x_1, \dots, x_n]$ whose positive values are precisely the prime numbers.

(a) Matijasevic proved the smallest n is 10, the polynomial degree $d \sim 1.6 \times 10^{45}$.

(b) JSW proved the smallest degree is 5 and the number of variables is 42.

Theorem 2.35. *If* $f \in \mathbb{Z}[t]$ *with* $\deg(f) > 1$*, then* f *cannot take just prime values for* $t \in \mathbb{Z}$.

Proof. Suppose $f(t) := a_k t^k + \cdots + a_1 t + a_0$ is such a polynomial. Let $n_0 \in \mathbb{Z}$ and p be prime such that $f(n_0) = p$. Let $s \in \mathbb{Z}$. Then there exists $Q \in \mathbb{Z}[t]$ such that

$$f(n_0 + sp) = a_k (n_0 + sp)^k + \cdots + a_1 (n_0 + sp) + a_0 = f(n_0) + pQ(s) = p + pQ(s) = p\left(1 + Q(s)\right).$$

So $p \mid f(n_0 + sp)$. By assumption, $f(n_0 + sp)$ is prime. So $f(n_0 + sp) = p$ for $s \in \mathbb{Z}$, i.e., $f(n_0 + sp) - p = 0$ for $s \in \mathbb{Z}$, contradicted by $\deg(f - p) = k$. □

2.2 Pythagorean Triple

Theorem 2.36 (Pythagorean theorem)**.** *We want all integer solution to the equation* $x^2 + y^2 = z^2$. *If* (a, b, c) *is a solution and* $(a, b, c) = 1$*, we say* (a, b, c) *is a primitive pythagorean triple.*

Proof. We only work with primitive solution. Note that $a^2, b^2, c^2 \equiv 0, 1 \pmod 4$. So c must be even. Without loss of generality, assume a is even and b odd . Then $b^2 = c^2 - a^2 = (c-a)(c+a)$. Claim. $\gcd(c-a, c+a) = 1$. Since $c - a$ is odd,

$$\gcd(c-a, c+a) = \gcd\left(c-a, c+a-(c-a)\right) = \gcd(c-a, 2a) = \gcd(c-a, a) = \gcd(c, a).$$

Suppose there exists prime p such that $p \mid \gcd(c, a)$, then $p \mid a$ and $p \mid c$. Then $p \mid c^2 - a^2 = b^2$ and so $p \mid b$. So $p \mid \gcd(a, b, c) = 1$, a contradiction. Hence $\gcd(c-a, c+a) = \gcd(c, a) = 1$. So there exist $m, n \in \mathbb{Z}$ such that $c + a = m^2$ and $c - a = n^2$. Hence $a = \frac{m^2-n^2}{2}$, $b = mn$ and $c = \frac{m^2+n^2}{2}$. Thus, any odd $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$ satisfying $2 \mid m^2 - n^2$ and $2 \mid m^2 + n^2$ can form a solution (a, b, c) with $a = \frac{m^2-n^2}{2}$, $b = mn$ and $c = \frac{m^2+n^2}{2}$. □

Remark. Since m, n are odd, $r := \frac{m+n}{2} \in \mathbb{Z}$ and $s := \frac{m-n}{2} \in \mathbb{Z}$. Then by Corollary 2.9, $\gcd(r, s) = \frac{1}{2}\gcd(m+n, m-n) = \frac{1}{2}\gcd(2m, 2n) = \gcd(m, n) = 1$. Also, we can show r and s have oppositve parity. Since $\frac{(r+s)^2-(r-s)^2}{2} = 2rs$, $(r+s)(r-s) = r^2 - s^2$ and $\frac{(r+s)^2+(r-s)^2}{2} = r^2 + s^2$, the primitive pythagorean triples are given by $\{r^2 - s^2, 2rs, r^2 + s^2\}$ for r, s coprime of opposite parity.

Example 2.37. Let $m = 1$ and $n = 3$, we have $\{a, b, c\} = \{3, 4, 5\}$.

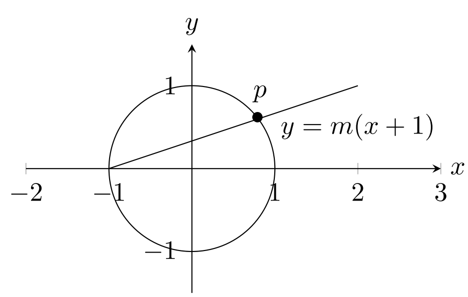
Theorem 2.38. *If $X^4 + Y^4 = Z^2$ for $(X, Y, Z) \in \mathbb{Z}^3$, then $XYZ = 0$.*

Proof. Let (x, y, z) be the solution with $x, y, z \in \mathbb{N}$ and smallest z. Then (x^2, y^2, z) is a primitive pythagorean triple. So there exist r, s coprime of opposite parity such that $x^2 = 2rs$, $y^2 = r^2 - s^2$ and $z = r^2 + s^2$. Then $r \leqslant r^2 < z$ and $s^2 + y^2 = r^2$. Since $(r, s) = 1$, (s, y, r) is a primitive pythagorean triple. Then there are coprime m and n of opposite parity such that $s = 2mn$, $y = m^2 - n^2$, and $r = m^2 + n^2$. So $x^2 = 2rs = 2(m^2 + n^2)(2mn) = 4mn(m^2 + n^2)$. Since m, n and $m^2 + n^2$ are pairwise coprime, there exist $a, b, c \in \mathbb{N}$ such that $m = a^2$, $n = b^2$ and $m^2 + n^2 = c^2$. Then $a^4 + b^4 = c^2$. So (a, b, c) is a solution. But $0 < c \leqslant c^2 = m^2 + n^2 = r < z$, a contradiction. □

Corollary 2.39. If $X^4 + Y^4 = Z^4$ for $(X, Y, Z) \in \mathbb{Z}^3$, then $XYZ = 0$.

2.2.1 Algebraic Methods to Find Pythagorean Triple

Example 2.40. Let (a, b, c) be primitive pythagorean triple $a^2 + b^2 = c^2$. Then $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$, which means $(\frac{a}{c}, \frac{b}{c})$ is a rational points on the unit cycle. To study primitive pythagorean triple, we can parametrize rational points on unit cycle.



Let p be the intersection. Then $p = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$. Let $m = \frac{s}{r}$ with $r \neq 0$. Then $p = \left(\frac{r^2-s^2}{r^2+s^2}, \frac{2rs}{r^2+s^2}\right)$.

Lemma 2.41. For coprime r, s,

$$\gcd(2, r^2+s^2) = \gcd(2rs, r^2+s^2) = \gcd(r^2-s^2, r^2+s^2).$$

Proof. Let $p \mid \gcd(rs, r^2+s^2)$, then $p \mid rs$. Since p is prime, $p \mid r$ or $p \mid s$. Without loss of generality, assume $p \mid r$. Also, since $p \mid r^2+s^2$. $p \mid s^2$. Since p is prime, $p \mid s$, a contradiction. So $\gcd(rs, r^2+s^2) = 1$. Note $\gcd(r^2-s^2, r^2+s^2) = \gcd(2r^2, r^2+s^2) = \gcd(2, r^2+s^2)$. ☐

Definition 2.42. For r, s coprime, define $\delta(r,s) = \gcd(2, r^2+s^2)$. Then

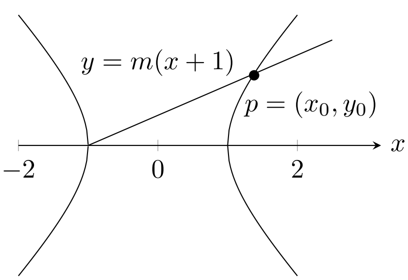
$$\delta(r,s) = \begin{cases} 1, & \text{if } r \not\equiv s \pmod 2 \\ 2, & \text{if } r \equiv s \pmod 2 \end{cases}.$$

Then $(\frac{r^2-s^2}{r^2+s^2}, \frac{2rs}{r^2+s^2}) = \left(\frac{\frac{r^2-s^2}{\delta(r,s)}}{\frac{r^2+s^2}{\delta(r,s)}}, \frac{\frac{2rs}{\delta(r,s)}}{\frac{r^2+s^2}{\delta(r,s)}}\right)$. By Lemma 2.41, this gives the primitive pythagorean triple

$$\{a,b,c\} = \left\{\frac{r^2-s^2}{\delta(r,s)}, \frac{2rs}{\delta(r,s)}, \frac{r^2+s^2}{\delta(r,s)}\right\}.$$

Remark. If we require r and s of opposite parity, then $\delta(r,s) = 1$ and we recover the previous result from our algebra computations.

Example 2.43. Consider the Pell's equation $x^2 - Dy^2 = 1$, for D a positive square-free integer.



It is easy to find given any rational number m, $p = \left(\frac{1+Dm^2}{1-Dm^2}, \frac{2m}{1-Dm^2}\right)$ is a rational solution of $x^2 - Dy^2 = 1$.

Remark. Note $x^2+y^2 = 1$ implies $x^2+y^2 = z^2$. Analogously, $x^2-Dy^2 = 1$ implies $x^2-Dy^2 = z^2$.

2.3 Congruences

In this section, assume $n \in \mathbb{N}$ and p is prime.

Definition 2.44. Defin *Euler's* ϕ-function by

$$\phi(n) := \#\{1 \leqslant a \leqslant n \mid \gcd(a,n) = 1\}.$$

Theorem 2.45.

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

Proof. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if there exists $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $ab \equiv 1 \pmod n$ if and only if there exists k such that $ab + nk = 1$ if and only if $\gcd(a, n) = 1$. □

Theorem 2.46 (Euler's theorem)**.** *If* $\gcd(a, n) = 1$*, then* $a^{\phi(n)} \equiv 1 \pmod n$*.*

Proof. Since $\gcd(a, n) = 1$, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. So $a^{\phi(n)} = a^{\#(\mathbb{Z}/n\mathbb{Z})^\times} \equiv 1 \pmod n$. □

Corollary 2.47 (Fermat's little theorem (FLT))**.** If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.

Proof. Since $\gcd(a, p) = 1$ and $\phi(p) = p - 1$, take $n = p$ in Euler's theorem. □

Remark. If we want to solve $ax \equiv b \pmod n$, we are asking if a has an inverse modulo n. If we consider this as an equation over $\mathbb{Z}/n\mathbb{Z}$, can we solve $ax = b$? Yes, if $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\gcd(a, n) = 1$.

Corollary 2.48.

$$a^p \equiv a \pmod p, \forall a \in \mathbb{Z}.$$

Proof. By Fermat's little theorem and $0^p \equiv 0 \pmod p$. □

Theorem 2.49 (Wilson's theorem)**.**

$$(p-1)! \equiv -1 \pmod p.$$

Proof. If $p = 2$ or 3, we are done. For $1 \leqslant a < p$, $\gcd(a, p) = 1$. Then there exists $1 \leqslant \widetilde{a} < p$ such that $\widetilde{a}a \equiv 1 \pmod p$. Pair them up. The issue is if $a^2 \equiv 1 \pmod p$, then $p \mid a^2 - 1 = (a+1)(a-1)$, i.e., $a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$. So $a = 1$ or -1. Then $\{2, \ldots, p-2\}$ can be grouped into pairs whose product is 1 modulo p, i.e.,

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) = 1 \cdot (p-1) \prod_{j=2}^{n-2} j \equiv (p-1) \cdot 1 \pmod p \equiv -1 \pmod p.$$ □

Theorem 2.50.

$$x^2 \equiv -1 \pmod p \begin{cases} \textit{has a solution} & \textit{if } p = 2 \textit{ or } p \equiv 1 \pmod 4 \\ \textit{has no solution} & \textit{if } p \equiv 3 \pmod 4 \end{cases}.$$

Proof. If $p = 2$, this is straightforward. If $p \equiv 1 \pmod 4$, set $r = \frac{p-1}{2}$. Then $2 \mid r$. Set $x = \pm(r!)$. Since $\frac{m-p}{2} \equiv \frac{m+p}{2} \pmod p$, we have

$$\begin{aligned} x^2 = (r!)^2 &= 1 \cdots \frac{p-1}{2}\frac{p-1}{2} \cdots 1 = 1 \cdots \frac{p-1}{2}\frac{p-1}{2} \cdots 1 \cdot (-1)^{\frac{p-1}{2}} \\ &= 1 \cdots \frac{p-1}{2}\frac{1-p}{2} \cdots (-1) \equiv 1 \cdots \frac{p-1}{2}\frac{1-p}{2} \cdots \frac{p-2-p}{2} \pmod p \\ &\equiv 1 \cdots \frac{p-1}{2}\frac{1+p}{2} \cdots \frac{p-2+p}{2} \pmod p \equiv 1 \cdots \frac{p-1}{2}\frac{p+1}{2} \cdots (p-1) \pmod p \\ &\equiv (p-1)! \pmod p \equiv -1 \pmod p. \end{aligned}$$

Next, let $p \equiv 3 \pmod 4$ and assume there is some x such that $x^2 \equiv -1 \pmod p$. Then $p \nmid x$, i.e., $\gcd(x, p) = 1$. Since $\frac{p-1}{2}$ is odd, we have $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$. Also, by Fermat's little theorem, $(x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod p$, a contradiction since $p \neq 2$. □

Corollary 2.51. If $p \mid a^2+b^2$ and $p \equiv 3 \pmod 4$, then $p \mid a$ and $p \mid b$.

Proof. Note $a^2 \equiv -b^2 \pmod p$. Suppose $p \nmid b$. Since p is prime, there exists $\widetilde{b}$ such that $b\widetilde{b} \equiv 1 \pmod p$. So $b^2\widetilde{b}^2 \equiv 1 \pmod p$ and then $(a\bar{b})^2 \equiv -1 \pmod p$, contradicted by $p \equiv 3 \pmod 4$. □

Lemma 2.52. $p = a^2+b^2$ for some a, b if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. $p = 2$ is straightforward.

$\Longrightarrow$ Suppose $p \equiv 3 \pmod 4$. Since p is prime, $a \neq 0$ and $b \neq 0$. Since $p = a^2+b^2$, then $p \mid a$ and $p \mid b$ by Corollary 2.51. So there exist $a_0, b_0 \in \mathbb{Z} \smallsetminus \{0\}$ such that $p = p^2(a_0^2+b_0^2)$, i.e., $1 = a_0^2+b_0^2$, a contradiction.

$\Longleftarrow$ Define $f(u,v) = u+vx, u, v \in \mathbb{Z}$ for some $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod p$. Set $k = \lfloor \sqrt{p} \rfloor$. Then $k < \sqrt{p} < k+1$. Let $S = \{(u,v) \mid 0 \leqslant u, v \leqslant k\}$. Then $\#S = (k+1)^2 > p$. So there is at least one residue class modulo p hit more than once by f when acting on S. Pick distinct $(u_1,v_1),(u_2,v_2) \in S$ such that $f(u_1,v_1) \equiv f(u_2,v_2) \pmod p$. Then $u_1 - u_2 \equiv (v_2-v_1)x \pmod p$, i.e., $(u_1-u_2)^2 \equiv (v_2-v_1)^2x^2 \equiv -(v_2-v_1)^2 \pmod p$, i.e., $(u_1-u_2)^2 + (v_2-v_1)^2 \equiv 0 \pmod p$. Let $a = u_1 - u_2$ and $b = v_2 - v_1$. Since $0 \leqslant u_1, u_2, v_1, v_2 \leqslant k$, we have $-k \leqslant a = u_1 - u_2 \leqslant k$ and $-k \leqslant b = v_1 - v_2 \leqslant k$. Since $k < \sqrt{p}$, we have $a^2+b^2 \leqslant 2k^2 < 2p$. Since a, b cannot be 0 at the same time, we have $0 < a^2+b^2 < 2p$. Also, since $a^2+b^2 \equiv 0 \pmod p$, we have $a^2+b^2 = p$. □

Theorem 2.53 (Fermat)**.** *Write*

$$n = 2^\alpha \left(\prod_{p \equiv 1 \pmod 4} p^\beta \right) \left(\prod_{q \equiv 3 \pmod 4} q^\gamma \right).$$

Then n is a sum of the 2 squares if and only if $2 \mid \gamma$ for each γ.

Proof. Observe

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (a+bi)(c+di)\overline{(a+bi)(c+di)} \\ &= \|ac-bd+(ad+bc)i\|^2 \\ &= (ac-bd)^2+(ad+bc)^2 = (ac+bd)^2+(ad-bc)^2.\end{aligned}$$

$\Longleftarrow$ Done by previous lemma and observation.

$\Longrightarrow$ Assume $n = a^2+b^2$. Let $q \mid n$ with $q \equiv 3 \pmod 4$. Then by Corollary 2.51, $q \mid a$ and $q \mid b$ and so $q^2 \mid n$. Then we can consider $\frac{n}{q^2} = \left(\frac{a}{q}\right)^2 + \left(\frac{b}{q}\right)^2$. If $\gamma = 2k+1$ for some $k \in \mathbb{N}$, given $\frac{n}{q^2}$ has the similar form as n, by inductive argument, we see $\frac{n}{q^{2k}} = \left(\frac{a}{q^k}\right)^2 + \left(\frac{b}{q^k}\right)^2$. □

Remark. The number of ways to write a $n \in \mathbb{N}$ as a sum of two squares is given by $s_n = \sum_{d \mid n} \chi_{-4}(d)$, where $\chi_{-4}(m) = \begin{cases} 1 & m \equiv 1 \pmod 4 \\ -1 & m \equiv 3 \pmod 4 \\ 0 & m \equiv 0, 2 \pmod 4 \end{cases}$.

Remark. We don't get every integer as a sum of 2 squares, what about the sum of r squares for $r > 2$? $r = 3$: no and $r = 4$: yes, which can be proved by the theorem of Lagrange. Use Hamiltonian quaternions to prove this: $\mathbb{Z}[i,j,k]$. Note $p = a^2+b^2 = (a+bi)(a-bi)$, which factors in $\mathbb{Z}[i]$ if $p = 2$ or $p \equiv 1 \pmod 4$ and does not factor in $\mathbb{Z}[i]$ if $p \equiv 3 \pmod 4$.

2.4 Chinese Remainder Theorem

In this section, assume p is prime. Let canonical factorization of n be $n = p_1^{e_1} \cdots p_r^{e_n}$.

Remark. If we are given $ax \equiv b \pmod{n}$, we know this has a solution if $\gcd(a, n) = 1$. Since there exist z, y such that $a(bz) + n(by) = b$, we have $x = bz$.

Theorem 2.54 (Chinese remainder theorem (CRT))**.** *Let $m_1, \dots, m_r$ denote r positive integers with $\gcd(m_i, m_j) = 1$ for any $i \neq j$. Let $a_1, \dots, a_m$ be in the system of congruence $x \equiv a_i \pmod{m_i}$ for $i = 1, \dots, r$. Then it has a solution. Moreover, if x_0 is a solution, then any other solution satisfies $x \equiv x_0 \pmod{m_1 \cdots m_n}$.*

Proof. Let $n = 2$. Then there exists $k_1 \in \mathbb{Z}$ such that $x - a_1 = m_1 k_1$. Then $a_1 + m_1 k_1 \equiv a_2 \pmod{m_2}$, i.e., $m_1 k_1 \equiv (a_2 - a_1) \pmod{m_2}$. Since $\gcd(m_1, m_2) = 1$, there exists $\widetilde{m}_1$ such that $m_1 \widetilde{m}_1 \equiv 1 \pmod{m_2}$. So $k_1 \equiv (a_2 - a_1)\widetilde{m}_1 \pmod{m_2}$. Then there exists $k_2 \in \mathbb{Z}$ such that $k_1 = (a_2 - a_1)\widetilde{m}_1 + k_2 m_2$. So $x = a_1 + m_1(a_2 - a_1)\widetilde{m}_1 + k_2 m_1 m_2$ and then $x \equiv a_1 + m_1(a_2 - a_1)\widetilde{m}_1 \pmod{m_1 m_2}$. The rest follows from the induction. □

Example 2.55. Find the solutons if any of $x \equiv 1 \pmod{15}$ and $x \equiv 2 \pmod{35}$. By the first congruence, we have $x \equiv 1 \pmod{3}$ and $x \equiv 1 \pmod{5}$. By the second congruence, we have $x \equiv 2 \pmod{5}$ and $x \equiv 2 \pmod{7}$. So $x \equiv 1 \pmod{5}$ and $x \equiv 2 \pmod{5}$, a contradiction.

Definition 2.56. (a) $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic function.*

(b) An arithmetic function f is *multiplicative* if for any $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, then $f(mn) = f(m)f(n)$.

(c) An arithmetic function f is *additive* if for any $m, n \in \mathbb{Z}_{\geqslant 1}$ with $\gcd(m, n) = 1$, then $f(mn) = f(m) + f(n)$.

(d) An arithmetic function f is *totally (completely) multiplicative* if $f(mn) = f(m)f(n)$ for any $m, n \in \mathbb{N}$.

(e) An arithmetic function f is *totally (completely) additive* if $f(mn) = f(m) + f(n)$ for any $m, n \in \mathbb{N}$.

Proposition 2.57. We have the followings.

(a) If f is completely multiplicative, then $\phi(n) = \phi(p_1)^{e_1} \cdots \phi(p_r)^{e_r}$.

(b) If f is multiplicative, then $\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r})$.

Definition 2.58. Any set $R \subseteq \mathbb{Z}$ is called a *reduced residue system modulo n* if

(a) $\gcd(r, n) = 1$ for $r \in R$;

(b) R contains $\phi(n)$ elements;

(c) no two elements of R are congruent modulo n.

Any set of n integers, no two of which are congruent modulo n, is called a *complete reduced residue system modulo n.*

Lemma 2.59.

$$\phi(p^k) = p^{k-1}(p-1), \forall k \in \mathbb{N}.$$

Proof. If $\gcd(p,d) > 1$ and $d \leqslant p^k$, then $d = p, 2p, \ldots, p^{k-1}p$, which has p^{k-1} of them. So $\phi(p^k) = p^k - p^{k-1}$. □

Theorem 2.60. *The arithmetic function ϕ is multiplicative. In particular,*

$$\phi(n) = \phi\left(\prod_{i=1}^{r} p_i^{e_i}\right) = \prod_{i=1}^{r} \phi(p_i^{e_i}) = \prod_{i=1}^{r} \left(p_i^{e_i} - p_i^{e_i-1}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. It is enough show ϕ is multiplicative. Let $n, n' \in \mathbb{N}$ with $\gcd(n,n') = 1$. Let a and a' run through a reduced residue system modulo n and n', respectively. The number of distinct pairs (a, a') is $\phi(n)\phi(n')$. Suppose $d := \gcd(an' + a'n, nn') \nmid n$. Then $d \neq 1$. Since $d \mid nn'$ and $\gcd(n,n') = 1$, without loss of generality, assume $d \mid n'$ and $d \nmid n$. Since $d \mid (an' + a'n)$, we have $d \mid a'$. Also, since $d \mid n'$ and $\gcd(a', n') = 1$, we have $\gcd(a', d) = 1$, contradicted by $d \mid a'$. Hence $d \mid n$. Similarly, $d \mid n'$. Then $d \mid \gcd(n, n') = 1$ and so $\gcd(an' + a'n, nn') = 1$. Thus, $an' + a'n \in (\mathbb{Z}/nn'\mathbb{Z})^\times$. Assume there exist a_1, a_2, a_1', a_2' such that $a_1 n' + a_1' n \equiv a_2 n' + a_2' n \pmod{nn'}$. Then $(a_1 - a_2)n' \equiv (a_2' - a_1')n \pmod{nn'}$ and so there exists k such that $(a_1 - a_2)n' = n\big((a_2' - a_1') + kn'\big)$, i.e., $(a_1 - a_2)n' \equiv 0 \pmod{n}$. Also, since $\gcd(n, n') = 1$, $a_1 \equiv a_2 \pmod{n}$. Simiarly, $a_1' \equiv a_2' \pmod{n'}$. Hence each $an' + a'n$ is a distinct reduced residue. Thus, $\phi(nn') \geqslant \phi(n)\phi(n')$.

Next, find b such that $\gcd(b, nn') = 1$. Then $\gcd(b, n) = 1 = \gcd(b, n')$. Claim. there are a, a' such that $an' + a'n \equiv b \pmod{n}$ with $\gcd(a, n) = 1 = \gcd(a', n')$. Write $\gcd(n, n') = 1 = nm' + n'm$ for some m, m'. Then $\gcd(m, n) = 1 = \gcd(m', n')$. Also, $b = b(nm' + n'm) = n(bm') + n'(bm) =: na + n'a'$. Since $\gcd(m, n) = 1$ and $\gcd(b, n) = 1$, $\gcd(bm, n) = 1$. Similarly, $\gcd(bm', n') = 1$. Since every reduced residue modulo nn' is of the form $an' + bn'$ with $\gcd(a, n) = 1 = \gcd(a', n')$, we have $\phi(n)\phi(n') \geqslant \phi(nn')$. □

Lemma 2.61. Let f be a multiplicative function. Define

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

Then g is also multiplicative.

Proof. Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. If $d \mid mn$, since $\gcd(m, n) = 1$, we can write $d = d_1 d_2$, where $d_1 = \gcd(d, m)$ and $d_2 = \gcd(d, n)$. Since $\gcd(d_1, d_2) = 1$, we have

$$g(mn) = \sum_{d \mid mn} f(d) = \sum_{d_1 d_2 \mid mn} f(d_1)f(d_2) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1)f(d_2) = \sum_{d_1 \mid m} f(d_1) \sum_{d_2 \mid n} f(d_2) = g(m)g(n).$$

□

Corollary 2.62.

$$\sum_{d \mid n} \phi(d) = n.$$

Proof. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the canonical factorization. Since the possible factors of $p_i^{e_i}$ are $p_i^0, \cdots, p_i^{e_i}$ and $\phi(1) = 1$, we have for $i = 1, \dots, r$,

$$\sum_{d | p_i^{e_i}} \phi(d) = \sum_{k=1}^{e_i} \phi(p_i^k) + 1 = 1 + \sum_{k=1}^{e_i} (p_i^k - p_i^{k-1}) = p_i^{e_i}.$$

Then by Proposition 2.57(b),

$$\sum_{d|n} \phi(d) = \sum_{d | p_1^{e_1} \cdots p_r^{e_r}} \phi\left(p_1^{e_1} \cdots p_r^{e_r}\right) = \sum_{d | p_1^{e_1}} \phi\left(p_1^{e_1}\right) \cdots \sum_{d | p_r^{e_r}} \phi\left(p_r^{e_r}\right) = p_1^{e_1} \cdots p_r^{e_r} = n.$$ □

Definition 2.63. Given $f(x) = a_r x^r + \cdots, a_1 x + a_0$, we say the *degree* of f modulo n is j if $a_j \not\equiv 0 \pmod{n}$ and $a_{j+1}, \dots, a_r \equiv 0 \pmod{n}$.

Theorem 2.64. *Let $f \in \mathbb{Z}[x]$ and $N_f(m)$ be the number of solution of $f \equiv 0 \pmod{m}$. Then N_f is a multiplicative function, i.e., $N_f(n) = N_f(\prod_{j=1}^r p_j^{e_j}) = \prod_{j=1}^r N_f(p_j^{e_j})$.*

Proof. Let $m_1, m_2 \in \mathbb{N}$ with $\gcd(m_1, m_2) = 1$. Assume $f(a) \equiv 0 \pmod{m_1 m_2}$ for some a. Let $a_j \equiv a \pmod{m_j}$ for $j = 1, 2$, then $f(a_j) \equiv f(a) \equiv 0 \pmod{m_j}$ for $j = 1, 2$. Given a, we get a distinct pair (a_1, a_2). So $N_f(m_1 m_2) \leqslant N_f(m_1) N_f(m_2)$.

Next, assume $f(a_1) \equiv 0 \pmod{m_1}$ and $f(a_2) \equiv 0 \pmod{m_2}$ for some a_1, a_2. Since $\gcd(m_1, m_2) = 1$, by CRT, there exist a such that $a \equiv a_1 \pmod{m_1}$ and $a \equiv a_2 \pmod{m_2}$. Then $f(a) \equiv f(a_1) \equiv 0 \pmod{m_1}$ and $f(a) \equiv f(a_2) \equiv 0 \pmod{m_2}$. So $m_1 \mid f(a)$ and $m_2 \mid f(a)$. Since $\gcd(m_1, m_2) = 1$, $m_1 m_2 \mid f(a)$, i.e., $f(a) \equiv 0 \pmod{m_1 m_2}$. So $N_f(m_1) N_f(m_2) \leqslant N_f(m_1 m_2)$. □

Example 2.65. $2x \equiv 0 \pmod{4}$. Then $x = 0$ and $x = 2$ are both solutions though $\deg(2x) = 1$.

Theorem 2.66. *Let $f \in \mathbb{Z}[x]$ have degree n modulo p with $n \geqslant 1$. Then the congruences $f(x) \equiv 0 \pmod{p}$ has at most n solutions.*

Proof. If $n = 1$, then $ax + b \equiv 0 \pmod{p}$, so $x \equiv -ba^{-1} \pmod{p}$. Proved by induction. Assume the result is true for all polynomials of degree less than n. Let $\deg(f) = n$. If f has no solutions, we are done. Suppose f has a solution a. Then $f(a) \equiv 0 \pmod{p}$. Then we can write $f(x) = (x - a)g(x)$ for some $g \in (\mathbb{Z}/p\mathbb{Z})[x]$. Then $\deg(g) < \deg(f) = n$, so induction hypothesis gives at most $\deg(g)$ solutions to $g(x) \equiv 0 \pmod{p}$. So $f(x) \equiv (x-a)g(x) \equiv 0 \pmod{p}$ implies $x = a$ or $g(x) \equiv 0 \pmod{p}$. Hence f has at most $1 + \deg(g) = \deg(f)$ roots. □

Corollary 2.67. If $d \mid p - 1$, then the congruence $x^d \equiv 1 \pmod{p}$ has precisely d solutions.

Example 2.68. (a) $x^2 \equiv -1 \pmod{p}$ has 2 solutions if $p \equiv 1 \pmod{4}$ and has 0 solutions if $p \equiv 3 \pmod{4}$.

(b) $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p - 1$ solutions by Fermat's little theorem. Then $x^{p-1} - 1 \equiv (x - 1) \cdots (x - (p - 1)) \equiv 0 \pmod{p}$. Plug in $x = 0$, $-1 \equiv (-1) \cdots \big(-(p - 1)\big) \equiv (p - 1)! \pmod{p}$, which is Wilson's theorem.

2.5 Newton's method

In this section, assume p is prime.

Theorem 2.69. *This method gives a sequence of real numbers x_n satisfying $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$. You hope $x_n \to x$.*

Example 2.70. Find a solution to the congruences $f(x) = x^2 + 1 \equiv 0 \pmod{5^4}$. Consider $x^2 + 1 \equiv 0 \pmod 5$, which has solutions $2, 3$. If $x_0 = 2$, then $f'(x_0) = 2x_0 \equiv 4 \equiv -1 \pmod 5$. Also, $f(x_0) = 5 \equiv 0 \pmod 5$. Then $x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} = 2 - \frac{5}{-1} = 7$. Then $f(x_1) = x_1^2 + 1 = 50 \equiv 0 \pmod{5^2}$ and $f'(x_1) = 2x_1 \equiv 14 \equiv -1 \pmod 5$. So $x_2 = x_1 - \frac{f(x_1)}{f'(x_1)} = 7 - \frac{50}{-1} = 57$. Then $f(x_2) = x_2^2 + 1 = 3250 \equiv 0 \pmod{5^3}$ and $f'(x_2) = 2x_2 = 114 \equiv -1 \pmod 5$. So $x_3 = x_2 - \frac{f(x_2)}{f'(x_2)} = 57 - \frac{3250}{-1} \equiv 182 \pmod{5^4}$. Then $x_3^2 + 1 \equiv 0 \pmod{5^4}$.

Lemma 2.71 (Hensel's lemma)**.** Let $f \in \mathbb{Z}[x]$. Suppose $f(a) \equiv 0 \pmod{p^j}$, $p^t \mid\mid f'(a)$ and $j \geqslant 2t + 1$. Then

(a) whenever $b \equiv a \pmod{p^{j-t}}$, we have $f(b) \equiv f(a) \pmod{p^j}$ and $p^t \mid\mid f'(b)$;

(b) there exists a unique $s \pmod p$ with the property that $f(a + sp^{j-t}) \equiv 0 \pmod{p^{j+1}}$.

Proof. (a) Write $b - a = hp^{j-t}$ for some h. Since $2(j - t) = j + j - 2t \geqslant j + 1 > j$ and $p^t \mid f'(a)$,

$$f(b) = f(a + hp^{j-t}) = f(a) + f'(a)hp^{j-t} + \frac{f''(a)}{2}(hp^{j-t})^2 + \cdots \equiv f(a) \pmod{p^j}.$$

Since $j - t \geqslant t + 1$,

$$f'(b) = f'(a + hp^{j-t}) = f'(a) + f''(a)hp^{j-t} \pmod{p^{2(j-t)}} \equiv f'(a) \pmod{p^{t+1}}.$$

Thus, $p^t \mid\mid f'(b)$.

(b) Write $f'(a) = gp^t$ for some g with $\gcd(p, g) = 1$. Note there exists $\bar{g}$ such that $g\bar{g} \equiv 1 \pmod p$, i.e., $1 - g\bar{g} \equiv 0 \pmod p$. Since $f(a) \equiv 0 \pmod{p^j}$, we have $f(a)(1 - g\bar{g}) \equiv 0 \pmod{p^{j+1}}$. Let $a' := a - p^{-t}\bar{g}f(a)$. Since $f(a) \equiv 0 \pmod{p^j}$, $p^{-t}f(a) \equiv 0 \pmod{p^{j-t}}$. Since $2(j - t) \geqslant j + 1$,

$$\begin{aligned} f(a') = f\big(a - p^{-t}\bar{g}f(a)\big) &\equiv f(a) - \big(p^{-t}\bar{g}f(a)\big)f'(a) + \frac{f''(a)}{2}\big(p^{-t}\bar{g}f(a)\big)^2 \pmod{p^{3(j-t)}} \\ &\equiv f(a) - \big(p^{-t}f(a)\bar{g}\big)f'(a) \pmod{p^{j+1}} = f(a) - f(a)g\bar{g} \pmod{p^{j+1}} \\ &\equiv f(a)(1 - g\bar{g}) \pmod{p^{j+1}} \equiv 0 \pmod{p^{j+1}}. \end{aligned}$$

With $g = p^{-t}f'(a)$, set $s := -p^{-j}f(a)\bar{g} \equiv -p^{-j}f(a)g^{-1} \pmod p = -p^{-j}f(a)\left[p^{-t}f'(a)\right]^{-1} \pmod p$.

Suppose we have two s' and s such that $f(a + sp^{j-t}) \equiv f(a + s'p^{j-t}) \pmod{p^{j+1}}$. Then $f(a) + sp^{j-t}f'(a) \equiv f(a) + s'p^{j-t}f'(a) \pmod{p^{j+1}}$, i.e., $sp^{j-t}f'(a) \equiv s'p^{j-t}f'(a) \pmod{p^{j+1}}$. Since $p^t \mid\mid f'(a)$, we have $p^j \frac{f'(a)}{p^t}(s - s') \equiv 0 \pmod{p^{j+1}}$. So $s \equiv s' \pmod p$. □

Remark. Let $f(a_1) \equiv 0 \pmod{p^j}$ with $p^t \mid\mid f'(a_1)$ and $j \geqslant 2t + 1$. Then there exists s_1 such that $f(a_2) := f(a_1 + s_1p^{j-t}) \equiv 0 \pmod{p^{j+1}}$. So $a_2 - a_1 = s_1p^{j-t} \equiv 0 \pmod{p^{t+1}}$. Next, since

$f'(a_2) = f'(a_1 + s_1 p^{j-t}) = f'(a_1) + f''(a_1)s_1 p^{j-t} \equiv f'(a_1) \pmod{p^{t+1}}$ and $p^t \mid\mid f'(a_1)$, $p^t \mid\mid f'(a_2)$. Also, since $j+1 \geqslant 2t+1$, there exists a unique $s_2 \pmod p$ such that $f(a_3) := f(a_2 + s_2 p^{j+1-t}) \equiv 0 \pmod{p^{j+1}}$. So $a_3 - a_2 = s_2 p^{j+1-t} \equiv 0 \pmod{p^{t+2}}$. By inducitive process, we have from root a_1 modulo p, we get a sequence $(a_m)_{m\geqslant 1}$ such that for any $n \leqslant m$, $a_m \equiv a_n \pmod{p^{t+n}}$.

Corollary 2.72. If $f \in \mathbb{Z}[x]$ and there exists a such that $f(a) \equiv 0 \pmod{p^j}$ and $p \nmid f'(a)$ and $j \geqslant 1$. Then there exists a unique $s \pmod p$ with the property that $f(a + sp^j) \equiv 0 \pmod{p^{j+1}}$.

Example 2.73. Find a solution to the congruences $f(x) = x^2 + 1 \equiv 0 \pmod{5^4}$. Consider $x^2 + 1 \equiv 0 \pmod{5^1}$, which has solution $2, 3$. Let $a_1 = 2$, then $f'(a_1) = 2a_1 = 4$. Since $5^0 \mid\mid 4$, $t = 0$. Let

$$s_1 = -5^{-1}f(2)[5^{-0}f'(2)]^{-1} \pmod 5 = -\frac{1}{5}5(4)^{-1} \pmod 5 = -4 \pmod 5 \equiv 1 \pmod 5.$$

Then consider $x^2 + 1 \equiv 0 \pmod{5^2}$ with root $a_2 = 2 + 1 \cdot 5^{1-0} \equiv 7 \pmod{5^2}$, we have $f(a_2) \equiv 50 \equiv 0 \pmod{5^2}$ and $f'(a_2) = 2a_2 = 14$. Let

$$s_2 = -5^{-2}f(7)[5^{-0}f'(7)]^{-1} \pmod 5 = -\frac{1}{25}50(14)^{-1} \pmod 5 = -8 \pmod 5 \equiv 2 \pmod 5.$$

Then consider $x^2 + 1 \equiv 0 \pmod{5^2}$ with root $a_3 = 7 + 2 \cdot 5^{2-0} = 57 \pmod{5^3}$, we have $f(a_3) \equiv 3250 \equiv 0 \pmod{5^3}$ and $f'(a_3) = 2a_3 = 114$. Let

$$s_3 = -5^{-3}f(57)[5^{-0}f'(57)]^{-1} \pmod 5 = -\frac{1}{125}3250\frac{1}{114} \pmod 5 = -26\cdot(4)^{-1} \pmod 5 \equiv 1 \pmod 5.$$

Then $a_4 = 57 + 5^{3-0} \cdot 1 \equiv 182 \pmod{5^4}$ and $f(a_4) \equiv 182^2 + 1 \equiv 0 \pmod{5^4}$.

2.6 p-adic numbers

In this section, assume p is prime.

Definition 2.74. Let $\mathcal{K}$ be a field. A real-valued function $|\cdot| : \mathcal{K} \to \mathbb{R}^+$ is a *valuation* if there is a $M \in \mathbb{R}^+$ such that the following conditions hold: for any $b, c \in \mathcal{K}$,

(a) $|b| = 0$ if and only if $b = 0$,

(b) $|bc| = |b||c|$,

(c) if $|b| \leqslant 1$, then $|1 + b| \leqslant M$.

Example 2.75. (a) The trivial valuation, taking $M = 1$, $|x| = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$.

(b) The absolute value on $\mathbb{R}$ is a valuation, taking $M = 2$.

(c) Usual absolute value on $\mathbb{C}$, taking $M = 2$.

Definition 2.76. (a) Define the *p-adic absolute value/norm* by

$$|n|_p = \begin{cases} p^{-\nu_p(n)} & \text{if } n \neq 0 \\ 0 & \text{if } n = 0 \end{cases},$$

where $\nu_p(n)$ is such that $p^{\nu_p(n)} \mid\mid n$.

(b) If $r \in \mathbb{Q} \smallsetminus \{0\}$, write $r = p^t \frac{a}{b}$ with $p \nmid ab$. Define the *p-adic absolute value/norm* by

$$|r|_p = \begin{cases} p^{-t} & \text{if } r \neq 0 \\ 0 & \text{if } r = 0 \end{cases}.$$

Theorem 2.77.

$$\left|\frac{m}{n}\right|_p = \frac{|m|_p}{|n|_p} = \frac{p^{-\nu_p(m)}}{p^{-\nu_p(n)}} = p^{-(\nu_p(m)-\nu_p(n))}, \forall \frac{m}{n} \in \mathbb{Q}.$$

Theorem 2.78. $|\cdot|_p$ *is a valuation on* $\mathbb{Q}$.

Proof. (a) It is straightforward.

(b) Let $r_1 = p^{t_1}\frac{a_1}{b_1}$ with $p \nmid a_1b_1$ and $r_2 = p^{t_2}\frac{a_2}{b_2}$ with $p \nmid a_2b_2$, then $r_1r_2 = p^{t_1+t_2}\frac{a_1a_2}{b_1b_2}$ with $p \nmid a_1a_2b_1b_2$. Then $|r_1r_2|_p = p^{-(t_1+t_2)} = |r_1|_p|r_2|_p$.

(c) Let $\alpha \in \mathbb{Q} \smallsetminus \{0\}$ such that $|\alpha|_p \leqslant 1$. Write $\alpha = p^t\frac{u}{v}$ with $p \nmid uv$, so $t \geqslant 0$. Let $s \geqslant 0$ such that $p^s \mid\mid v + p^t u$ and so $|1+\alpha|_p = \left|\frac{v+p^tu}{v}\right|_p = \frac{|v+p^tu|_p}{|v|_p} = \frac{p^{-s}}{1} \leqslant 1$. □

Theorem 2.79.

$$|x+y|_p \leqslant \max\{|x|_p, |y|_p\}, \forall x, y,$$

which is ultrametric inequality that is stronger than triangle inequality.

Definition 2.80. Given $|\cdot|$, $x \in \mathbb{Q}$ and $\epsilon \in \mathbb{R}_{>0}$, define an *open ball* by

$$B_{|\cdot|_p}(x,\epsilon) = \{y \in \mathbb{Q} : |x-y|_p < \epsilon\}.$$

Theorem 2.81. *Any point is the center of the disk.*

Proof. Let $a, b \in B_{|\cdot|}(x,\epsilon)$, then

$$|a-b|_p \leqslant |x-b+a-x|_p \leqslant \max\{|x-b|, |a-x|\} < \epsilon.$$

Hence $B_{|\cdot|_p}(a,\epsilon) = B_{|\cdot|_p}(x,\epsilon) = B_{|\cdot|_p}(b,\epsilon)$. □

Remark. In the p-adic integers, congruences are approximations: for $a, b \in \mathbb{Z}$, $a \equiv b \pmod{p^n}$ is the same as $|a-b|_p \leqslant \frac{1}{p^n}$. Turning information modulo one power of p into similar information modulo a higher power of p can be interpreted as improving an approximation.

Example 2.82. Define a sequence $a_1 = 4$, $a_2 = 34$, $a_3 = 334$, $a_4 = 3334$, $\cdots$. Then $a_n = \left\lceil \frac{10^n}{3} \right\rceil$ or $3a_n = 10^n + 2$, i.e., $3a_n - 2 = 10^n$. Then $|3a_n - 2|_5 = |10^n|_5 = 5^{-n} \to 0$. So $a_n \xrightarrow{|\cdot|_5} \frac{2}{3}$. Thus,

$$\frac{2}{3} = \lim_{n\to\infty} a_n = 3 + 3 \cdot 10 + 3 \cdot 10^2 + 3 \cdot 10^3 + \cdots.$$

Definition 2.83. Let $\mathcal{K}$ be any field with valuation $|\cdot|$. A sequence $\langle a_n \rangle \subseteq \mathcal{K}$ *converges* to b if for any $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that $|a_n - b| < \epsilon$ for any $n \geqslant N$.

Definition 2.84. We say a field $\mathcal{K}$ is *complete* if every Cauchy sequence in $\mathcal{K}$ converges to an element of $\mathcal{K}$.

Remark. Recall that when one completes $\mathbb{Q}$ with respect to the usual absolute value, we arrive at $\mathbb{R}$. We will develop a completion of $\mathbb{Q}$ based upon the p-adic absolute value $|\cdot|_p$, leading us to the complete metric space $\mathbb{Q}_p$, the field of p-adic **numbers**.

Remark. Given a valuation $|\cdot|$ on $\mathcal{K}$, we get a topology on $\mathcal{K}$ with basis given by open balls.

Definition 2.85. Let $\mathcal{K}$ be a field with valuation $|\cdot|$. We say $\mathcal{F} \supseteq \mathcal{K}$ together with a valuation $|\cdot|_{\mathcal{F}}$ that extend $|\cdot|$ is a *completion* of $\mathcal{K}$ w.r.t. $|\cdot|$ if

(a) $\mathcal{F}$ is complete.

(b) $\mathcal{F}$ is the closure of $\mathcal{K}$.

Theorem 2.86. *Given a field $\mathcal{K}$ with valuation $|\cdot|$, there is a completion of $\mathcal{K}$ w.r.t. $|\cdot|$. Moreover, any two completions are canonically isomorphic.*

Definition 2.87.

$$\mathbf{Q}_p = \textit{completion} \text{ of } \mathbb{Q} \text{ w.r.t. } |\cdot|_p.$$

Definition 2.88. A valuation $|\cdot|$ on $\mathcal{K}$ is called *non-archimedean* if it satisfies the ultrametric inequality. Otherwise, we say it is archimedean.

Example 2.89. $|\cdot|_p$ is non-archimedean on $\mathbb{Q}$. The absolute value $|\cdot|$ is archimedean on $\mathbb{Q}$.

Theorem 2.90 (Ostrowski)**.** *Let $\mathcal{K}$ be a field. If $\mathcal{K}$ is complete w.r.t archmedean valution $|\cdot|$, then $\mathcal{K}$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.*

Theorem 2.91. *If we consider $\mathbb{Q}$, the only valuation on $\mathbb{Q}$ are powers of $|\cdot|$, or $|\cdot|_p$.*

Definition 2.92. Let $\mathcal{K}$ be a field with non-archmedean valuation $|\cdot|$. Define

$$\mathcal{O} = \{x \in \mathcal{K} : |x| \leqslant 1\},$$
$$\mathfrak{p} = \{x \in \mathcal{K} : |x| < 1\},$$
$$\mathcal{O}^\times = \{x \in \mathcal{K} : |x| = 1\} = \mathcal{O} \smallsetminus \mathfrak{p}.$$

Theorem 2.93. *(a) The set $\mathcal{O}$ is a ring, which is called the valuation ring. The set $\mathcal{O}$ is also referred to as the $(|\cdot|)$-adic integers, for example $\mathbf{Z}_p$: p-adic integers.*

(b) The set $\mathfrak{p}$ is the maximal ideal in the local ring $\mathcal{O}$. $\mathcal{O}/\mathfrak{p}$ is called residue class field.

(c) The set $\mathcal{O}^\times$ is the units in $\mathcal{O}$.

Example 2.94. Let $\frac{2}{3} \in \mathbb{Q}$. Then $\frac{2}{3}$ is a 5-adic **integer** since $\left|\frac{2}{3}\right|_5 = 1$, but not a 3-adic integer since $\left|\frac{2}{3}\right|_3 = 3$.

Remark. If $\mathcal{K} = \mathbf{Q}_p$, then $\mathcal{O} =: \mathbf{Z}_p$, which is where our sequence of lifted solutions from Hensel's lemma.

Example 2.95. Let $\mathcal{K} = \mathbf{Q}_p$, then with $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \smallsetminus \{0\}$,

$$\mathcal{O} = \left\{\frac{a}{b} : p \nmid b\right\},$$
$$\mathfrak{p} = \left\{\frac{a}{b} \in \mathcal{O} : p \mid a\right\},$$
$$\mathcal{O}^\times = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid ab\right\} = \left\{\frac{a}{b} \in \mathcal{O} : p \nmid a\right\}.$$

Definition 2.96. Let $\hat{\mathcal{K}}$ be the completion of $\mathcal{K}$ w.r.t. $|\cdot|$. Let $\hat{\mathcal{O}}$ be the valuation ring of $\hat{\mathcal{K}}$. Let $\hat{\mathfrak{p}}$ be the maximal ideal in $\hat{\mathcal{O}}$. Let $\hat{\mathcal{O}}^{\times}$ be the units in $\hat{\mathcal{O}}$.

Lemma 2.97. The natural map $\mathcal{O}/\mathfrak{p} \to \hat{\mathcal{O}}/\hat{\mathfrak{p}}$ induced via $\mathcal{O} \hookrightarrow \hat{\mathcal{O}}$ is an isomorphism.

$$\begin{array}{ccc} \mathcal{K} & \hookrightarrow & \hat{\mathcal{K}} \\ \uparrow & & \uparrow \\ \mathcal{O} & \dashrightarrow & \hat{\mathcal{O}} \end{array}$$

$$|\cdot|_{\hat{\mathcal{K}}}\big|_{\mathcal{K}} = |\cdot|_{\mathcal{K}}.$$

Proof. Let $R \overset{\psi}{\hookrightarrow} S$ be a ring homomorphism and $I \leqslant R$ and $J \leqslant S$ be ideals with $\psi(I) \subseteq J$. Define $\phi : R/I \to S/J$ by $r + I \mapsto \psi(r) + J$. Let $r_1 + I = r_2 + I \in R/I$. Since ψ is a ring homomorphism, $\psi(r_1) - \psi(r_2) = \psi(r_1 - r_2) \in \psi(I) \subseteq J$. So $\psi(r_1) + J = \psi(r_2) + J$. Hence ϕ is well-defined. Clearly, it is also a ring homomorphism.

Consider $\varphi : \mathcal{O}/\mathfrak{p} \to \hat{\mathcal{O}}/\hat{\mathfrak{p}}$ by $a + \mathfrak{p} \mapsto a + \hat{\mathfrak{p}}$. Then φ is a well-defined ring homomorpism since $f : \mathfrak{p} \overset{\subseteq}{\longrightarrow} \hat{\mathfrak{p}}$ is a ring homomorphism and $f(\mathfrak{p}) = \mathfrak{p} \subseteq \hat{\mathfrak{p}}$. Let $a + \mathfrak{p} \in \mathrm{Ker}(\varphi)$ with $a \in \mathcal{O}$. Then $a + \hat{\mathfrak{p}} = \hat{\mathfrak{p}}$, i.e., $a \in \hat{\mathfrak{p}}$. Then $|a|_{\mathcal{K}} = |a|_{\hat{\mathcal{K}}} < 1$. So $a \in \mathfrak{p}$ and then $a + \mathfrak{p} = \mathfrak{p}$. Thus, it is 1-1. Let $\alpha + \hat{\mathfrak{p}} \in \hat{\mathcal{O}}/\hat{\mathfrak{p}}$ with $\alpha \in \hat{\mathcal{O}}$. Since $\hat{\mathcal{K}}$ is the closure of $\mathcal{K}$, there exists $a \in \mathcal{K}$ such that $|a - \alpha|_{\hat{\mathcal{K}}} < 1$. Also, since $\alpha \in \hat{\mathcal{O}}$, $|\alpha|_{\hat{\mathcal{K}}} \leqslant 1$. So $|a|_{\mathcal{K}} = |a|_{\hat{\mathcal{K}}} = |\alpha + (a - \alpha)|_{\hat{\mathcal{K}}} \leqslant \max\{|\alpha|_{\hat{\mathcal{K}}}, |a - \alpha|_{\hat{\mathcal{K}}}\} \leqslant 1$. So $a \in \mathcal{O}$. Also, since $|a - \alpha|_{\hat{\mathcal{K}}} < 1$, $a - \alpha \in \hat{\mathfrak{p}}$. Hence $\varphi(a + \mathfrak{p}) = a + \hat{\mathfrak{p}} = \alpha + \hat{\mathfrak{p}}$. Thus, φ is onto. ☐

Example 2.98 (Exercise)**.** Let $\mathcal{K} = \mathbf{Q}_p$. Show that $\mathcal{O}/\mathfrak{p} \cong \mathbb{F}_p$.

Remark. Our result gives $\hat{\mathcal{K}} = \mathbf{Q}_p$, $\hat{\mathcal{O}} = \mathbf{Z}_p$ and $\hat{\mathcal{O}}/\hat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p} \cong \mathbb{F}_p$.

Let $|\cdot|$ be nonarchmedean.

Definition 2.99. The set $\{|a| : a \in \mathcal{K}^{\times}\}$ is a subgroup of $(\mathbb{R}_{>0}, \cdot)$. This is called the *valuation group.*

Example 2.100 (Exercise)**.** The valuation groups of $\mathcal{K}$ and $\hat{\mathcal{K}}$ coincides.

Definition 2.101. A valuation $|\cdot| : \mathcal{K} \to \mathbb{R}^+$ is *discrete* if there exists $\delta > 0$ such that when $1 - \delta \leqslant |a| \leqslant 1 + \delta$, we have $|a| = 1$.

Lemma 2.102. A valuation $|\cdot| : \mathcal{K} \to \mathbb{R}^+$ is discrete if and only if the max ideal $\mathfrak{p}$ is principal.

Proof. $\Longleftarrow$ Let $\mathfrak{p} = \langle \varpi \rangle \mathcal{O}$ for some $\varpi \in \mathcal{K}$. If $|a| < 1$, then $a \in \mathfrak{p}$ and so $a = \varpi b$ for some $b \in \mathcal{O}$. So $|a| \leqslant |\varpi|$. If $|a| > 1$, then $\left|\frac{1}{a}\right| < 1$ and so $\frac{1}{a} \in \mathfrak{p}$. Then $\frac{1}{a} = \varpi c$ for some $c \in \mathcal{O}$. So $|a| \geqslant |\varpi|^{-1}$. This gives $|\cdot|$ is discrete since when $|\varpi| < |a| < |\varpi|^{-1}$, then $|a| = 1$.

$\Longrightarrow$ Since $|\cdot|$ is discrete, the set $S = \{|a| : |a| < 1\}$ attains an upper bound. Say this happens at ϖ. Let $c \in \mathfrak{p}$. Then $\left|\frac{c}{\varpi}\right| = \frac{|c|}{|\varpi|} \leqslant 1$ and so $\frac{c}{\varpi} \in \mathcal{O}$. Hence $c = \varpi \frac{c}{\varpi} \in \langle \varpi \rangle \mathcal{O}$ and so $\mathfrak{p} \subseteq \langle \varpi \rangle$. Clearly, $\langle \varpi \rangle \subseteq \mathfrak{p}$. Thus, $\mathfrak{p} = \langle \varpi \rangle$. ☐

Example 2.103. $\mathfrak{p} =$ max ideal of $\mathbf{Z}_p = p\mathbf{Z}_p$ and $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbb{F}_p$.

Lemma 2.104. Let $\mathcal{K}$ be complete w.r.t. a non-archmedean valuation $|\cdot|$. Then $\sum_{n=0}^{\infty} a_n$ converges if and only if $\lim_{n\to\infty} a_n = 0$.

Proof. Assume $\lim_{n\to\infty} a_n = 0$. Then given $\epsilon > 0$, there exists $N_\epsilon \in \mathbb{N}$ such that whenever $N > N_\epsilon$, $|a_N| < \epsilon$. Let $N \geqslant M > N_\epsilon$, then $\left|\sum_{i=0}^{N} a_i - \sum_{i=0}^{M} a_i\right| = \left|\sum_{i=M+1}^{N} a_i\right| \leqslant \max_{M+1\leqslant i\leqslant N}|a_i| < \epsilon$. So $\{\sum_{i=0}^{N} a_i\}$ is Cauchy and thus that $\mathcal{K}$ complete means it converges. □

Lemma 2.105. Let $\mathcal{K}$ be complete w.r.t. non-archmedean discrete valuation $|\cdot|$. Let $\varpi \in \mathcal{O}$ such that $\mathfrak{p} = (\varpi)$. Let $\mathcal{A} \subseteq \mathcal{O}$ be a set of representatives of $\mathcal{O}/\mathfrak{p}$. Then every $a \in \mathcal{O}$ has a unique representation $a = \sum_{n=0}^{\infty} a_n\varpi^n$ with $a_n \in \mathcal{A}$. Conversely, every such sum converges to an element of $\mathcal{O}$.

Proof. $\Longrightarrow$ Let $a \in \mathcal{O}$. Then there is a unique element $a_0 \in \mathcal{A}$ such that $a \in a_0 + \mathfrak{p}$. So $a = a_0 + \varpi b_1$ for some $b_1 \in \mathcal{O}$. Note there is a unique $a_1 \in \mathcal{A}$ such that $b_1 = a_1 + \varpi b_2$ for some $b_2 \in \mathcal{O}$. Then $a = a_0 + \varpi a_1 + \varpi^2 b_2$. Continue this and we get a unique sequence with $a = a_0 + a_1\varpi + a_2\varpi^2 + \cdots + a_n\varpi^n + b_{n+1}\varpi^{n+1}$. Since $\left|b_{n+1}\varpi^{n+1}\right| \leqslant \left|\varpi^{n+1}\right| = |\varpi|^{n+1} \to 0$, $a - \sum_{k=0}^{n} a_k\varpi^k = b_{n+1}\varpi^{n+1} \to 0$. Thus, $\sum_{n=0}^{\infty} a_j\varpi^j \to a$.

"$\Leftarrow$" It follows from Lemma 2.104. □

Corollary 2.106. Given a element of $\mathbf{Z}_p$, since $p\mathbf{Z}_p = \langle p\rangle$, we can write it uniquely in the form $\alpha = \sum_{n=0}^{\infty} a_n p^n$ with $a_n \in \{0, \ldots, p-1\}$.

Example 2.107. Suppose we want to find an element α in $\mathbf{Z}_7$ such that $5\alpha = 1$, i.e., $\alpha = \frac{1}{5}$. Let $\alpha = \sum_{n=0}^{\infty} a_n 7^n$. Then $0 = -1+5\alpha = -1+\sum_{n=0}^{\infty} 5a_n 7^n$, i.e., $-1+5a_0 \equiv 0 \pmod 7$, so $a_0 = 3$. Hence $\alpha = 3+\sum_{n=1}^{\infty} a_n 7^n$. Note $0 = -1+5\alpha = 14+\sum_{n=1}^{\infty} 5a_n 7^n$, i.e., $7\left((2+5a_1)+\sum_{n=2}^{\infty} 5a_n 7^{n-1}\right) = 0$. Then $2 + 5a_1 \equiv 0 \pmod 7$. So $a_1 = 1$. Hence $\alpha = 3 + 1\cdot 7^1 + \sum_{n=2}^{\infty} a_n 7^n$. Actually, $\frac{1}{5} = \alpha = 3 + 1\cdot 7 + 4\cdot 7^2 + 5\cdot 7^3 + \cdots$.

Proposition 2.108. Let $\{a_n\}_{n\in\mathbb{N}}$ be a Cauchy sequence in $\mathbf{Z}_p$. If $a_n \xrightarrow{|\cdot|_p} \alpha$, then $\alpha \in \mathbf{Z}_p$.

Proof. Since $a_n \xrightarrow{|\cdot|_p} \alpha$ in $\mathbf{Q}_p$, there is $N \in \mathbb{N}$ such that $|a_n - \alpha|_p < 1$ when $n \geqslant N$. Also, since $a_N \in \mathbf{Z}_p$, $|a_N|_p \leqslant 1$. So $|\alpha|_p = |\alpha - a_N + a_N|_p \leqslant \max\{|\alpha - a_N|_p, |a_N|_p\} \leqslant 1$. Thus, $\alpha \in \mathbf{Z}_p$. □

Proposition 2.109. (a) $\mathbb{Z}$ is dense in $\mathbf{Z}_p$. Formally, that means that for every $\alpha \in \mathbf{Z}_p$ and every $\epsilon > 0$, $B_{|\cdot|_p}(\alpha, \epsilon) \cap \mathbb{Z} \neq \emptyset$.

(b) $\mathbb{Q}$ is dense in $\mathbf{Q}_p$.

Proof. (a) Let $\epsilon > 0$. Then there exists $n \in \mathbb{N}$ such that $p^{-n} < \epsilon$. Let $\alpha \in \mathbf{Z}_p$. Then by Corollary 2.106, α has the unique representation $\sum_{k=1}^{\infty} a_k p^k$ with $a_k \in \mathbf{Z}_p$. Let $\beta = \sum_{k=1}^{n-1} a_k p^k \in \mathbb{Z}$. Then $|\alpha - \beta|_p \leqslant p^{-n} < \epsilon$.

(b) It is similar. □

Theorem 2.110 (A basic version of Hensel's lemma)**.** *If $f \in \mathbf{Z}_p[x]$ and $a \in \mathbf{Z}_p$ satisfies $f(a) \equiv 0 \pmod p$ and $f'(a) \not\equiv 0 \pmod p$, then there is a unique $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \pmod p$.*

Proof. We prove this by induction on $n \in \mathbb{N}$, there exists an $a_n \in \mathbf{Z}_p$ such that $f(a_n) \equiv 0 \pmod{p^n}$ and $a_n \equiv a \pmod p$. The case $n = 1$ is trivial, using $a_1 = a$. Assume the inductive hypothesis holds for n, we seek $a_{n+1} \in \mathbf{Z}_p$ such that $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$ and $a_{n+1} \equiv a \pmod p$. Since $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$ implies $f(a_{n+1}) \equiv 0 \pmod{p^n}$, any root of $f(X) \bmod p^{n+1}$ reduces to a root of $f(X)$ mod p^n. By the inductive hypothesis there is a root a_n mod p^n, so we seek an $a_{n+1} \in \mathbf{Z}_p$ such that $a_{n+1} \equiv a_n \pmod{p^n}$ and $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Write $a_{n+1} = a_n + t_n p^n$. The goal is to find $t_n \in \mathbf{Z}_p$ such that $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Assume $\deg(f) \geqslant 2$. Claim. $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$ for some $g \in \mathbf{Z}_p[X,Y]$. Write for some $d \geqslant 2$, $f(X) = \sum_{j=0}^{d} c_j X^j \in \mathbf{Z}_p[x]$. Then

$$
\begin{aligned}
f(X+Y) = \sum_{j=0}^{d} c_j (X+Y)^j &= c_0 + c_1(X+Y) + \sum_{j=2}^{d} c_j \left[X^j + \binom{j}{1} X^{j-1}Y + g_j(X,Y)Y^2 \right] \\
&= c_0 + c_1 X + c_1 Y + \sum_{j=2}^{d} c_j X^j + \sum_{j=2}^{d} c_j j X^{j-1} Y + \sum_{j=2}^{d} c_j g_j(X,Y)Y^2 \\
&= \sum_{j=0}^{d} c_j X^j + \sum_{j=0}^{d} c_j j X^{j-1} Y + \sum_{j=2}^{d} c_j g_j(X,Y)Y^2 = f(X) + f'(X)Y + g(X,Y)Y^2.
\end{aligned}
$$

Since $2n \geqslant n+1$ and $\frac{f(a_n)}{p^n} \in \mathbf{Z}_p$,

$$
\begin{aligned}
& f(a_{n+1}) = f(a_n + t_n p^n) \equiv 0 \pmod{p^{n+1}} \\
\iff & f(a_n) + f'(a_n) t_n p^n + g(a_n, t_n p^n)(t_n p^n)^2 \equiv 0 \pmod{p^{n+1}} \\
\iff & f(a_n) + f'(a_n) t_n p^n \equiv 0 \pmod{p^{n+1}} \\
\iff & f'(a_n) t_n p^n \equiv -f(a_n) \pmod{p^{n+1}} \\
\iff & f'(a_n) t_n \equiv -\frac{f(a_n)}{p^n} \pmod{p},
\end{aligned}
$$

Since $a_n \equiv a \pmod{p}$, $f'(a_n) \equiv f'(a) \not\equiv 0 \pmod{p}$. So there is a solution for t_n in the congruence mod p. Since $a_{n+1} = a_n + t_n p^n$ and $a_n \equiv a \pmod{p}$, we have $a_{n+1} \equiv a \pmod{p}$. This completes the induction. This also gives a sequence $\{a_j\}_{j \in \mathbb{N}}$ satisfying $f(a_j) \equiv 0 \pmod{p^j}$ and $a_{j+1} \equiv a_j \pmod{p^j}$, for $j \in \mathbb{N}$. Note $|a_{j+1} - a_j|_p \leqslant p^{-j}$ for $j \in \mathbb{N}$. So the sequence $\{a_j\}_{j \in \mathbb{N}}$ is Cauchy, which converges to some $\alpha \in \mathbf{Z}_p$. Also, note $a_m \equiv a_n \pmod{p^n}$ for any $m > n \geqslant 1$. Letting $m \to \infty$, we have $\alpha \equiv a_n \pmod{p^n}$ for $n \in \mathbb{N}$. In particular, $\alpha \equiv a \pmod{p}$. Also, since $f(\alpha) \equiv f(a_n) \equiv 0 \pmod{p^n}$, $|f(\alpha)|_p \leqslant \frac{1}{p^n}$ for $n \in \mathbb{N}$. Thus, $f(\alpha) = 0$. Suppose there exists $\beta \in \mathbf{Z}_p$ such that $f(\beta) = 0$ and $\beta \equiv a \pmod{p}$. Claim. $\beta = \alpha$. It is enough to show $\beta \equiv \alpha \pmod{p^n}$ for all $n \in \mathbb{N}$. Proof by induction. Since $\beta \equiv a \equiv \alpha \pmod{p}$, the case $n = 1$ is straightforward. Assume $\beta \equiv \alpha \pmod{p^n}$. Then $\beta = \alpha + p^n \gamma_n$ with $\gamma_n \in \mathbf{Z}_p$. We have $f(\beta) = f(\alpha + p^n \gamma_n) \equiv f(\alpha) + f'(\alpha) p^n \gamma_n \pmod{p^{n+1}}$. Since $f(\alpha) = 0 = f(\beta)$, $0 \equiv f'(\alpha) p^n \gamma_n \pmod{p^{n+1}}$ and then $f'(\alpha)\gamma_n \equiv 0 \pmod{p}$. Since $f'(\alpha) \equiv f'(a) \not\equiv 0 \pmod{p}$, we have $\gamma_n \equiv 0 \pmod{p}$. Thus, $\beta \equiv \alpha \pmod{p^{n+1}}$. □

Remark. In general, if $f'(a) \equiv 0 \pmod{p}$, then sometimes there are no lifts and sometimes there are multiple lifts.

Remark. A similar argument shows that for all $n \geqslant 1$, f has a unique root mod p^n that reduces to $a \pmod{p}$. So we can think about the uniqueness of the lifting of the mod p root in two ways: it has a unique lifting to a root in $\mathbf{Z}_p$ or it has a unique lifting to a root in $\mathbb{Z}/(p^n)$ for all $n \geqslant 1$.

Example 2.111. Let $f(x) = 5x - 1 \in \mathbf{Z}_7[x]$ and $a = 3$. Then $f(3) \equiv 0 \pmod{7}$ and $f'(x) = 5 \not\equiv 0 \pmod{7}$. So we have a unique $\alpha \in \mathbf{Z}_7$ such that $5\alpha = 1$ and $\alpha \equiv 3 \pmod{7}$. In previous example, we saw approximations to α.

Example 2.112. Let $f(x) = x^3 - 2 \in \mathbf{Z}_5[x]$. Note $f(3) \equiv 0 \pmod 5$, $f'(x) = 3x^2$ and $f'(3) \not\equiv 0 \pmod 5$. Then there exists unique $\alpha \in \mathbf{Z}_5$ such that $\alpha \equiv 3 \pmod 5$ and $\alpha^3 = 2$ in $\mathbf{Z}_5$. Note $\alpha = 3 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + \cdots$.

Example 2.113. Let $f(x) = x^3 - x - 2 \in \mathbf{Z}_2[x]$. Then $f(0) \equiv 0 \pmod 2$, $f(1) \equiv 0 \pmod 2$, $f'(x) \equiv 3x^2 - 1 \equiv x^2 - 1 \pmod 2$, $f'(0) \not\equiv 0 \pmod 2$ and $f'(1) \equiv 0 \pmod 2$. Hensel's lemma says you have a unique $\alpha \in \mathbf{Z}_2$ such that $f(\alpha) = 0$ and $\alpha \equiv 0 \pmod 2$. Explicitly, $\alpha = 0+2+2^2+2^4+2^7+\cdots$.

Example 2.114. Let $n \in \mathbb{Z}$, $p \nmid n$ and $u \in \mathbf{Z}_p$ such that $u \equiv 1 \pmod{p\mathbf{Z}_p}$, i.e., $u = 1 + a_1 p + a_2 p^2 + \cdots$ for some $a_1, a_2 \cdots \in \mathbb{Z}_p$. Then there exists $\beta \in \mathbf{Z}_p$ such that $\beta^n = u$. Let $f(x) = x^n - u$. Note $f(1) = 1^n - u = 1 - u \equiv 0 \pmod p$, $f'(x) = nx^{n-1}$ and $f'(1) = n \not\equiv 0 \pmod p$. By Hensel's lemma, there exists a unique $\beta \in \mathbf{Z}_p$ such that $f(\beta) = 0$ and $\beta \equiv 1 \pmod p$.

Definition 2.115. In mathematics, a root of unity, occasionally called a de Moivre number, is any complex number that gives 1 when raised to some positive integer power n. In field theory and ring theory the notion of root of unity also applies to any ring with a multiplicative identity element.

Any algebraically closed field has exactly n n^{th} roots of unity if n is not divisible by the characteristic of the field.

Example 2.116. Consider $f(x) = x^p - x \in \mathbf{Z}_p[x]$. By Fermat's little theorem, for $k = 0, \ldots, p-1$, $f(k) \equiv 0 \pmod p$ and $f'(x) = px^{p-1} - 1 \equiv -1 \not\equiv 0 \pmod p$. Hensel's lemma says for $k = 0, \ldots, p-1$, there exists a unique $w_k \in \mathbf{Z}_p$ such that $f(w_k) = 0$ and $w_k \equiv k \pmod p$. For $k = 1, \ldots, p-1$, we have $w_k^{p-1} = 1$. The numbers $\{w_k, 0 \leqslant k \leqslant p-1\}$ are distinct since they are already distinct when reduced modulo p. Thus, for each non-zero residue class modulo p, we get a unique $(p-1)^{\text{th}}$ root of unity. So $x^p - x = x\left(x^{p-1} - 1\right)$ splits completely over $\mathbf{Z}_p[x]$. Its roots in $\mathbf{Z}_p$ are 0 and p-adic $(p-1)^{\text{th}}$ roots of unitys. Note $w_0 = 0$, $w_1 = 1$ and $w_{p-1} = -1$. Other w_k's are more interesting. For instance, when $p = 5$, w_k is a root of $x^5 - x = x(x^4-1) = x(x-1)(x+1)(x^2+1)$. So w_2 and w_3 are square roots of -1 in $\mathbf{Z}_5$: $w_2 = 2+5+2\cdot5^2+5^3+3\cdot5^4+4\cdot5^5+\cdots$, $w_3 = 3+3\cdot5+2\cdot5^2+3\cdot5^3+5^4+\cdots$. Then $w_2, w_3 \in \mathbf{Z}_5$ such that $w_2^2 = -1$ and $w_3^2 = -1$.

Theorem 2.117 (A strong version of Hensel' lemma)**.** *Let $f(x) \in \mathbf{Z}_p[x]$ and $a \in \mathbf{Z}_p$ such that $|f(a)|_p < |f'(a)|_p^2$. There is a unique $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$ and $|\alpha - a|_p < |f'(a)|_p$. Moreover,*

(a) $|\alpha - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p < |f'(a)|_p$,

(b) $|f'(\alpha)|_p = |f'(a)|_p$.

Remark. In the basic version of Hensel' lemma, since $f'(a) \not\equiv 0 \pmod p$ if and only if $|f'(a)|_p = 1$, we have $|f(a)|_p < |f'(a)|_p^2 = 1$ if and only if $p \mid f(a)$.

2.6.1 Roots of unity in $\mathbf{Q}_p$ via Hensel's lemma

In this section, assume p is prime.

Remark. Hensel's lemma is often considered to be a method of finding roots to polynomials, but that is just the one aspect: the existence of a root. There is also a uniqueness part to Hensel's lemma: it tells us there is a unique root within a certain distance of an approximate root. We will use the uniqueness to find all of the roots of unity in $\mathbf{Q}_p$.

Theorem 2.118. *The roots of units in* $\mathbf{Q}_p$ *are the* $(p-1)^{th}$ *root of unity for* p *odd and* ± 1 *for* $p = 2$.

Proof. Let $x \in \mathbf{Q}_p$ with $x^n = 1$. Then $|x|_p^n = 1$. So $|x|_p = 1$. Hence $x \in \mathbf{Z}_p^\times \subseteq \mathbf{Z}_p$. Therfore, we work in $\mathbf{Z}_p$ right from the start. Let's consider roots of unity of order relatively prime to p. Let ξ_1 and ξ_2 be roots of unity in $\mathbf{Z}_p$ with order prime to p and let m be the product of their order. Then both of ξ_1 and ξ_2 are roots of $f(x) = x^m - 1$ and $p \nmid m$. Since $p \nmid 1$, we have $p \nmid \xi_j$ and then $|f'(\xi_j)|_p = \left|m\xi_j^{m-1}\right|_p = |\xi_j|_p^{m-1} = 1$ for $j = 1, 2$. Since $f(\xi_j) = 0$, the uniqueness of Hensel's lemma says that the only root α of $x^m - 1$ satisfying $|\alpha - \xi_j|_p < |f'(\xi_j)|_p = 1$ is ξ_j for $j = 1, 2$. So if $\xi_2 \equiv \xi_1 \pmod{p\mathbf{Z}_p}$, then by the uniqueness, $\xi_2 = \xi_1$. These statements says distinct roots of unity in $\mathbf{Z}_p$ having order prime to p cannot be congruent modulo p. In Example 2.116, we have showed in $\mathbf{Z}_p$, each w_k (congruence class) for $k = 1, \ldots, p-1$ is a root of $x^{p-1} - 1$ and $p - 1$ is prime to p. So each congruence class mod $p\mathbf{Z}_p$ contains a unique $(p-1)^{\text{th}}$ root of unity. Hence the only roots of unity of order prime to p in $\mathbf{Q}_p$ are roots of $x^{p-1} - 1$.

Claim. the only p^{th} root of unity in $\mathbf{Z}_p^\times$ is 1 for odd p and the only 4^{th} roots of unity in $\mathbf{Z}_2^\times$ are ± 1. This implies the only p^{th} power roots of unity in $\mathbf{Z}_p^\times$ are 1 for odd p and ± 1 for $p = 2$. First we consider roots of unity of p-power order. We first consider p odd and suppose $\xi \in \mathbf{Z}_p^\times = \{\sum_{k=0}^{\infty} a_k p^k \in \mathbf{Z}_p \mid a_0 \neq 0\}$ such that $\xi^p = 1$. Then $\gcd(\xi, p) = 1$ and $\xi \equiv 1 \pmod{p\mathbf{Z}_p}$. Consider $f(x) = x^p - 1$. Then $f(\xi) = 0$ and $|f'(\xi)|_p = \left|p\xi^{p-1}\right|_p = |p|_p |\xi|_p^{p-1} = |p|_p = \frac{1}{p}$. So the uniqueness in Hensel's lemma implies the ball

$$\left\{x \in \mathbf{Q}_p : |x - \xi|_p < |f'(\xi)|_p\right\} = \left\{x \in \mathbf{Q}_p : |x - \xi|_p \leqslant \frac{1}{p^2}\right\} = \xi + p^2\mathbf{Z}_p$$

contains no p^{th} root of unity other than ξ. Claim. $\xi \equiv 1 \pmod{p^2\mathbf{Z}_p}$, so 1 is in that ball and thus $\xi = 1$. Write $\xi = 1 + py$ for some $y \in \mathbf{Z}_p$. Then

$$1 = \xi^p = (1 + py)^p = 1 + p(py) + \sum_{k=2}^{p-1} \binom{p}{k} (py)^k + (py)^p \equiv 1 + p(py) \pmod{p^3},$$

i.e., $p^2 y \equiv 0 \pmod{p^3}$. So $p \mid y$. Thus, $\xi \equiv 1 \pmod{p^2}$ which forces $\xi = 1$. Now we turn to $p = 2$. We want to show the only 4^{th} roots of unity in $\mathbf{Z}_2^\times$ are ± 1. This won't use Hensel's lemma. Let $\xi \in \mathbf{Z}_2^\times$ be a 4^{th} root of unity and $\xi \neq \pm 1$. Since $x^4 - 1 = (x^2 - 1)(x^2) + 1$, we have $\xi^2 = -1$ and then $\xi^2 \equiv -1 \pmod 4$. However, since $\xi \in \mathbf{Z}_2^\times$, we have $\xi \equiv 1$ or $3 \pmod 4$ and then $\xi^2 \equiv 1 \pmod 4$, a contradiction. For any prime p, a root of unity is a (unique) product of a root of unity of p-power order and a root of unity of order prime to p, so the only root of unity in $\mathbf{Q}_p$, are the roots of $X^{p-1} - 1$ for $p \neq 2$ and ± 1 for $p = 2$. □

Lemma 2.119. $p\mathbf{Z}_p$ is the unique ideal of $\mathbf{Z}_p$.

Remark (Notation)**.** Usually, write μ_n for the n^{th} root unity. $\mu_n(\mathbb{C}) \subseteq \mathbb{C}$ where $\mu_n(\mathbb{C})$ is the set of n^{th} root of unity in $\mathbb{C}$. We showed $\mu_p(\mathbf{Q}_p) \subseteq \mathbf{Z}_p$.

Example 2.120. For $d \in \mathbb{Z}$, the equation $x^3 + 2y^3 + 5z^3 + dw^2 = 0$ has a nontrivial solution $(x, y, z, w) \in \mathbf{Z}_{17}^4$.

Proof. Note $(1, 2, 0, 0)$ satisfies $1^3 + 2 \cdot 2^3 + 5 \cdot 0^3 + d \cdot 0^3 \equiv 0 \pmod{17}$. Fix $(y, z, w) = (2, 0, 0)$ and set $f(x) = x^3 + 16$. Since $|f(1)|_{17} = |17|_{17} = \frac{1}{17} < 1$ and $|f'(1)|^2 = |3|_{17}^2 = 1^2 = 1$, we have $|f(1)|_{17} < |f'(1)|_{17}^2$. So Hensel's lemma applies to give $\alpha \in \mathbf{Z}_{17}$ with $f(\alpha) = 0$. Hence $\alpha^3 + 2 \cdot (2^3) + 5 \cdot 0^3 + d \cdot 0^3 = 0$, i.e., $(\alpha, 2, 0, 0) \in \mathbf{Z}_{17}^4$ is a nontrivial solution. □

2.6.2 Primitive roots

In this section, assume p is prime.

Definition 2.121. Let $n \in \mathbb{N}$ and $\gcd(a,n)=1$. Let $\mathrm{ord}_n(a)$ denote the (multiplicative) *order* of a modulo n,

Lemma 2.122. Let $n \in \mathbb{N}$ and $\gcd(a,n)=1$. Then the order of a modulo n exists and divides $\phi(n)$. Moreover, if $a^k \equiv 1 \pmod{n}$, then the order of a modulo n divides k.

Proof. By Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. Then the order exists and let $d = \mathrm{ord}_n(a)$. Since $\langle a \rangle \leqslant (\mathbb{Z}/n\mathbb{Z})^\times$, by Lagrange' theorem, $\mathrm{ord}_n(a) \mid \phi(n)$. Suppose $a^k \equiv 1 \pmod{n}$. Division algorithm allows us to write $k = d\epsilon + r$ with $r, d \in \mathbb{Z}$ and $0 \leqslant r < d$. So $a^k = a^{d\epsilon+r} = (a^d)^\epsilon \cdot a^r \equiv a^r \pmod{n}$. Since $a^k \equiv 1 \pmod{n}$, $a^r \equiv 1 \pmod{n}$. Then by the minimality of d, $r=0$. Thus, $d \mid k$. ☐

Lemma 2.123. Suppose $\mathrm{ord}_m(a) = h$. Then $\mathrm{ord}_m(a^k) = \frac{h}{\gcd(h,k)}$.

Proof. Since $\mathrm{ord}_m(a) = h$, $\gcd(a,m)=1$. So $\gcd(a^k,m)=1$. Assume $(a^k)^j \equiv 1 \pmod{m}$, then $h \mid kj$ by Lemma 2.122. Note $h \mid kj$ if and only if $\frac{h}{\gcd(h,k)} \mid \frac{k}{\gcd(h,k)} j$. Since $\gcd\left(\frac{h}{\gcd(h,k)}, \frac{k}{\gcd(k,h)}\right) = 1$, we have $\frac{h}{\gcd(h,k)} \mid j$. So $\frac{h}{\gcd(h,k)} \mid \mathrm{ord}_m(a^k)$. Note $(a^k)^{\frac{h}{\gcd(h,k)}} = a^{\frac{kh}{\gcd(h,k)}} = (a^h)^{\frac{k}{\gcd(h,k)}} \equiv 1 \pmod{m}$. So $\mathrm{ord}_m(a^k) \mid \frac{h}{\gcd(h,k)}$. ☐

Lemma 2.124. Let $\mathrm{ord}_m(a) = h$ and $\mathrm{ord}_m(b) = k$. If $\gcd(h,k)=1$, then $\mathrm{ord}_m(ab) = hk$.

Proof. Let $d = \mathrm{ord}_m(ab)$. Since $(ab)^{hk} = a^{hk} \cdot b^{hk} = (a^h)^k (b^k)^h \equiv 1^k \cdot 1^h \pmod{m} \equiv 1 \pmod{m}$, $d \mid hk$. Since $1 \equiv a^h \equiv (a^h)^d \pmod{m}$, $b^{dh} \equiv (a^h)^d b^{dh} \equiv \left[(ab)^d\right]^h \equiv 1 \pmod{m}$. So $k = \mathrm{ord}_m(b) \mid dh$. Since $\gcd(h,k)=1$, $k \mid d$. Similarly, $h \mid d$. This gives $hk = \frac{hk}{\gcd(h,k)} = \mathrm{lcm}(h,k) \mid d$. ☐

Definition 2.125. Let $m \in \mathbb{N}$. We say g is a *primitive root modulo* m if $\mathrm{ord}_m(g) = \phi(m)$.

Theorem 2.126. *g is a primitive root modulo m if and only if g is generator of $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. $\Longrightarrow$ Since $\mathrm{ord}_m(g)$ is defined, $\gcd(g,m)=1$. So $g \in (\mathbb{Z}/m\mathbb{Z})^\times$. Note $\mathrm{ord}_m(g) = \phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$.

$\Longleftarrow$ It is straightforward. ☐

Theorem 2.127. *There exists $\phi(p-1)$ primitive roots modulo p.*

Proof. If $p=2$, this is straightforward. Assume p is odd prime. Then each element in $\{1,\dots,p-1\}$ has order (modulo p) dividing $\phi(p) = p-1$. Given $d \mid p-1$, let $\psi(d)$ denotes the number of elements in $\{1,\dots,p-1\}$ with order d modulo p. So $\sum_{d \mid p-1} \psi(d) = p-1$. Claim. $\psi(d) = \phi(d)$ for any $d \mid p-1$. Let $d \mid p-1$. Suppose $\mathrm{ord}_p(a) = d$. Then $a, \dots, a^d$ are all inequivalent modulo p. These are all solutions of $x^d - 1 \equiv 0 \pmod{p}$ and no other solutions. So anythings of order d must be in this list. Alo, since $\mathrm{ord}_p(a^k) = \frac{d}{\gcd(d,k)}$ by Lemma 2.123, the elements of order d are precisely those a^k with $\gcd(d,k)=1$. These are $\phi(d)$ such powers. So in particular, $\psi(p-1) = \phi(p-1)$, which is the number of elements in $\{1,\dots,p-1\}$ with order $p-1 = \phi(p)$. ☐

Theorem 2.128. *Let g be a primitive root modulo p, then there exists x such that $g+px$ is a primitive root modulo p^2. Moreover, $g+px$ is a primitive root modulo p^k for $k \in \mathbb{N}$ when p is odd. (Thus, we have primitive roots modulo p^k, i.e., $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic for $k \in \mathbb{N}$).*

Proof. Want to find an x such that $g' := g+px$ is primitive modulo p^2. Since $\operatorname{ord}_p(g) = \phi(p) = p-1$, $g^{p-1} = 1 + py$ for some y. We have $(g')^{p-1} = (g + px)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}px \pmod{p^2}$. So $(g')^{p-1} = 1+pz$ with $z \equiv \frac{g^{p-1}-1}{p} + (p-1)g^{p-2}x \pmod{p^2}$. Since $(p-1)g^{p-2}$ is prime to p and we can choose x such that $\gcd(z,p) = 1$ (first choose such a z, and then solve for x). Since $g' \equiv g \pmod p$, g' is primitive modulo p. Let $k \geqslant 2$ and $d = \operatorname{ord}_{p^k}(g')$. Then $d \mid \phi(p^k) = p^{k-1}(p-1)$. We have $(g + px)^d = g'^d \equiv 1 \pmod p$, i.e., $g^d \equiv 1 \pmod p$. So $p - 1 \mid d$. Since $(g')^{p-1} = 1 + pz$ with $\gcd(p,z) = 1$, $(g')^{p-1} \not\equiv 1 \pmod{p^2}$. So $d \neq p-1$ and then $d > p-1$. Since $\phi(p) = (p-1) \mid d \mid p^{j-1}(p-1)$ for $j \geqslant 2$, $(p-1) \mid d \mid p(p-1)$.

Let $k = 2$. Since $d > p-1$, $\operatorname{ord}_{p^2}(g') = d = p(p-1) = \phi(p^2)$. Thus, g' is primitive modulo p^2.

For higher power $k \geqslant 3$, assume p is odd. Suppose $d = \operatorname{ord}_{p^k}(g') < \phi(p^k) = p^{k-1}(p-1)$. Since $\phi(p) = p-1 \mid d \mid p^{k-1}(p-1)$, we have $d = p^j(p-1)$ for some $0 \leqslant j \leqslant k-1$. Since p is odd, $\left((g')^{p-1}\right)^{p^j} = (1+pz)^{p^j} = 1 + p^{j+1}z_j$ for some z_j with $\gcd(z_j,p) = 1$ since $\gcd(z,p) = 1$. So if $(g')^{p^j(p-1)} \equiv 1 \pmod{p^k}$, then $j+1 \geqslant k$, a contradiction. Thus, we must have $d = \phi(p^k)$. ☐

Exercise 2.129. What does the proof fail for $p = 2$?

Corollary 2.130. (a) The number of primitive root modulo p is $\phi(p-1)$.

(b) The number of primitive roots modulo p^2 is $(p-1)\phi(p-1)$.

(c) The number of primitive roots modulo p^k is $p^{k-2}(p-1)\phi(p-1)$, where p is odd.

Proof. Let m be a modulus in each question. Then by Theorem 2.128, there exists a primitive root g modulo m. ☐

Theorem 2.131. *There exists primitive root modulo m if and only if $m = 2, 4, p^k$ or $2p^k$ for p odd prime.*

Proof. For $2, 4, p^k$ with p odd, we are done. Let p be odd and $m = 2p^k$, By Theorem 2.128, there is a primitive root modulo p^k denoted by g. Since p^k is odd, either g or $g + p^k$ is odd. Set g' be whichever is odd. Then $g' \equiv g \pmod{p^k}$. Suppose there exists $b \in \mathbb{N}$ and $b < \phi(p^k)$ such that $g'^b \equiv 1 \pmod{2p^k}$, then $g'^b \equiv 1 \pmod{p^k}$, a contradiction. So the order of g' modulo $2p^k$ must be at least $\phi(p^k) = \phi(2)\phi(p^k) = \phi(2p^k)$. Thus, g' is a primitive root modulo $2p^k$.

Next, suppose m is none of these forms. Write $m = n_1n_2$ with $\gcd(n_1,n_2) = 1$ and $n_1, n_2 > 2$. If $\gcd(j,n) = 1$, then $\gcd(n-j,n) = 1$. So for $n > 2$, all numbers relatively prime to n can be matched up into pairs $\{j, n-j\}$. Hence $\phi(n_1)$ and $\phi(n_2)$ are even. Take a with $\gcd(a,m) = 1$. Then $\gcd(a,n_1) = 1 = \gcd(a,n_2)$. By Euler's theorem, $a^{\phi(n_1)} \equiv 1 \pmod{n_1}$. Since ϕ is multiplicative, $a^{\frac{1}{2}\phi(m)} = a^{\frac{1}{2}\phi(n_1)\phi(n_2)} \equiv \left(a^{\phi(n_1)}\right)^{\frac{\phi(n_2)}{2}} \equiv 1 \pmod{n_1}$. Similarly, $a^{\frac{1}{2}\phi(m)} \equiv 1 \pmod{n_2}$. Since $\gcd(n_1,n_2) = 1$, we have $a^{\frac{1}{2}\phi(m)} \equiv 1 \pmod n$. Thus, every a with $\gcd(a,m) = 1$ has order $\leqslant \frac{1}{2}\phi(m) < \phi(m)$, so there is no primitive root modulo m.

At last, suppose $m = 2^r$ with $r \geqslant 3$. Then the numbers relatively prime to m is odd. Claim. given an odd integer $a \geqslant 3$, we have $a^{2^{r-2}} \equiv 1 \pmod{2^r}$. So there is no primitive root modulo m. Claim. for any $r > 2$, $2^r \mid\mid (5^{2^{r-2}} - 1)$. Assume this is true for k. Then $2^k \mid\mid (5^{2^{k-2}} + 1)$. So $2^{k+1} \mid\mid (5^{2^{k-2}} - 1)(5^{2^{k-2}} + 1) = 5^{2^{k-1}} - 1$. Hence the claim is proved. This gives 5 has order 2^{r-2} modulo 2^r. So the residues 5^k with $k = 1, \ldots, 2^{r-2}$ are all distinct. Check the residues -5^k for $k = 1, \ldots, 2^{r-2}$ are distinct and distinct from 5^k's, so this gives all residues since $\phi(2^r) = 2^r - 2^{r-1} = 2^{r-1}$. Hence all **reduced** residues modulo 2^r can be written as $(-1)^l 5^k$ for $l = 0, 1,\ k = 1, \ldots, 2^{r-2}$. Note $\left((-1)^l 5^k\right)^{2^{r-2}} = (5^k)^{2^{r-2}} \equiv 1 \pmod{2^r}$. ☐

Corollary 2.132.

$$\begin{aligned}(\mathbb{Z}/p^r\mathbb{Z})^\times &\cong C_{\phi(p^r)},\ p \text{ odd},\\ (\mathbb{Z}/2\mathbb{Z})^\times &\cong C_1 = C_1,\\ (\mathbb{Z}/4\mathbb{Z})^\times &\cong C_2 = \mathbb{Z}/2\mathbb{Z},\\ (\mathbb{Z}/2^r\mathbb{Z})^\times &\cong C_2 \times C_{2^{r-2}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z},\ r \geqslant 3.\end{aligned}$$

Theorem 2.133. *Let* $m = 2^e \prod_{p^r || m, p>2} p^r$*. Then*

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong G \times \prod_{p^r || m, p>2} C_{\phi(p^r)},$$

where

$$G \cong \begin{cases} C_1, & e = 0, 1 \\ C_2, & e = 2 \\ C_2 \times C_{2^{e-2}} & e > 2 \end{cases}.$$

Proof. By Corollary 2.132 and Chinese Remainder Theorem. □

Chapter 3

Quadratic Reciprocity

Let p be prime.

3.1 Legendre symbol

Definition 3.1. Let $\gcd(a, m) = 1$. If $x^n \equiv a \pmod{m}$ has a solution, we say a is an n^{th} *power residue modulo* m. If $n = 2$, we say a is *quadratic residue* if this has a solution and *quadratic non-residue*, otherwise.

Definition 3.2. Let p be odd. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ is quadratic residue and } p \nmid a \\ -1, & a \text{ is not quadratic residue and } p \nmid a \\ 0, & p \mid a \end{cases}.$$

Theorem 3.3. *Let $p \nmid a$. Then the congruence $x^n \equiv a \pmod{p}$ is solvable if and only if $a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$.*

Proof. "$\Rightarrow$". Since $p \nmid x$, by Fermat's little theorem, we have $a^{\frac{p-1}{\gcd(n,p-1)}} \equiv (x^n)^{\frac{p-1}{\gcd(n,p-1)}} \equiv (x^{p-1})^{\frac{n}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$.

"$\Leftarrow$". Let g be a primitive root modulo p. Then $a \equiv g^r \pmod{p}$ for some $r \in \mathbb{N}$. We have $1 \equiv (g^r)^{\frac{p-1}{\gcd(n,p-1)}} \equiv g^{\frac{r(p-1)}{\gcd(n,p-1)}} \pmod{p}$. Then $\operatorname{ord}_p(g) = (p-1) \mid \frac{r(p-1)}{\gcd(n,p-1)}$. So $\gcd(n, p-1) \mid r$. Write $r = knx + k(p-1)y$ for some k, x, y. So $a \equiv g^r \equiv g^{knx+k(p-1)y} \equiv (g^{kx})^n \cdot (g^{p-1})^{ky} \equiv (g^{kx})^n \pmod{p}$. $\square$

Example 3.4. Is 3 a 4^{th} power modulo 17 ? Note $x^4 \equiv 3 \pmod{17}$ has a solution if and only if $3^{\frac{16}{\gcd(4,16)}} \equiv 1 \pmod{17}$ if and only if $3^4 \equiv 1 \pmod{17}$, not true.

Assumption 3.5. Let p be odd.

Theorem 3.6 (Euler' Criterion)**.**

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

Proof. If $p \mid a$, we are done. Assume $p \nmid a$. Then by Fermat's little theorem, $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$, i.e., $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. By Theorem 3.3, $a^{\frac{p-1}{2}} = a^{\frac{p-1}{\gcd(2,p-1)}} \equiv 1 \pmod{p}$ if and only if $\left(\frac{a}{p}\right) = 1$. □

Theorem 3.7. *(a)* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(b) If $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(c) If $\gcd(a,p) = 1$, *then* $\left(\frac{a^2}{p}\right) = 1$ *and* $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

(d) $\left(\frac{1}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Proof. (a) Since $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$ and $\left(\frac{ab}{p}\right), \left(\frac{a}{p}\right), \left(\frac{b}{p}\right) \in \{0, 1, -1\}$ and $p \geqslant 3$, we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Theorem 3.8. *The number of solutions of* $x^2 \equiv a \pmod{p}$ *is exactly* $1 + \left(\frac{a}{p}\right)$.

Proof. If x_0 is a solution, then $-x_0 \equiv p - x_0 \pmod{p}$ is also a solution. If $p \mid a$, then $x^2 \equiv a \pmod{p}$ only has one solution. □

Definition 3.9. Let $n \in \mathbb{N}$. Define the *numerically least residue of a modulo n* to be a' such that $a' \equiv a \pmod{n}$ and $-\frac{1}{2}n < a' \leqslant \frac{1}{2}n$.

Lemma 3.10 (Gauss's lemma)**.** Let $\gcd(a,p) = 1$. Write a_j to be numerically least residue of aj modulo p for $j \in \mathbb{N}$. Then $\left(\frac{a}{p}\right) = (-1)^l$, where

$$l = \#\left\{1 \leqslant j \leqslant \frac{p-1}{2} \;\middle|\; a_j < 0\right\}.$$

Proof. Claim. The numbers $\left\{|a_j|, 1 \leqslant j \leqslant \frac{p-1}{2}\right\}$ are the numbers $1, 2, \ldots, \frac{p-1}{2}$ in some order. By definition of a_j's, it's enough to show that $|a_j|$'s are distinct. Suppose first $a_j = a_k$ for some $j, k \in \{1, \cdots, \frac{p-1}{2}\}$ with $j \neq k$. This gives $aj \equiv ak \pmod{p}$. Since $\gcd(a,p) = 1$, we have $j \equiv k \pmod{p}$, a contradiction. Suppose $a_j = -a_k$ for some $j \neq k$. This gives $aj \equiv -ak \pmod{p}$, i.e., $a(j+k) \equiv 0 \pmod{p}$. Similarly, $g + k \equiv 0 \pmod{p}$, a contradiction. Write $r = \frac{p-1}{2}$. Then $(-1)^l r! = a_1 \cdots a_r \equiv (1a) \cdots (ra) \pmod{p}$, i.e., $r! a^r \equiv (-1)^l r! \pmod{p}$. Since $\gcd(r!, p) = 1$, we have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^r \equiv (-1)^l \pmod{p}$. □

Example 3.11. Since $4^2 \equiv 5 \pmod{11}$, we have $\left(\frac{5}{11}\right) = 1$. Note

j	aj	a_j
1	5	5
2	10	−1
3	15	4
4	20	−2
5	25	3

Then $l = 2$. So $\left(\frac{5}{11}\right) = (-1)^2 = 1$.

Corollary 3.12. Let $\gcd(a, 2p) = 1$, then $\left(\frac{a}{p}\right) = (-1)^l$, where $l = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$. Moreover, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. Consider $a, 2a, \ldots, \frac{p-1}{2}a$. Let $r_1, \ldots, r_n$ denote the residues of these ja's modulo p that exceed $\frac{p}{2}$, and $s_1, \ldots, s_k$ be the residues between 0 and $\frac{p}{2}$. Note $n + k = \frac{p-1}{2}$ and $\gcd(a, p) = 1$. Using $ja = p\left\lfloor \frac{ja}{p} \right\rfloor +$ remainder, we have

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j. \tag{3.1}$$

Since $\frac{p}{2} < r_i < p$, we have the numerically least residue of r_i is $r_i - p$ for $i = 1, \ldots, n$. By the proof in Gauss's lemma, we have the absolute value of numericlally residues, i.e., $(p - r_i)$'s and s_j's are all distinct and are the numbers $1, \ldots, \frac{p-1}{2}$ in some order.
Then

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j. \tag{3.2}$$

Let (3.1) - (3.2), we have $(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor - np + 2\sum_{j=1}^{n} r_j$, i.e.,

$$(a-1)\frac{p^2-1}{8} = p\left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n\right) + 2\sum_{j=1}^{n} r_j. \tag{3.3}$$

Since $\gcd(a, 2p) = 1$, a is odd. So $0 \equiv p\left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n\right) \pmod 2$. Since $\gcd(p, 2) = 1$, $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \equiv n \pmod 2$. By Gauss's lemma, we have $\left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor}$. Moreover, if $a = 2$, we have $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2j}{p} \right\rfloor = \sum_{j=1}^{\frac{p-1}{2}} 0 = 0$ and then $\frac{p^2-1}{8} \equiv -np \equiv n \pmod 2$ by 3.3. So by Gauss's lemma, we have $\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$. ☐

Remark. Take $a = -1$, since $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{-j}{p} \right\rfloor = \sum_{j=1}^{\frac{p-1}{2}}(-1) = -\frac{p-1}{2}$, we have $0 \equiv p\left(-\frac{p-1}{2} - n\right) \pmod 2$, i.e., $n \equiv -\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod 2$. Then

$$\left(\frac{-1}{p}\right) = (-1)^n = (-1)^{\frac{p-1}{2}}.$$

So if $p \equiv 1 \pmod 4$, then -1 is a square root modulo p; if $p \equiv 1 \pmod 4$, then not. Then

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}.$$

Theorem 3.13 (Quadratic reciprocity (QR)). *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. Let $S = \left\{(x,y) \in \mathbb{N}^2 \mid 1 \leqslant x \leqslant \frac{p-1}{2},\ 1 \leqslant y \leqslant \frac{q-1}{2}\right\}$. Let $S_1 = \{(x,y) \in S \mid qx > py\}$ and $S_2 = \{(x,y) \in S \mid qx < py\}$. Let $(x,y) \in S$. Suppose $qx = py$, then $p \mid qx$, i.e., $p \mid q$ or $p \mid x$, a contradiction. Hence $S = S_1 \sqcup S_2$. Also, $S_1 = \left\{(x,y) \in S \;\middle|\; 1 \leqslant x \leqslant \frac{p-1}{2}, 1 \leqslant y < \frac{qx}{p}\right\}$ and $S_2 = \left\{(x,y) \in S \;\middle|\; 1 \leqslant y \leqslant \frac{q-1}{2}, 1 \leqslant x < \frac{py}{q}\right\}$. So $\#S_1 = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$ and $\#S_2 = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$. Since $\#S = \#S_1 + \#S_2$, $\frac{p-1}{2}\frac{q-1}{2} = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$. Thus, since $\gcd(p, 2q) = 1 = \gcd(q, 2p)$, by Corollary 3.12, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{y=1}^{\frac{p-1}{2}} \lfloor \frac{py}{q} \rfloor} \cdot (-1)^{\sum_{x=1}^{\frac{q-1}{2}} \lfloor \frac{qx}{p} \rfloor} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Remark. $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$ by Theorem 2.52 if and only if $\left(\frac{-1}{p}\right) = 1$; $p = x^2 + 2y^2$ if and only if $\left(\frac{-2}{p}\right) = 1$.

Example 3.14.

$$\left(\frac{21}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{7}{71}\right) = (-1)^{\frac{3-1}{2}\frac{71-1}{2}}\left(\frac{71}{3}\right)(-1)^{\frac{7-1}{2}\frac{71-1}{2}}\left(\frac{71}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{7}\right) = (-1)^{\frac{3^2-1}{8}} \cdot 1 = 1.$$

Example 3.15. Since $\left(\frac{1}{3}\right) = 1$ and $\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \pmod 3 \\ -1 & p \equiv 2 \pmod 3 \end{cases}.$$

3.1.1 Algebraic number theory proof of QR

2 is a square modulo p if and only if $p \equiv 1, 7 \pmod 8$, i.e., $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. We already proved this, but we will give a new proof. Let $\xi_n = e^{\frac{2\pi i}{n}}$ be a primitive n^{th} root of unity in $\mathbb{C}$.

Definition 3.16. Set

$$\mathbb{Z}[\xi_n] = \{a_0 + a_1\xi_n + \cdots + a_{n-1}\xi_n^{n-1}\},$$

which is a ring.

Definition 3.17. Let $\mathcal{K}/\mathbb{Q}$ be a finite field extention. We say $\alpha \in \mathcal{K}$ is an *algebraic integer* if there exists a monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Fact 3.18. Show that the algebraic integer in $\mathbb{Q}$ are the ususal integers.

Notation 3.19. Denote the set of algebraic integers in $\mathcal{K}$ by $\mathcal{O}_{\mathcal{K}}$. So $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Theorem 3.20. *Every element of $\mathbb{Z}[\xi_n]$ is an algebraic integer. Moreover, $\mathbb{Z}[\xi_n] \cap \mathbb{Q} = \mathbb{Z}$.*

Proof. Let $\alpha \in \mathbb{Z}[\xi_n]$. Then we can write $\alpha\xi_n^i = \sum_{j=0}^{n-1} a_{ij}\xi_n^j$ for $i = 0, \ldots, n-1$. Define a matrix $A = (a_{ij}) \in \mathrm{Mat}_n(\mathbb{Z})$ and $P(t) = \det(tI_n - A) \in \mathbb{Z}[t]$, which is monic. Define $V = {}^t(1, \xi_n, \xi_n^2, \ldots, \xi_n^{n-1})$. Then the set of equations can be re-written as $AV = \alpha V$, which implies α is an eigenvalue of A. So α is a root of the monic polynomial $P \in \mathbb{Z}[t]$. □

Fact 3.21.

$$\mathcal{O}_{\mathbb{Q}(\xi_n)} = \mathbb{Z}[\xi_n].$$

Notation 3.22. For $x, y \in \mathbb{Z}[\xi_n]$, write $x \equiv y \pmod{p\mathbb{Z}[\xi_n]}$ to mean $x - y \in p\mathbb{Z}[\xi_n]$.

Fact 3.23. Since $\mathbb{Z} \subseteq \mathbb{Z}[\xi_n]$, if $x, y \in \mathbb{Z}$, $x \equiv y \pmod{p\mathbb{Z}[\xi_n]}$ is the same as $x \equiv y \pmod{p}$.

Theorem 3.24 (New proof)**.**

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof. Set $\xi = \xi_8$ and $\mathcal{O} = \mathbb{Z}[\xi_8]$. Then $0 = \xi^8 - 1 = (\xi^4 - 1)(\xi^4 + 1)$. Since ξ is primitive 8^{th} root of unity, we have $\xi^4 + 1 = 0$, i.e., $\xi^2 + \xi^{-2} = 0$. Set $\tau = \xi + \xi^{-1}$. Then $\tau^2 = (\xi + \xi^{-1})^2 = \xi^2 + 2 + \xi^{-2} = 2$. So $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\xi)$. By Euler's criterion, $\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$. So $\tau^{p-1} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p\mathcal{O}}$, i.e., $\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p\mathcal{O}}$.

(a) Assume $p \equiv 1 \pmod 8$. Then $\xi^p = \xi$ and $\xi^{-p} = \xi^{-1}$. So $\tau^p = (\xi + \xi^{-1})^p \equiv \xi^p + \xi^{-p} = \xi + \xi^{-1} = \tau \pmod{p\mathcal{O}}$. Thus, $\tau \equiv \left(\frac{2}{p}\right)\tau \pmod{p\mathcal{O}}$. Note $p\mathcal{O}$ is not prime ideal, so we can't just cancel τ. Multiply by τ, we have $\tau^2 \equiv \left(\frac{2}{p}\right)\tau^2 \pmod{p\mathcal{O}}$, i.e., $2 \equiv \left(\frac{2}{p}\right)2 \pmod{p\mathcal{O}}$. So $2 \equiv \left(\frac{2}{p}\right)2 \pmod{p}$ by Fact 3.23. Since $\gcd(p, 2) = 1$, $1 \equiv \left(\frac{2}{p}\right) \pmod{p}$. So $\left(\frac{2}{p}\right) = 1$.

(b) Assume $p \equiv -1 \pmod 8$. Then $\xi^p = \xi^{-1}$, $\xi^{-p} = \xi$. So everything else is the same and as a result, we have $\left(\frac{2}{p}\right) = 1$.

(c) Assume $p \equiv 3 \pmod 8$. Since $\xi^4 = -1$, we have

$$\tau^p \equiv \xi^p + \xi^{-p} \equiv \xi^3 + \xi^{-3} \equiv \xi^4\xi^{-1} + \xi^{-4}\xi \equiv -\xi^{-1} - \xi = -(\xi + \xi^{-1}) \equiv -\tau \pmod{p\mathcal{O}}.$$

So $-\tau \equiv \left(\frac{2}{p}\right)\tau \pmod{p\mathcal{O}}$. Multiply by τ, we have $-2 \equiv \left(\frac{2}{p}\right)2 \pmod{p}$. Similarly, $\left(\frac{2}{p}\right) = -1$.

(d) Assume $p \equiv -3 \pmod 8$. Then $\xi^p = \xi^{-3}$ and $\xi^{-p} = \xi^3$. So everything else is the same and as a result, we have $\left(\frac{2}{p}\right) = -1$. □

Remark. We calculate $\left(\frac{2}{p}\right)$ using algebraic number theorem. Main input: $\tau = \xi_p + \xi_p^{-1}$, $\tau^2 = 2$ and $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\xi_8)$. These are enough information to calculate $\left(\frac{2}{p}\right)$.

Remark. To prove QR, we need to consider $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$. Want to do the same type of argument in $\mathbb{Q}(\xi_8)$, so we want some $\tau \in \mathbb{Z}[\xi_p]$ so that $\tau^2 = p$. Unfortunately, this isn't always possible. Since $\xi_8 = \frac{1-\sqrt{-3}}{2}$ and $\sqrt{-3} = 1 - 2\xi_8$, $\mathbb{Q}(\xi_8) = \mathbb{Q}(\sqrt{-3})$. So there can be no element $\tau \in \mathbb{Z}[\xi_8] \subseteq \mathbb{Q}(\xi_8)$ satisfying $\tau^2 = 3$ since we would get $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{-3})$, a contradiction. Thus, we can find τ such that in general, the best we can hope for is to find $\tau \in \mathbb{Z}[\xi_p]$ such that $\tau^2 = \pm p$.

Proposition 3.25. There are the same number of quadratic residue as non-residue in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let ϖ be an primitive root modulo p. Then $\varpi, \dots, \varpi^{p-1}$ are distinct. Let $k \in \{1, \cdots, p-1\}$ be odd. Suppose $(\varpi^j)^2 \equiv \varpi^k \pmod p$ for some $j \in \{1, \dots, p-1\}$. Since $\gcd(\varpi, p) = 1$, $\varpi^{2j-k} \equiv 1 \pmod p$. Also, since $\mathrm{ord}_p(\varpi) = p-1$, we have $p-1 \mid 2j-k$. Since $2j-k \leqslant 2j-1 \leqslant 2(p-1)-1 < 2(p-1)$, we have $2j-k = p-1$, contradicted by k is odd. Hence ϖ^k if a quadractic residue if and only if k is even. □

Definition 3.26. Define a Gauss sum

$$\tau = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \xi_p^t = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \xi_p^t.$$

Theorem 3.27.

$$\tau^2 = (-1)^{\frac{p-1}{2}} p.$$

Proof. Define $\tau_q = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \xi_p^{qt}$ for $q = 1, \cdots, p-1$. Then by Proposition 3.25, $\tau_0 = 0$. So $\left(\frac{q}{p}\right) \tau_q = \sum_{t=1}^{p-1} \left(\frac{qt}{p}\right) \xi_p^{qt} = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \xi_p^t = \tau$ since $\{q, 2q, \cdots, (p-1)q\}$ is a complete reduced residue system modulo p. Since $p \nmid q$, we have $\left(\frac{q}{p}\right)^2 = 1$ and then $\tau_q = \left(\frac{q}{p}\right) \tau$. Hence

$$\sum_{q=1}^{p-1} \tau_q \tau_{-q} = \sum_{q=1}^{p-1} \left(\frac{-q^2}{p}\right) \tau^2 = \sum_{q=1}^{p-1} \left(\frac{-1}{p}\right) \tau^2 = \sum_{q=1}^{p-1} (-1)^{\frac{p-1}{2}} \tau^2 = (-1)^{\frac{p-1}{2}} (p-1) \tau^2.$$

Moreover,

$$\tau_q \tau_{-q} = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \xi_p^{qt} \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \xi_p^{-qs} = \sum_{t=1}^{p-1} \sum_{s=1}^{p-1} \left(\frac{t}{p}\right) \left(\frac{s}{p}\right) \xi_p^{q(t-s)}.$$

Note for $1 \leqslant t, s \leqslant p-1$, if $t = s$, then $\sum_{q=0}^{p-1} \xi_p^{q(t-s)} = p$; if $t \neq s$, then since $2-p \leqslant t-s \leqslant p-2$, we have $p \nmid t-s$ and so $\sum_{q=0}^{p-1} \xi_p^{q(t-s)} = \sum_{q=0}^{p-1} \xi_p^q = \frac{1-\xi_p^p}{1-\xi_p} = 0$. Hence

$$\sum_{q=0}^{p-1} \tau_q \tau_{-q} = \sum_{q=0}^{p-1} \left(\sum_{t=1}^{p-1} \sum_{s=1}^{p-1} \left(\frac{t}{p}\right) \left(\frac{s}{p}\right) \xi_p^{q(t-s)} \right) = \sum_{t=1}^{p-1} \sum_{s=1}^{p-1} \left(\frac{t}{p}\right) \left(\frac{s}{p}\right) \sum_{q=0}^{p-1} \xi_p^{q(t-s)} = \sum_{t=1}^{p-1} 1 \cdot p = p(p-1).$$

Thus, $p(p-1) = (-1)^{\frac{p-1}{2}} (p-1) \tau^2$. i.e., $(-1)^{\frac{p-1}{2}} p = \tau^2$. □

Theorem 3.28 (QR: New Proof)**.** *Let p, q be distinct odd primes.*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Proof. Set $p^* = (-1)^{\frac{p-1}{2}} p$. Since Gauss sum $\tau \in \mathbb{Z}[\xi_p] \subseteq \mathbb{Q}(\xi_p)$ and $\tau^2 = p^*$, $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\xi_p)$. So

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Hence $\left(\frac{p^*}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Thus, to show QR, it is equivalent to show $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. Note $\tau^{q-1} = (\tau^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod q$ by Euler's criterion. Then $\tau^q \equiv \left(\frac{p^*}{q}\right)\tau \pmod q$. Since $q \nmid p$ is odd and by Freshmen's dream, we have

$$\tau^q = \left(\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\xi_p^t\right)^q \equiv \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)^q \xi_p^{qt} = \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\xi_p^{qt} \pmod{q\mathbb{Z}[\xi_p]}.$$

Let $\widetilde{q}$ for the inverse of q modulo p. Let $qt \equiv k \pmod p$, then $t \equiv \widetilde{q}k \pmod p$ and so

$$\left(\frac{p^*}{q}\right)\tau \equiv \tau^q = \sum_{k=0}^{p-1}\left(\frac{\widetilde{q}k}{p}\right)\xi_p^k = \left(\frac{\widetilde{q}}{p}\right)\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)\xi_p^k \equiv \left(\frac{\widetilde{q}}{p}\right)\tau \pmod{q\mathbb{Z}[\xi_p]}.$$

Since $\left(\frac{\widetilde{q}}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{\widetilde{q}q}{p}\right) = \left(\frac{1}{p}\right) = 1$, we have $\left(\frac{\widetilde{q}}{p}\right) = \left(\frac{q}{p}\right)$. So $\left(\frac{p^*}{q}\right)\tau \equiv \left(\frac{q}{p}\right)\tau \pmod{q\mathbb{Z}[\xi_p]}$. Hence $\left(\frac{p^*}{q}\right)\tau^2 \equiv \left(\frac{q}{p}\right)\tau^2 \pmod{q\mathbb{Z}[\xi_p]}$, i.e., $\left(\frac{p^*}{q}\right)p^* \equiv \left(\frac{q}{p}\right)p^* \pmod q$. Since $\gcd(p^*, q) = 1$, $\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod q$. Thus, $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. □

3.2 Jacobi symbol

Definition 3.29. Let $n \in \mathbb{N}$ be odd, the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined as the product of the Legendre symbols corresponding to the prime factors of n, i.e.,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\cdots\left(\frac{a}{p_r}\right)^{e_r},$$

where $n = p_1^{e_1}, \cdots p_r^{e_r}$ is the canonical factorization of n.

Theorem 3.30. *Let $Q = p_1 \cdots p_s$, where p_i's are odd primes and not necessarily distinct. Then*

(a) $\left(\frac{a}{1}\right) = 1$.

(b) If $\gcd(a, Q) \neq 1$, *then* $\left(\frac{a}{Q}\right) = 0$.

(c) If $\gcd(a, Q) = 1$, *then* $\left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_s}\right)$.

Remark. This symbol does not tell you about quadratic residues.

Theorem 3.31. *Let $Q, Q' \in \mathbb{N}$ be odd.*

(a) $\left(\frac{p}{Q}\right)\left(\frac{p}{Q'}\right) = \left(\frac{p}{QQ'}\right)$.

(b) $\left(\frac{p}{Q}\right)\left(\frac{p'}{Q}\right) = \left(\frac{pp'}{Q}\right)$.

(c) If $\gcd(p, Q) = 1$, *then* $\left(\frac{p}{Q^2}\right) = \left(\frac{p^2}{Q}\right) = 1$.

(d) If $\gcd(pp', QQ') = 1$*, then* $\left(\frac{p'p^2}{Q'Q^2}\right) = \left(\frac{p'}{Q'}\right)$.

(e) If $p \equiv p' \pmod{Q}$*, then* $\left(\frac{p}{Q}\right) = \left(\frac{p'}{Q}\right)$.

Proof. (a) Write $Q = p_1 \cdots p_s$ and $Q = p'_1, \cdots, p'_t$ with p_i's and p_i's odd primes. Then we have $\left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_s}\right) \left(\frac{p}{p'_1}\right) \cdots \left(\frac{p}{p'_t}\right) = \left(\frac{p}{QQ'}\right)$. □

Remark. The Jacobi symbol does not determine if something is residue modulo Q. For example, if $7 \nmid a$, then $\left(\frac{a}{49}\right) = \left(\frac{a}{7^2}\right) = \left(\frac{a}{7}\right)\left(\frac{a}{7}\right) = 1$. But not every a is a QR modulo 49. On the other hand, if $\left(\frac{a}{Q}\right) = -1$, then $-1 = \left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_s}\right)$, which means at least one of these must be -1, say $\left(\frac{a}{p_j}\right) = -1$. Suppose $x^2 \equiv a \pmod{Q}$, then since $p_j \mid Q$, we have $x^2 \equiv a \pmod{p_j}$, as well, which is a contradiction since $\left(\frac{a}{p_j}\right) = -1$. So if $\left(\frac{a}{Q}\right) = -1$, it means there is no solution for $x^2 \equiv a \pmod{Q}$.

Theorem 3.32. *Let* $Q \in \mathbb{N}$ *be odd, then*

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}} \text{ and } \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}.$$

Proof. Write $Q = p_1 \cdots p_s$ with p_i's odd prime. Then

$$\left(\frac{-1}{Q}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_s}\right) = (-1)^{\frac{p_1-1}{2}} \cdots (-1)^{\frac{p_s-1}{2}} = (-1)^{\sum_{j=1}^{s} \frac{p_j-1}{2}}.$$

Let n_1 and n_2 be odd. Then

$$\frac{1}{2}(n_1-1) + \frac{1}{2}(n_2-1) = \frac{1}{2}(n_1n_2-1) - \frac{1}{2}(n_1-1)(n_2-1) \equiv \frac{1}{2}(n_1n_2-1) \pmod{2}.$$

Hence by induction, $\left(\frac{-1}{Q}\right) = (-1)^{\frac{1}{2}(p_1\cdots p_s-1)} = (-1)^{\frac{1}{2}(Q-1)}$. Note

$$\left(\frac{2}{Q}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_s}\right) = (-1)^{\frac{p_1^2-1}{8}} \cdots (-1)^{\frac{p_s^2-1}{8}} = (-1)^{\sum_{j=1}^{s} \frac{p_j^2-1}{8}}.$$

Let n_1 and n_2 be odd. Since $n_1^2 \equiv 1 \equiv n_2^2 \pmod{4}$, $\frac{1}{8}(n_1^2-1)(n_2^2-1) \equiv 0 \pmod{2}$. This gives

$$\frac{1}{8}(n_1^2-1) + \frac{1}{8}(n_2^2-1) = \frac{1}{8}(n_1^2n_2^2-1) - \frac{1}{8}(n_1^2-1)(n_2^2-1) \equiv \frac{1}{8}(n_1^2n_2^2-1) \pmod{2}.$$

Hence by induction, $\left(\frac{2}{Q}\right) = (-1)^{\frac{1}{8}(p_1^2\cdots p_s^2-1)} = (-1)^{\frac{1}{8}(Q^2-1)}$. □

Theorem 3.33 (Jacobi)**.** *Let* $Q \in \mathbb{N}$ *be odd and* $\gcd(p, Q) = 1$. *Then*

$$\left(\frac{p}{Q}\right)\left(\frac{Q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{Q-1}{2}}.$$

Proof. Use the same techniques as Theorem 3.32. □

Remark. We can use Jacobi to quickly calculate Legendre symbol.

Example 3.34.

$$\begin{aligned}\left(\frac{1111}{8093}\right) &= (-1)^{\frac{1}{4}8092\cdot 1110}\left(\frac{8093}{1111}\right) = \left(\frac{316}{1111}\right) = \left(\frac{2}{1111}\right)^2\left(\frac{79}{1111}\right) = (-1)^{\frac{1}{4}78\cdot 1110}\left(\frac{1111}{79}\right)\\ &= -\left(\frac{5}{79}\right) = -(-1)^{\frac{1}{4}4\cdot 78}\left(\frac{79}{5}\right) = -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)^2 = -1.\end{aligned}$$

So 1111 is not a quadratic residue modulo 8093.

Remark. Sum of squares: arithemetric in $\mathbb{Z}[i]$. Quadratic reciprocity: arithemetric in $\mathbb{Z}[\xi_p]$. Binary quadratic: arithemetric in $\mathbb{Q}(\sqrt{d})$.

Chapter 4

Binary Quadratic Residue

Definition 4.1. A *binary quadratic form* is a homogeneous polynomial

$$f : ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y].$$

We will sometimes denote this as $[a, b, c]$. Given n, we say f reresents n if there exists $(x_0, y_0) \in \mathbb{Z}^2$ such that $f(x_0, y_0) = n$.

Remark. Classical motivation: Figure out which integers are represented by a given form. We have an example already.

Theorem 4.2. *Let $f = x^2 + y^2$. Then an integer n is represented by f if and only if n has a prime factorization*

$$n = 2^e \prod_{p_j \equiv 1 \pmod 4} p_j^{e_j} \prod_{q_i \equiv 3 \pmod 4} q_i^{h_i},$$

where $h_i \equiv 0 \pmod 2$ for all $q_i \mid n$ and $q_i \equiv 3 \pmod 4$.

Proof. By Theorem 2.53. □

Theorem 4.3. *$f = x^2 + y^2$ and $g = x^2 + 2xy + 2y^2$ represent the same integers.*

Proof. If $n = g(x_0, y_0) = x_0^2 + 2x_0y_0 + 2y_0^2$, then $n = f(x_0 + y_0, y_0)$. If $n = f(x_1, y_1) = x_1^2 + y_1^2$, then $n = g(x_1 - y_1, y_1)$. □

Corollary 4.4. Let $f = x^2 + 2xy + 2y^2$. Then an integer n is represented by f if and only if n has a prime factorization

$$n = 2^e \prod_{p_j \equiv 1 \pmod 4} p_j^{e_j} \prod_{q_i \equiv 3 \pmod 4} q_i^{h_i},$$

where $h_i \equiv 0 \pmod 2$ for all $q_i \mid n$ and $q_i \equiv 3 \pmod 4$.

Remark. We should think of f and g above as equivalent binary quadratic forms (b.q.f.'s). Note $f(x, y) = (x, y) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = (x, y) \begin{bmatrix} x \\ y \end{bmatrix} = x^2 + y^2$ and $g(x, y) = (x, y) \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = x^2 + 2xy + 2y^2$. We could ask for the matrices to be similar: ${}^t \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ by elementary transformation. Maybe what we want is the matrices associated to f and g to be similar matrices.

Definition 4.5. Given any $f = ax^2 + bxy + cy^2 = (x, y) \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$, associate the *matrix*

$$\begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}.$$

Assumption 4.6. Let f, g be binary quadratic forms.

Definition 4.7. We say f and g are *equivalent* if the associated matrices are $\mathrm{SL}_2(\mathbb{Z})$-similar.

Remark. We can define an action γ of $\mathrm{SL}_2(\mathbb{Z})$ on the set of binary quadratic forms f by

$$f|\gamma(x, y) = (f \circ \gamma)(x, y) = f(\gamma(x, y)) = f\left(\gamma \begin{bmatrix} x \\ y \end{bmatrix}\right),$$

when regarding γ as a matrix. For example, let $\gamma = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$. Then $\gamma \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} px + qy \\ rx + sy \end{bmatrix}$ and $f\left(\gamma \begin{bmatrix} x \\ y \end{bmatrix}\right) = f(px + qy, rx + sy)$. Check this gives a right group action.

Definition 4.8. We say f and g are *similar*, write $f \sim g$ if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $f = g \circ \gamma$.

Exercise 4.9. Definitions 4.7 and 4.8 are equivalent.

Theorem 4.10. *If $f \sim g$, then f and g represent the same set of integers.*

Proof. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $g = f \circ \gamma$. Let $\tau \in \mathrm{SL}_2(\mathbb{Z})$ such that $f = g \circ \tau$. Let $(x_0, y_0) \in \mathbb{Z}^2$ such that $f(x_0, y_0) = n$. Then $g\big(\gamma^{-1}(x_0, y_0)\big) = f\big(\gamma(\gamma^{-1}(x_0, y_0))\big) = f(x_0, y_0) = n$. Let $(x_1, y_1) \in \mathbb{Z}^2$ such that $g(x_1, y_1) = m$. Then $f\big(\tau^{-1}(x_1, y_1)\big) = g\big(\tau(\tau^{-1}(x_1, y_1))\big) = g(x_1, y_1) = m$. □

Example 4.11. Consider the binary quadratic form $f = [458, 214, 25]$. Note $f(-1, -1) = 17 \cdot 41$, $f(-1, 0) = 2 \cdot 229$, $f(0, 1) = 5^2$, $f(1, 1) = 269$, $f(-1, 2) = 2 \cdot 5 \cdot 13$, $f(-1, 3) = 41$. Check: Let $\gamma = \begin{bmatrix} 4 & -3 \\ -17 & 13 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then $(f \circ \gamma)(x, y) = x^2 + y^2$.

Definition 4.12. The *discriminant* of a binary quadratic form $f = [a, b, c]$ is $b^2 - 4ac$. Write

$$\mathrm{disc}(f) = b^2 - 4ac.$$

Remark. Note

$$\mathrm{disc}([a, b, c]) = -4 \begin{vmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{vmatrix}.$$

Theorem 4.13. *If $f \sim g$, then* $\mathrm{disc}(f) = \mathrm{disc}(g)$.

Proof. Let $g = f \circ \gamma$. View the corresponding matrices, $\mathrm{disc}(g) = \mathrm{disc}(f \circ \gamma) = \det(\gamma)\,\mathrm{disc}(f)\det(\gamma) = \mathrm{disc}(f)$. □

Remark. The converse is not true. $x^2 + 6y^2$ represents 1, $2x^2 + 3y^2$ does not represent 1 but they have same determinant -24.

Theorem 4.14. *The set of all discriminants of binary quadratic forms is exactly the set of integers d such that $d \equiv 0, 1 \pmod 4$.*

Proof. Let $f = [a, b, c]$. Then $d = b^2 - 4ac$. So $d \equiv b^2 \pmod 4$. Hence $d \equiv 0, 1 \pmod 4$. Next, assume $d \equiv 0, 1 \pmod 4$. Then $d = b^2$ for some b by Lemma 2.52. Set $f(x) = bxy$. $\square$

Theorem 4.15. *If* $\operatorname{disc}(f) < 0$*, then f is a definite form. If* $\operatorname{disc}(f) > 0$*, then f is an indefinite form.*

Proof. Set $c = \begin{cases} -\frac{d}{4} & \text{if } d \equiv 0 \pmod 4 \\ -\frac{d-1}{4} & \text{if } d \equiv 1 \pmod 4 \end{cases}$. When $c = -\frac{d}{4}$, $[1, 0, c]$ has disciminant d; when $c = -\frac{d-1}{4}$, $[1, 1, c]$ has disciminant d. The forms $\left[1, 0, -\frac{d}{4}\right]$ and $\left[1, -1, -\frac{d-1}{4}\right]$ are the principal binary quadratic forms of disciminant d. Consider $f = [a, b, c]$. Then $4af = 4a(ax^2 + bxy + cy^2) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - \operatorname{disc}(f)y^2$.

(a) If $\operatorname{disc}(f) < 0$, then $4ac = b^2 - \operatorname{disc}(f) > 0$, i.e., $ac > 0$. Also, $f \neq 0$ except $(x, y) = (0, 0)$. So f is positive (negative) definite if $a > 0$ $(a < 0)$.

(b) If $\operatorname{disc}(f) > 0$, then $f(1, 0) = a$ and $f(b, -2a) = -a \cdot \operatorname{disc}(f)$, which have opposite sign unless $a = 0$; similarly, $f(0, 1) = c$ and $f(-2c, b) = -c \cdot \operatorname{disc}(f)$, which have opposite sign unless $c = 0$. When $a = 0 = c$, we have $f(1, 1) = b \neq 0$ and $f(1, -1) = -b \neq 0$, which have opposite sign. Thus, f is indefinite.

(c) Assume $\operatorname{disc}(f) = 0$. If $a \neq 0$, since $f(b, -2a) = 0$, $f = \frac{(2ax+by)^2}{4a}$ is semidefinite. If $a = 0$, then $b = 0$ and then $f(x, y) = cy^2$, since $f(1, 0) = 0$, f is semidefinite. $\square$

Assumption 4.16. Let D be a square-free integer.

Definition 4.17. Set the field

$$\mathcal{K} = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Definition 4.18. The *ring of integer* of $\mathcal{K}$ is

$$\mathcal{O}_{\mathcal{K}} = \{a \in \mathcal{K} \mid a \text{ is integral over } \mathbb{Z}\} = \{a \in \mathcal{K} \mid a \text{ is a root of } f, f \in \mathbb{Z}[x] \text{ is monic}\}.$$

Fact 4.19. The map $\tau : \mathcal{K} \to \mathcal{K}$ given by $a + b\sqrt{D} \mapsto a - b\sqrt{D}$ is an isomorphism of fields.

Remark. Observe $\mathcal{K}$ as a 2-dimensional $\mathbb{Q}$-vector space with a basis $\{1, \sqrt{D}\}$. For example, let $\beta = a + b\sqrt{D} \in \mathcal{K}$ with $a, b \in \mathbb{Q}$. Define $\tau_\beta : \mathcal{K} \to \mathcal{K}$ by $x \mapsto \beta x$. Then $\tau_\beta \in \operatorname{Hom}_{\mathbb{Q}}(\mathcal{K}, \mathcal{K})$. Note $\tau_\beta(1) = a + b\sqrt{D}$ and $\tau_\beta(\sqrt{D}) = (a + b\sqrt{D})\sqrt{D} = bD + a\sqrt{D}$. So the matrix of τ_β is $m_\beta = \begin{bmatrix} a & bD \\ b & a \end{bmatrix}$. Since $\tau(\beta) = \overline{\beta}$, $\det(m_\beta) = a^2 - b^2D = \beta\overline{\beta} = \beta \cdot \tau(\beta) =: \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\beta)$. Also, $\operatorname{Tr}(m_\beta) = 2a = \beta + \overline{\beta} =: \operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(\beta)$. The characteristic polynomial of the action of β is

$$\begin{aligned} C_{m_\beta}(x) = \det(x \cdot I_2 - m_\beta) &= \det \begin{bmatrix} x - a & -bD \\ -b & x - a \end{bmatrix} = (x - a)^2 - b^2D \\ &= x^2 - 2ax + a^2 - b^2D = x^2 - \operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(\beta)x + \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\beta). \end{aligned}$$

Since $C_{m_\beta}(x) = (x - a)^2 - b^2D$, $C_{m_\beta}(a \pm b\sqrt{D}) = 0$.

Theorem 4.20. *Set* $\alpha = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \\ \sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \end{cases}$. *Then*

$$\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\alpha] := \{a + b\alpha \mid a, b \in \mathbb{Z}\} = (1, \alpha)\mathbb{Z}.$$

Proof. "$\supseteq$". Method 1: Let $y = a + b\alpha \in \mathbb{Z}[\alpha]$. Left to consider $\alpha = \frac{1+\sqrt{D}}{2}$. Then $\tau_y(1) = a + b\frac{1+\sqrt{D}}{2} = a + \frac{b}{2} + \frac{b}{2}\sqrt{D}$ and $\tau_y(\sqrt{D}) = \left(a + b\frac{1+\sqrt{D}}{2}\right)\sqrt{D} = \frac{bD}{2} + \left(a + \frac{b}{2}\right)\sqrt{D}$. So $m_y = \begin{bmatrix} a + \frac{b}{2} & \frac{b}{2} \\ \frac{bD}{2} & a + \frac{b}{2} \end{bmatrix}$. Note

$$\begin{aligned} C_{m_y}(x) = \det(x \cdot I_2 - m_y) &= \left(x - a - \frac{b}{2}\right)^2 - \frac{b^2 D}{4} \\ &= x^2 - (2a+b)x + a^2 + ab + \frac{1-D}{4}b^2 = x^2 - \operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(y) + \operatorname{N}_{\mathcal{K}/\mathbb{Q}}(y). \end{aligned}$$

Also, $C_{m_y}\left(a + \frac{b}{2} \pm \frac{b\sqrt{D}}{2}\right) = C_{m_y}\left(a + b\frac{1\pm\sqrt{D}}{2}\right) = 0$, so $C_{m_y}(a + b\alpha) = 0$. Hence $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{\mathcal{K}}$.

Method 2. Let $y = a + b\alpha \in \mathbb{Z}[\alpha]$. Use a theorem, to show $y \in \mathcal{O}_{\mathcal{K}}$, it suffices to show $\operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(y),\ \operatorname{N}_{\mathcal{K}/\mathbb{Q}}(y) \in \mathbb{Z}$. Note

$$\operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha) = \begin{cases} 1 & \text{if } D \equiv 1 \pmod 4 \\ 0 & \text{if } D \not\equiv 1 \pmod 4 \end{cases} \in \mathbb{Z} \text{ and } \operatorname{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) = \begin{cases} \frac{1-D}{4} & \text{if } D \equiv 1 \pmod 4 \\ -D & \text{if } D \not\equiv 1 \pmod 4 \end{cases} \in \mathbb{Z}\,.$$

So

$$\operatorname{Tr}(\mathcal{K}/\mathbb{Q})(y) = \operatorname{Tr}(\mathcal{K}/\mathbb{Q})(a + b\alpha) = \operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(a) + \operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(b\alpha) = 2a + b\begin{cases} 1 & \text{if } D \equiv 1 \pmod 4 \\ 0 & \text{if } D \not\equiv 1 \pmod 4 \end{cases} \in \mathbb{Z},$$

and

$$\operatorname{N}_{\mathcal{K}/\mathbb{Q}}(y) = (a + b\alpha)(a + b\overline{\alpha}) = a^2 + ab(\alpha + \overline{\alpha}) + b^2\alpha\overline{\alpha} = a^2 + ab\operatorname{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha) + b^2\operatorname{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}.$$

Thus, $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{\mathcal{K}}$.

"$\subseteq$". Let $x = a + b\sqrt{D} \in \mathcal{O}_{\mathcal{K}}$ with $a, b \in \mathbb{Q}$. Then $c_{m_x}(t) = t^2 - 2at + (a^2 - b^2)D$. Also, $2a = \operatorname{Tr}(\mathcal{K}_{\mathbb{Q}})(x) \in \mathbb{Z}$ and $a^2 - b^2 D = \operatorname{N}_{\mathcal{K}_{\mathbb{Q}}}(x) \in \mathbb{Z}$. So $a = \frac{a'}{2}$ for some $a' \in \mathbb{Z}$. Then $\left(\frac{a'}{2}\right)^2 - b^2 D \in \mathbb{Z}$. So $a'^2 - (2b)^2 D \in \mathbb{Z}$. Hence $(2b)^2 D \in \mathbb{Z}$. Since $D \in \mathbb{Z}$ is square-free, the denominator of b is 1 or 2.

(a) If the denominator of b is 1, then the denominator of a is 1 since $a^2 - b^2 D \in \mathbb{Z}$. So $a, b \in \mathbb{Z}$. Hence we can write $x = \begin{cases} (a-b) + 2b\frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \\ a + b\sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \end{cases}$.

(b) Similarly, if the denominator of b is 2, then the denominator of a is 2. So $a - b \in \mathbb{Z}$. Since $2b \in \mathbb{Z}$ is odd and $(a')^2 \equiv (2b)^2 D \pmod 4$, D is a perfect square modulo 4. So $D \equiv 1 \pmod 4$. Thus, $x \in \mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{D}}{2}$, i.e., $x = (a-b) + (2b)\frac{1+\sqrt{D}}{2}$. □

Example 4.21. $\mathcal{O}_{\mathbb{Q}\sqrt{-1}} = \mathbb{Z}[i]$ and $\mathcal{O}_{\mathbb{Q}\sqrt{5}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Definition 4.22. Let $\mathcal{K} = \mathbb{Q}(\sqrt{D})$. Define

$$\operatorname{disc}(\mathcal{K}) := \begin{cases} D & \text{if } D \equiv 1 \pmod 4 \\ 4D & \text{if } D \not\equiv 1 \pmod 4). \end{cases}.$$

Remark. We will see there is a bijection between certain equivalence classes of ideals in $\mathcal{O}_{\mathcal{K}}$, $\mathcal{K}$ discriminant d (positive definite) and equivalence classes of binary quadratic forms of discriminant d.

Example 4.23. The minimal polynomial of $\mathbb{Q}(\sqrt{-1})$ is $f = x^2 + 1 = [1, 0, 1]$. Then $\operatorname{disc}(f) = -4$. Note $\operatorname{disc}(\mathbb{Q}(\sqrt{-1})) = -4$.

Definition 4.24. A positive definite binary quadratic form $[a, b, c]$ is *reduced* if $|b| \leqslant a \leqslant c$ and if $|b| = a$ or $a = c$, then $b \geqslant 0$.

Remark. If $|b| \leqslant a \leqslant c$, then $D = \operatorname{disc}[a, b, c] = b^2 - 4ac < 0$.

Example 4.25. $x^2 + y^2$ is reduced, but $2x^2 + y^2$ is not reduced.

Remark. Let $[a, b, c]$ be reduced. Set $\tau = \frac{-b+\sqrt{D}}{2a}$. Then τ is a root of $ax^2 + bx + c$, and has positive imaginary part. So $\tau \in \mathfrak{H} := \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$.

Fact 4.26. We have a right action of $\mathrm{SL}_2(\mathbb{Z})$ on binary quadratic forms. This corresponds to a left action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$ by linear fractional transformation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az + b}{cz + d}.$$

Definition 4.27. The *fundamental domain* for the group action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$ is

$$\mathfrak{F} = \left\{ z \in \mathfrak{H} \;\middle|\; \operatorname{Re}(z) \in \left[-\frac{1}{2}, \frac{1}{2} \right) ; |z| > 1 \text{ or } |z| = 1 \text{ and } \operatorname{Re}(z) \leqslant 0 \right\}.$$

This means everything in $\mathfrak{H}$ is equivalent under the group action of $\mathrm{SL}_2(\mathbb{Z})$ to exactly one element in the upper half plane $\mathfrak{F}$ and no two elements in $\mathfrak{F}$ are equivalent.

Theorem 4.28. *$[a, b, c]$ is reduced if and only if $\tau \in \mathfrak{F}$.*

Proof. "⇒". If $[a, b, c]$ is reduced, then since $|b| \leqslant a$, $\operatorname{Re}(\tau) = -\frac{b}{2a} \in \left[-\frac{1}{2}, \frac{1}{2}\right)$. Since $0 < a \leqslant c$, $|\tau| = \sqrt{\frac{b^2}{4a^2} + \frac{-D}{4a^2}} = \sqrt{\frac{b^2+4ac-b^2}{4a^2}} = \sqrt{\frac{c}{a}} \geqslant 1$. If $|\tau| = 1$, then $b \geqslant 0$, so $\operatorname{Re}(\tau) \leqslant 0$.

"⇐". Reverse the argument. □

Theorem 4.29. *There is exactly one reduced form in each equivalence class of positive definite binary quadratic form ($a > 0, D < 0$).*

Proof.
- Step 1: Claim. Each equivalence class contains a reduced form. Let ζ be an equivalence class of positive definite binary quadratic forms of discriminant D. Let $[a, b, c] \in \zeta$ with minimal a. Note ${}^t\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & -\frac{b}{2} \\ \frac{b}{2} & a \end{bmatrix}$ or $g(x, y) = f|\gamma(x, y) = f(px+qy, rx+sy) = f(-y, x)$, where $p = 0, q = -1, r = 1, s = 0$. If $c > a$, then $[a, b, c] \sim [c, -b, a] \in \zeta$, a

contradiction since a is the minimal. So $a \leqslant c$. Apply $\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with $k = \lfloor \frac{a-b}{2a} \rfloor$, then we have $g(x,y) = ax^2 + (2ak+b)xy + (ak^2+bk+c)y^2$. Since $k \in \left(\frac{a-b}{2a} - 1, \frac{a-b}{2a}\right]$, we have $2ak + b \in (-a, a]$. Note (two ways to see it) $a \leqslant ak^2 + ak + c$. So $|2ak+b| \leqslant a \leqslant ak + bk + c$. Hence $[a, 2ak+b, ak^2+bk+c] \in \zeta$ is a reduced form. When $a = ak^2+bk+c$, but $2ak+b < 0$, then we can apply $\gamma = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ to get a reduced form $[ak+bk+c, -2ak-b, a] \in \zeta$.

- Step 2: Assume $[a,b,c] \in \zeta$ is a reduced form. Claim. There is only one reduced form in each equivalence class. Suppose there exists another reduced form $[a', b', c'] \in \zeta$. Then there exists $\gamma = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $[a,b,c] \begin{bmatrix} p & q \\ r & s \end{bmatrix} = [a', b', c']$ with $a' = ap^2 + bpr + cr^2$. Since $ps - qr = 1$, $\gcd(p, r) = 1$. Note

  $$a' = ap^2 + bpr + cr^2 = ap^2\left(1 + \frac{b}{a}\frac{r}{p}\right) + cr^2 = ap^2 + cr^2\left(1 + \frac{b}{c}\frac{p}{r}\right).$$

  If $p = 0$, then $r \neq 0$ and $a' = cr^2 \geqslant c \geqslant a$.
  Assume now $p \neq 0$.

  (a) Assume $\left|\frac{r}{p}\right| \leqslant 1$. Then $1 + \frac{b}{a}\frac{r}{p} \geqslant 0$. So $a' \geqslant cr^2 \geqslant a$.

  (b) Assume $\left|\frac{r}{p}\right| > 1$. Then $0 < \left|\frac{p}{r}\right| < 1$. So $1 + \frac{b}{c}\frac{p}{r} \geqslant 0$. Since $p \neq 0$, $a' \geqslant ap^2 \geqslant a$.

  Thus, $a' \geqslant a$. Since

  $$ax^2 + bxy + cy^2 \geqslant a(x^2+y^2) + bxy \geqslant a(x^2+y^2) - a|xy| \geqslant a|xy|,$$

  the minimal nonzero positive integer $[a,b,c]$ can represent is equal to or greater than a. Actually, when $(x,y) = (\pm 1, 0)$, $[a,b,c]$ represent a. Similarly, the minimal nonzero (positive) integer that $[a', b', c']$ can represent is a'. Since $[a,b,c] \sim [a',b',c']$, we have they represent the same set of integers. So $a = a'$. Then $\gamma = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ for some k. So $b' = b + 2ak$. Since $a = a'$ and $[a', b', c']$ is reduced, $b, b' \in (-a, a]$. Then $k = 0$ and $b = b'$. So $c = c'$. □

Remark. How to find an equivalence reduced form.

(a) If $c < a$, replace $[a,b,c]$ by $[c, -b, a]$ under $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

(b) If $|b| > a$, replace $[a,b,c]$ by $[a, b', c']$, where $b' = b + 2a\lfloor \frac{a-b}{2a} \rfloor \in (-a, a]$, and c' is found from $(b')^2 - 4ac' = D = \mathrm{disc}\,([a,b,c])$, i.e., $c' = \frac{(b')^2 - D}{4a} = ak^2 + bk + c$.

(c) Repeat until you have a reduced form.

Example 4.30. Let $f = [458, 214, 25]$.

(a) $f \sim [25, -214, 458]$.

(b) $\lfloor \frac{a-b}{2a} \rfloor = \lfloor \frac{239}{50} \rfloor = 4$ and $f \sim [25, -14, 2]$.

(c) $f \sim [2, 14, 25]$, $\left\lfloor \frac{a'-b'}{2a'} \right\rfloor = \lfloor -3 \rfloor = -3$ and $f \sim [2, 2, 1]$.

(d) $f \sim [1, -2, 2]$, $\left\lfloor \frac{a''-b''}{2a''} \right\rfloor = \left\lfloor \frac{3}{2} \right\rfloor = 1$, $f \sim [1, 0, 1] = x^2 + y^2$.

Theorem 4.31. *Let $D < 0$ be a discriminant. There are only finitely many equivalence classes of positive definite binary quadratic forms of discriminant D.*

Proof. It is enough to show there are finitely many reduced forms of discriminant D. If $[a, b, c]$ is reduced, then $|b| \leqslant a \leqslant c$. Since $b^2 \leqslant a^2 \leqslant ac$, $D = b^2 - 4ac \leqslant -3ac$. So $-D \geqslant 3ac$. There are only finitely many a, c that satisfy this. □

Definition 4.32. A binary quadratic form $[a, b, c]$ is *primitive* if $\gcd(a, b, c) = 1$.

Definition 4.33. The *class number* h_D of discriminant $D < 0$ is the number of equivalence classes of primitive positive definite binary quadratic forms of discriminant D.

Definition 4.34. D is a *fundamental discriminant* if and only if one of the following statements holds:

(a) $D \equiv 1 \pmod 4$ and is square-free.

(b) $D = 4m$, where $m \equiv 2, 3 \pmod 4$ and m is square free.

Theorem 4.35 (Heeger, Stark-Baker, Goldfeld-Gross-Zagier)**.** *Let D be a negative, fundamental discriminant. Then*

(a) $h_D = 1$ only for $D = -3, -4, -7, -8, -11, -19, -43, -67, -164$.

(b) $h_D = 2$ only for $-15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, -427$.

(c) $h_D = 3$ only for $-23, -31, -59, -83, -107, -139, -211, -283, -307, -331, -379, -499, -547, -643, -883, -907$.

Definition 4.36. The number of equivalence classes of binary quadratic forms of discriminant D with positive leading coefficient is called the *class number* and denoted $H(D)$.

Theorem 4.37.

$$H(D) \leqslant \begin{cases} 2D, & D > 0 \\ \frac{8}{3}|D|, & D < 0 \end{cases}.$$

Proof. Let $f = [a, b, c]$ be reduced of discriminant D. If a and c have the same sign, $D = b^2 - 4ac = b^2 - 4|ac| \leqslant a^2 - 4|ac| \leqslant a^2 - 4a^2 = -3a^2 < 0$.

(a) If $D > 0$, since $[a, b, c]$ is reduced, we have a and c have opposite signs, then $D = b^2 - 4ac = b^2 + 4|ac| \geqslant 4|ac| \geqslant 4a^2$. So $0 < |a| \leqslant \frac{1}{2}\sqrt{D}$. Then (although the ratio cannot be -1) $-\frac{1}{2}\sqrt{D} \leqslant b \leqslant \frac{1}{2}\sqrt{D}$. Note $c = \frac{b^2-D}{4a}$. Hence $H(D) \leqslant 2\left(\frac{1}{2}\sqrt{D}\right)(\sqrt{D}+1)(1) = D + \sqrt{D} \leqslant 2D$.

(b) If $D < 0$, then a and c have same sign and then $|D| = 4ac - b^2 \geqslant 4a^2 - b^2 \geqslant 4a^2 - a^2 = 3a^2$. So $0 < |a| \leqslant \left|\frac{D}{3}\right|^{\frac{1}{2}}$. Then $-\left|\frac{D}{3}\right|^{\frac{1}{2}} \leqslant b \leqslant \left|\frac{D}{3}\right|^{\frac{1}{2}}$. Hence $H(D) \leqslant 2\left|\frac{D}{3}\right|^{\frac{1}{2}}\left(2\left|\frac{D}{3}\right|^{\frac{1}{2}} + 1\right)(1) = \frac{4}{3}|D| + 2\left|\frac{D}{3}\right|^{\frac{1}{2}} \leqslant \frac{8}{3}|D|$. □

Example 4.38. Determine $H(-4)$ and the prime numbers represented by positive definite binary quadratic forms of discriminant -4. Let $f = [a, b, c]$ be a reduced binary quadratic form of discriminant -4. Then $b^2 - 4ac = -4$ and $-a < b \leqslant a < c$ or $0 \leqslant b \leqslant a = c$. Then $4 = 4ac - b^2 \geqslant 4ac - ac = 3ac$. So $1 \leqslant ac \leqslant \frac{4}{3}$, i.e., $ac = 1$, i.e., $a = c = 1$. So $b = 0$. The only reduced form of discriminant -4 is $x^2 + y^2$. Hence $H(-4) = 1$. The primes represented are $p = 2,\ p \equiv 1 \pmod 4$.

Definition 4.39. We say n is *properly represented* by $f = [a, b, c]$ if there exist x_0, y_0 with $\gcd(x_0, y_0) = 1$ such that $f(x_0, y_0) = n$.

Theorem 4.40. *Let $n \neq 0$, then there exists a binary quadratic form of discriminant D that represents n properly if and only if the congruence $x^2 \equiv D \pmod{4|n|}$ has a solution.*

Proof. "$\Leftarrow$". Suppose b is a solution to the congruence. Write $b^2 - D = 4nc$. The form $f(x, y) = nx^2 + bxy + cy^2$ has integer coefficient, has discriminant D, $f(1, 0) = n$ and $\gcd(1, 0) = 0$.

"$\Rightarrow$". Suppose there exist x_0, y_0 with $\gcd(x_0, y_0) = 1$ and some $f = [a, b, c]$ such that $f(x_0, y_0) = n$. Let $D = b^2 - 4ac$. Since $\gcd(x_0, y_0) = 1$, there exists m_1, m_2 such that $m_1m_2 = 4|n|$, $\gcd(m_1, m_2) = 1$, $\gcd(m_1, y_0) = 1$ and $\gcd(m_2, x_0) = 1$, since we can let m_1 be the product of prime factors p^α of $4n$ for which $p \mid x_0$ if such p exists, otherwise, let $m_1 = 1$, and then let $m_2 = \frac{4n}{m_1}$. Recall $4af(x, y) = (2ax + by)^2 - Dy^2$. So $4an = (2ax_0 + by_0)^2 - Dy_0^2$. Then $(2ax_0 + by_0)^2 \equiv Dy_0^2 \pmod{m_1}$. Since $\gcd(m_1, y_0) = 1$, there exists $\bar{y}_0 \in \mathbb{Z}$ such that $y_0\bar{y}_0 \equiv 1 \pmod{m_1}$. Then $(2ax_0+by_0)^2\bar{y}_0^2 \equiv D \pmod{m_1}$. So the congruence $x^2 \equiv D \pmod{m_1}$ has a solution. Play the same game with $4cf(x_0, y_0)$ to get a solution to $x^2 \equiv D \pmod{m_2}$. Now use the Chinese remainder theorem to get a solution to $x^2 \equiv D \pmod{m_1m_2}$, i.e., $x^2 \equiv D \pmod{4|n|}$. ☐

Example 4.41. Determine the set of primes represented by $f(x, y) = x^2 + xy + 3y^2$. Note $\operatorname{disc}(f) = -11$. Claim. f is the only reduced form of discriminant -11. Suppose $g(x, y) = ax^2 + bxy + cy^2$ is a reduced binary quadratic form of discriminant -11. Then $3ac \leqslant 4ac - b^2 \leqslant 4ac$, i.e., $3ac \leqslant 11 \leqslant 4ac$, i.e., $\frac{11}{4} \leqslant ac \leqslant \frac{11}{3}$. So $ac = 3$. Since $a \leqslant c$, $a = 1$, $c = 3$. Then $b^2 = 4ac - 11 = 1$, i.e., $b = \pm 1$. If $b = -1$, then $|b| = a$, so $b \geqslant 0$, a contradiction. So $b = 1$. Thus, $g = f$ and $H(-11) = 1$. We just need to determine for which p, we can solve $x^2 \equiv -11 \pmod{4p}$. If $p = 2$, $x^2 \equiv -11 \equiv 5 \pmod 8$ has no solution. So you cannot represent 2. Assume $p > 2$. Consider $x^2 \equiv -11 \pmod{4p}$. Since $x^2 \equiv -11 \equiv 1 \pmod 4$, it has a solution. Consider $x^2 \equiv -11 \pmod p$. Want $1 = \left(\frac{-11}{p}\right) = (-1)^{\frac{1}{2}(p-1)}(-1)^{\frac{1}{4}(p-1)(11-1)}\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right)$. So $p \equiv 1, 3, 4, 5, 9 \pmod{11}$. By Chinese remainder theorem, when $p \equiv 1, 3, 4, 5, 9 \pmod{11}$, $x^2 \equiv -11 \pmod{4p}$ has a solution. Thus, these p's are the primes represented by f.

4.1 Fractional Ideal

Definition 4.42. Let $\mathcal{K} = \mathbb{Q}(\sqrt{D})$. A *fractional ideal* of $\mathcal{O}_\mathcal{K}$ is a nonzero subgroup $\mathfrak{a} \subseteq K$ such that

(a) $\beta\mathfrak{a} \subseteq \mathfrak{a}$ for $\beta \in \mathcal{O}_\mathcal{K}$;

(b) there exists $\gamma \in \mathcal{O}_\mathcal{K} \setminus \{0\}$ such that $\gamma\mathfrak{a} \leqslant \mathcal{O}_\mathcal{K}$ is ideal.

Remark. Let $\alpha \in \mathcal{O}_\mathcal{K} \setminus \{0\}$. Then $\alpha^{-1} = \frac{\bar{\alpha}}{\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha)} \in \mathcal{K}$. But in general it will no longer be contained in $\mathcal{O}_\mathcal{K}$. Nonetheless, it is very convenient to have the ability to divide two elements of

$\mathcal{O}_{\mathcal{K}}$. Fractional ideals are a generalization of ordinary ideals which do admit inverses. A fractional ideal is to an ordinary ideal as $\mathbb{Q}$ is to $\mathbb{Z}$. We will sometimes call ordinary ideals of $\mathcal{O}_{\mathcal{K}}$ integral ideals.

Remark. Since $\gamma\mathfrak{a} \leqslant \mathcal{O}_{\mathcal{K}}$, we have any fractional ideal has the form $\mathfrak{a} = \alpha\mathfrak{b}$ for an integral ideal $\mathfrak{b} \leqslant \mathcal{O}_{\mathcal{K}}$ and an element $\alpha = \gamma^{-1} \in \mathcal{K} \setminus \{0\}$.

Remark. Since $\bar{\gamma} \in \mathcal{O}_{\mathcal{K}}$ and $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\gamma) \in \mathbb{Z}$, $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\gamma)\mathfrak{a} = \gamma\bar{\gamma}\mathfrak{a} \subseteq \mathcal{O}_{\mathcal{K}}$. Thus, for (b), you can always find n, not just $\gamma \in \mathcal{O}_{\mathcal{K}}$. We have any fractional ideal has the form $\mathfrak{a} = \alpha\mathfrak{b}$ with $\mathfrak{b} \leqslant \mathcal{O}_{\mathcal{K}}$ and an element, i.e., fractional ideal looks like $\frac{1}{n}\mathfrak{b}$ with $\mathfrak{b} \leqslant \mathcal{O}_{\mathcal{K}}$.

Example 4.43. Let $K = \mathbb{Q}$, then $\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ and $n\mathbb{Z} \leqslant \mathbb{Z}$. Let $m \in \mathbb{Z}$, then $\mathfrak{a} = \frac{1}{m}n\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. A fraction ideal has the form rA for $r \in \mathbb{Q}^{\times}$ and $A \leqslant \mathbb{Z}$. Since any ideal is principal, we have $A = \langle n \rangle$ for some $n \in \mathbb{Z} \setminus \{0\}$, and hence $rA = r\langle n \rangle = (rn)\mathbb{Z}$. Since rn is an arbitrary element of $\mathbb{Q}^{\times}$, we have $\{\text{fractional ideals in } \mathbb{Q}\} = \{r\mathbb{Z} : r \in \mathbb{Q}^{\times}\}$.

Example 4.44. Let $\mathcal{K} = \mathbb{Q}(i)$, then $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[i]$, a PID. Fractional ideal looks like $\alpha\langle\beta\rangle = \langle\gamma\rangle$, where $\gamma = \alpha\beta \in \mathbb{Q}(i)^{\times}$, $\alpha \in \mathbb{Q}(i)$ and $\beta \in \mathbb{Z}[i] \setminus \{0\}$. So $\{\text{fractional ideals}\} = \{\alpha\mathbb{Z}[i], \text{where } \alpha \in \mathbb{Q}(i)^{\times}\}$. For example, we can draw a picture for $\mathfrak{a} = \left(\frac{1}{2} + \frac{1}{2}i\right)\mathbb{Z}[i] = \frac{1}{2}(1+i)\mathbb{Z}[i]$.

Example 4.45. $\mathbb{Q}(\sqrt{D})$ is not a fractional ideal as you cannot clear the denominator.

Definition 4.46. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}(\sqrt{D})$, not all 0, the *fractional ideal* generated by $\alpha_1, \ldots, \alpha_n$ is

$$\langle \alpha_1, \ldots, \alpha_n \rangle := \left\{ \sum_{j=1}^{n} \beta_j \alpha_j \;\middle|\; \beta_j \in \mathcal{O}_{\mathcal{K}} \right\}.$$

Proof. Note there exist $a_i, b_i \in \mathbb{Q}$ such that $\alpha_i = a_i + b_i\sqrt{D}$ for any i. Then just choose m to clear the denominators of all the a_i, b_i'. So $m(\alpha_1, \ldots, \alpha_n) = (m\alpha_1, \ldots, m\alpha_n) \leqslant \mathcal{O}_{\mathcal{K}}$. □

Definition 4.47. We say a fractional ideal $\mathfrak{a}$ is a *principal ideal* if

$$\mathfrak{a} = \langle \alpha \rangle = \alpha\mathcal{O}_{\mathcal{K}} \text{ for some } \alpha \in \mathbb{Q}(\sqrt{D}).$$

Remark. Every ideal $I \leqslant \mathcal{O}_{\mathcal{K}} \subseteq \mathbb{Q}(\sqrt{D})$ gives a lattice in $\mathcal{K}$. But a fractional ideal $\mathfrak{a}$ is just $\mathfrak{a} = \frac{1}{n}I$. So it is a lattice in $\mathcal{K}$ as well. Hence there exist $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$ such that $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$. You can show this gives $\mathfrak{a} = \langle \alpha, \beta \rangle$. In other words, any fractional ideal can be generated by two elements.

Definition 4.48. Let $\mathfrak{a}$ be a fractional ideal. The product fractional ideal is

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{\text{finite}} \alpha_i\beta_i, \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b} \right\}.$$

Remark. (a) This is a fractional ideal.

(b) If $\mathfrak{a} = \langle \alpha_1, \alpha_2 \rangle$, $\mathfrak{b} = \langle \beta_1, \beta_2 \rangle$, then $\mathfrak{a}\mathfrak{b} = \langle \alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2 \rangle$.

Theorem 4.49. *The set of all fractional ideal of* $\mathbb{Q}(\sqrt{D})$ *is an abelian group under multiplication if fractional ideals with the identity element* $\mathcal{O}_{\mathcal{K}}$.

Proof. Well-defined, abelian, associativity, all are essentially either for free or straightforward. Note $\mathcal{O}_{\mathcal{K}} = \langle 1 \rangle$ is easily seen to act as identity under multiplication. It remains to show we have inverses, which can be seen from algebraic number theory. $\square$

Definition 4.50. Let $\mathcal{I}$ be the *group of fractional ideals* in $\mathbb{Q}(\sqrt{D})$. Let $\mathfrak{p} \subseteq \mathcal{I}$ be the subgroup of *principal fractional ideals.* The *class of group* of $\mathbb{Q}(\sqrt{D})$ is the quotient $\mathrm{Cl}\left(\mathbb{Q}(\sqrt{D})\right) := \mathcal{I}/\mathfrak{p}$.

Fact 4.51. $\mathrm{Cl}\left(\mathbb{Q}(\sqrt{D})\right)$ is a finite abelian group.

Remark. The size of $\mathrm{Cl}\left(\mathbb{Q}(\sqrt{D})\right)$ measures how far from a unique factorization domain $\mathcal{O}_{\mathcal{K}}$ is. If $\mathrm{Cl}\left(\mathbb{Q}(\sqrt{D})\right)$ is trival, we have unique factorization in $\mathcal{O}_{\mathcal{K}}$.

Theorem 4.52. *Let $I \leqslant \mathcal{O}_{\mathcal{K}}$. There exist a, b, c with $c \mid a$ and $0 \leqslant b \leqslant a$ such that $I = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$, where $\omega = \frac{D+\sqrt{D}}{2}$. Note $\{1, \omega\}$ is a basis of $\mathcal{O}_{\mathcal{K}}$. Then $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a smith norm form? One has $\#(\mathcal{O}_{\mathcal{K}}/I) = ac = \mathrm{N}(I)$ is finite.*

Remark. Given a fractional ideal $\mathfrak{a}$, we associate a binary quadratic form as follows. Take a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ of $\mathfrak{a}$ with $\omega_1 \in \mathbb{Q}_{>0}$. Then

(a) $\frac{\omega_2\bar{\omega}_1 - \omega_1\bar{\omega}_2}{\sqrt{D}} > 0$,

(b) $\omega_2 - \bar{\omega}_2 = \sqrt{D}$,

(c) $\omega_1 \mid \omega_2\bar{\omega}_2$,

(d) The binary quadratic form $f_{\mathfrak{a}}(x, y) = \frac{\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(x\omega_1 - y\omega_2)}{\mathrm{N}(\mathfrak{a})} = \frac{(x\omega_1 - y\omega_2)(x\bar{\omega}_1 - y\bar{\omega}_2)}{\mathrm{N}(\mathfrak{a})}$.

Fact 4.53. (a) $f_{\mathfrak{a}}$ is an integral binary quadratic form, i.e., usual binary quadratic form with integral coefficients.

(b) $f_{\mathfrak{a}}$ is a primitive binary quadratic form.

Definition 4.54. Let D be a non-square congruent to $0, 1 \pmod 4$. Let

$$\mathcal{F}(D) = \{\text{set of equivalent class of primitive binary quadratic of discriminant } D \text{ module the action of } \mathrm{PSL}_2(\mathbb{Z})\},$$

where $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm\mathbb{1}_2\}$. Set

$$\mathcal{F}^+(D) = \{\text{set of equivalent class of primitive b.q.f. } [a, b, c] \text{ with } a > 0 \text{ of discriminant } D \text{ module the action of } \mathrm{PSL}_2(\mathbb{Z})\}.$$

Theorem 4.55. *Let $D < 0$ be congruent to $0, 1 \pmod 4$. Then the map $\Phi([a, b, c]) = a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}$ and $\phi(\mathfrak{a}) = \frac{\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(x\omega_1 - y\omega_2)}{\mathrm{N}(A)}$, where $\mathfrak{a} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with $\frac{\omega_2\bar{\omega}_1 - \omega_1\bar{\omega}_2}{\sqrt{D}} > 0$ induces a bijection between $\mathcal{F}^+(D)$ and $\mathrm{Cl}\left(\mathbb{Q}(\sqrt{D})\right)$.*

Chapter 5

Continued Fraction

Given a real number θ, we can find a rational number as close to θ as we like.

Theorem 5.1 (Dirichlet 1842). *Let $\theta \in \mathbb{R}$ and $Q \in \mathbb{R}_{>1}$, then there exist p, q with $1 \leqslant q < Q$ such that $|q\theta - p| \leqslant \frac{1}{Q}$, i.e., $\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{qQ}$.*

Proof. Let $N = \lfloor Q \rfloor$. Define $\{x\} = x - \lfloor x \rfloor \in [0, 1)$. Consider the following $N+1$ unordered numbers in $[0, 1]$: $0, 1, \{\theta\}, \{2\theta\}, \ldots, \{(N-1)\theta\}$. Partition the unit intervals into N disjoint intervals of length $\frac{1}{N}$. Note $0 = 0\theta - 0$ and $1 = 0\theta - (-1)$ and $\{j\theta\} = j\theta - \lfloor j\theta \rfloor \in [0, 1)$ for $j = 1, \ldots, N-1$. Then the difference between any two of these $N+1$ numbers is of the form $q'\theta - p'$ for some p', q' with $1 \leqslant q' < N$. By PHP, at least 2 of the $N+1$ numbers must lie in the same intervals. Thus, there exist p, q with $1 \leqslant q < N \leqslant Q$ and $|q\theta - p| \leqslant \frac{1}{N} \leqslant \frac{1}{Q}$. □

Corollary 5.2. Whenever θ is irrational, there exists infinitely many distinct pairs (p, q) with $q \in \mathbb{N}$ such that $\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{q^2}$.

Proof. Let $Q \geqslant 2$. Then there exist p, q with $1 \leqslant q < Q$ such that $0 < \left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{qQ} < \frac{1}{q^2}$. Let $Q' > \left|\theta - \frac{p}{q}\right|^{-1}$. Then there exist p', q' with $1 \leqslant q' < Q'$ such that $0 < \left|\theta - \frac{p'}{q'}\right| \leqslant \frac{1}{q'Q'} < \frac{1}{q'}\left|\theta - \frac{p}{q}\right| \leqslant \left|\theta - \frac{p}{q}\right|$. So $\frac{p'}{q'} \neq \frac{p}{q}$. Moreover, $\left|\theta - \frac{p'}{q'}\right| < \frac{1}{q'Q'} < \frac{1}{q'^2}$. Continue and we will get infinitely many distinct such pairs. □

Remark (Fact: Roth,1958). If θ is an algebraic number, then for $\epsilon > 0$, there exist $C_\epsilon > 0$ such that $\left|\theta - \frac{p}{q}\right| \leqslant \frac{C_\epsilon}{q^{2+\epsilon}}$ has only finitely many solutions.

Remark. $q \in \mathbb{Q}$ has finitely continued fractional. $p \in \mathbb{R} \setminus \mathbb{Q}$ has infinitely continued fractional.

Theorem 5.3 (Algorithm). *Let $\theta \in \mathbb{R}$. Define a_j as follows.*

(a) Let $a_0 = \lfloor \theta \rfloor$. If $a_0 = \theta$, stop. If $a_0 \neq \theta$, define θ_1 such that $\theta = a_0 + \frac{1}{\theta_1}$, i.e., $\theta_1 = \frac{1}{\theta - a_0} = \frac{1}{\{\theta\}}$.

(b) Let $a_1 = \lfloor \theta_1 \rfloor$. If $a_1 = \theta_1$, stop. If $a_1 \neq \theta$, define θ_2 such that $\theta_1 = a_1 + \frac{1}{\theta_2}$, i.e., $\theta_2 = \frac{1}{\theta_1 - a_1} = \frac{1}{\{\theta_1\}}$. Then $\theta = a_0 + \frac{1}{\theta_1} = a_0 + \frac{1}{a_1 + \frac{1}{\theta_2}}$.

(c) Continue this, if it stops at n^{th} step, then θ is rational and write

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}} = [a_0, a_1, \ldots, a_n].$$

If $\theta \in \mathbb{R} \setminus \mathbb{Q}$, it never stops, then θ is irrational and write $\theta = [a_0, a_1, a_2, a_3, \cdots]$.

Corollary 5.4. $a_n = \lfloor \theta_n \rfloor$ and $\theta_n = [a_n, a_{n+1}, \cdots]$.

Example 5.5. Let $\theta = \frac{57}{32}$. Then $a_0 = \left\lfloor \frac{57}{32} \right\rfloor = 1$. Set $\theta_1 = \frac{1}{\theta - a_0} = \frac{32}{25}$. Then $a_1 = \left\lfloor \frac{32}{25} \right\rfloor = 1$. Set $\theta_2 = \frac{1}{\theta_1 - a_1} = \frac{25}{7}$. Then $a_2 = 3$. Set $\theta_3 = \frac{1}{\theta_2 - a_2} = \frac{7}{4}$. Then $a_3 = 1$. Set $\theta_4 = \frac{1}{\theta_3 - a_3} = \frac{4}{3}$. Then $a_4 = 1$. Set $\theta_5 = \frac{1}{\theta_4 - a_4} = 3 = a_5$. So

$$\theta = 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}}} = [1, 1, 3, 1, 1, 3].$$

Example 5.6. Let $\theta = \sqrt{3}$. Then $a_0 = 1$. Set $\theta_1 = \frac{1}{\theta - a_0} = \frac{1}{\sqrt{3} - 1} = \frac{1}{2}(\sqrt{3} + 1)$. Then $a_1 = 1$. Set $\theta_2 = \frac{1}{\theta_1 - a_1} = \sqrt{3} + 1$. Then $a_2 = 2$. Set $\theta_3 = \frac{1}{\theta_2 - a_2} = \frac{1}{\sqrt{3} - 1} = \theta_1$. So

$$\theta = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}}} = [1, 1, 2, 1, 2, 1, 2, \cdots] = [1, \overline{1, 2}].$$

Example 5.7. $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \cdots]$.

Definition 5.8. The a_i's are known as the partial quotients of θ. The θ_i's are the complete quotients of θ. The rational numbers $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ with $\gcd(p_n, q_n) = 1$ and $q_n \geqslant 1$ are called the *convergents* to θ. The integers p_n and q_n satisfy the following recursive relations.

Theorem 5.9. *Let $\theta \in \mathbb{R}$. Let a_n be the partial quotients of θ, θ_n the complete quotients of θ. Then the convergents $\frac{p_n}{q_n}$ satisfy the recurrence relations $p_0 = a_0,\ q_0 = 1,\ p_1 = a_0a_1 + 1,\ q_1 = a_1$, $p_n = a_np_{n-1} + p_{n-2}$ and $q_n = a_nq_{n-1} + q_{n-2}$. Furthermore, $p_nq_n - p_{n-1}q_n = (-1)^{n+1}$ for $n \in \mathbb{N}$ and $\lim_{n\to\infty} q_n = \infty$ and $\lim_{n\to\infty} \frac{p_n}{q_n} = \theta$.*

Proof. Since $\frac{p_0}{q_0} = [a_0] = a_0$, we have $p_0 = a_0,\ q_0 = 1$. Since $\frac{p_1}{q_1} = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1+1}{a_1}$, we have $p_1 = a_0a_1 + 1,\ q_1 = a_1$. Since

$$\frac{p_2}{q_2} = [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_2(a_0a_1 + 1) + a_0}{a_1a_2 + 1} = \frac{a_2p_1 + p_0}{a_2q_1 + a_0},$$

we have $p_2 = a_2p_1 + p_0,\ q_2 = a_2q_1 + q_0$. So the recurrence relation holds for $n = 2$. Since $\gcd(a, b) = \gcd(a + bn, b)$ for $n \in \mathbb{Z}$, we have $1 = \gcd(a_0, 1)$, $1 = \gcd(1, a_1) = \gcd(a_0a_1 + 1, a_1)$

and $1 = \gcd(1, a_2) = \gcd(a_2, a_1a_2 + 1) = \gcd(a_0a_1a_2 + a_2 + a_0, a_1a_2 + 1)$. So $\gcd(p_i, q_i) = 1$ for $i = 0, 1, 2$. Assume the statement is true for any $n \leqslant m$. Then

$$\frac{p_{m+1}}{q_{m+1}} = [a_0, a_1, \ldots, a_m, a_{m+1}] = \left[a_0, a_1, \ldots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right] = \frac{\left(a_m + \frac{1}{a_{m+1}}\right)p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right)q_{m-1} + q_{m-2}}$$
$$= \frac{(a_{m+1}a_m + 1)p_{m-1} + a_{m+1}p_{m-2}}{(a_{m+1}a_m + 1)q_{m-1} + a_{m+1}q_{m-2}} = \frac{a_{m+1}(a_mp_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_mq_{m-1} + q_{m-2}) + q_{m-1}} = \frac{a_{m+1}p_m + p_{m-1}}{a_{m+1}q_m + q_{m-1}}.$$

Claim. $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n+1}$. When $n = 1$, $p_1q_0 - p_0q_1 = (a_0a_1 + 1) - a_0a_1 = 1 = (-1)^{1+1}$. Assume the result holds for $k = n - 1$. Then

$$\begin{aligned} p_nq_{n-1} - p_{n-1}q_n &= (a_np_{n-1} + p_{n-2})q_{n-1} - p_{n-1}(a_nq_{n-1} + q_{n-2}) \\ &= -(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

Similarly, $p_nq_{n+1} - p_{n+1}q_n = (-1)^{n+1}$. Define $\{a_0\} = a_0,\ \{a_0, a_1\} = a_0a_1 + 1$ and $\{a_0, \ldots, a_n\} = \{a_0, \ldots, a_{n-1}\}a_n + \{a_0, \ldots, a_{n-2}\}$. Then by induction

$$\{a_0, \ldots, a_n\}\{a_1, \ldots, a_{n-1}\} - \{a_1, \ldots, a_n\}\{a_0, \ldots, a_{n-1}\} = (-1)^{n+1}.$$

So $\gcd(\{a_0, \ldots, a_{m+1}\}, \{a_1, \ldots, a_{m+1}\}) = 1$. Also, by induction, $a_{m+1}p_m + p_{m-1} = \{a_0, \ldots, a_{m+1}\}$ and $a_{m+1}q_m + q_{m-1} = \{a_1, \ldots, a_{m+1}\}$. So $\gcd(a_{m+1}p_m + p_{m-1}, a_{m+1}q_m + q_{m-1}) = 1$. Thus, $\gcd(p_i, q_i) = 1$ for $i \geqslant 0$. Since $a_i \geqslant 1$ for $i \in \mathbb{N}$, we have $q_n = a_nq_{n-1} + q_{n-2} \geqslant q_{n-1} + q_{n-2} > q_{n-1}$. So $\{q_n\}$ form a strictly increasing sequence of integers and thus $\lim_{n\to\infty} q_n = \infty$. Since $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n+1}$, we have $\left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_{n-1}q_n}$. Also, $\theta = [a_0, a_1, \ldots, a_{n-1}, \theta_n]$, where $0 < \frac{1}{\theta_n} \leqslant \frac{1}{\lfloor\theta_n\rfloor} = \frac{1}{a_n}$. So θ lies between $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$. Hence $\left|\theta - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_{n-1}q_n} \to 0$. Thus, $\lim_{n\to\infty} \frac{p_n}{q_n} = \theta$. □

Remark. Let $\theta = \frac{s}{t}$ with $\gcd(s, t) = 1$. For any convergent $\frac{p_n}{q_n}$, we have either $\frac{p_n}{q_n} = \theta$ or $\frac{1}{tq_n} \leqslant \left|\frac{sq_n - tp_n}{tq_n}\right| = \left|\frac{s}{t} - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_nq_{n+1}}$. Eventually, $q_{n+1} > t$, so it must be that for some large n, $\frac{p_n}{q_n} = \frac{s}{t}$. Thus, if $\theta \in \mathbb{Q}$, θ has a finite continued fraction expression.

Corollary 5.10.

$$\theta = \frac{\theta_np_{n-1} + p_{n-2}}{\theta_nq_{n-1} + q_{n-2}}.$$

Definition 5.11. $\theta \in \mathbb{R}$ is a *quadratic irrational* when there exist a, b, c such that $a\theta^2 + b\theta + c = 0$ and $b^2 - 4ac > 0$ is not a perfect square.

Theorem 5.12. *The continued fraction* $[a_0, a_1, \cdots]$ *represents a quadratic irrational if and only if the sequence* $\{a_j\}$ *is ultimately periodic.*

Proof. "$\Leftarrow$". Suppose $\theta = [a_0, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}}]$. Write $\phi = [\overline{a_k, \ldots, a_{k+m-1}}]$. Then $\phi = [a_k, \ldots, a_{k+m-1}, \phi]$. Let $\frac{p'_m}{q'_m}$ be the convergents to ϕ. Then $\frac{p'_M}{q'_M} = [a_k, \ldots, a_{k+M}]$. Then $p'_0 = a_k,\ q'_0 = 1,\ p'_1 = a_ka_{k+1} + 1,\ q'_1 = a_k,\ p'_M = a_{k+M}p'_{M-1} + p'_{M-2}$ for $2 \leqslant M \leqslant m - 1$ and $q'_M = a_{k+M}q'_{M-1} + q'_{M-2}$ for $2 \leqslant M \leqslant m - 1$. So $\frac{p'_M}{q'_M} = [a_k, \ldots, a_{k+M}] = \frac{a_{k+M}p'_{M-1} + p'_{M-2}}{q_{k+M}q'_{M-1} + q'_{M-2}}$. Then

$\phi = [a_k, \dots, a_{k+m-1}, \phi] = \frac{\phi p'_{m-1}+p'_{m-2}}{\phi q'_{m-1}+q'_{m-2}}$. Hence $q'_{m-1}\phi^2 + (q'_{m-2} - p'_{m-1})\phi - p'_{m-2} = 0$. Thus, ϕ is a quadratic irrational. Let $\frac{p_m}{q_m}$ be the convergents to θ. Then $\theta = [a_0, \dots, a_{k-1}, \phi] = \frac{p_{k-1}\phi+p_{k-2}}{q_{k-1}\phi+q_{k-2}}$. Assume $\phi = \frac{a'\sqrt{D}+b'}{d'}$, $a', b', c' \in \mathbb{Z}$ with $D > 0$ is not a perfect square. Plug it in, we also have θ can be written as $\theta = \frac{a\sqrt{D}+b}{d}$.

"$\Rightarrow$". Let θ be a quadratic irrational. Assume $a\theta^2 + b\theta + c = 0, a, b, c \in \mathbb{Z}$, with $D = b^2 - 4ac > 0$ is not a perfect square. Let $f(x, y) = ax^2 + bxy + cy^2$. Let $\frac{p_n}{q_n}$ be convergents to θ. Set $r_n = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$. Then $\det(r_n) = p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$. So r_n takes f to an "equivalent form" $f_n(x, y) = a_n x^2 + b_n xy + c_n y^2$, which has the same discriminant as f. Then $f(p_n, q_n) = ap_n^2 + bp_n q_n + cq_n^2 = a_n$, $a_{n-1} = f(p_{n-1}, q_{n-1}) = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 = c_n$. So $f\left(\frac{p_n}{q_n}, 1\right) = a\frac{p_n^2}{q_n^2} + b\frac{p_n}{q_n} + c = \frac{a_n}{q_n^2}$. Since $f(\theta, 1) = 0$, we have

$$\frac{a_n}{q_n^2} = f\left(\frac{p_n}{q_n}, 1\right) = f\left(\frac{p_n}{q_n}, 1\right) - f(\theta, 1) = \left(a\left(\frac{p_n}{q_n} + \theta\right) + b\right)\left(\frac{p_n}{q_n} - \theta\right).$$

So $|a_n| = q_n^2 \left|a\left(\frac{p_n}{q_n} + \theta\right) + b\right|\left|\frac{p_n}{q_n} - \theta\right|$. Since $\left|\frac{p_n}{q_n} - \theta\right| \leqslant \frac{1}{q_n q_{n-1}} \leqslant \frac{1}{q_n^2}$, we have

$$|a_n| \leqslant \left|a\left(\frac{p_n}{q_n} + \theta\right) + b\right| = |a|\left|\frac{p_n}{q_n} + \theta\right| + |b| \leqslant |a|\left(2|\theta| + \left|\frac{p_n}{q_n} - \theta\right|\right) + |b| \leqslant |a|\left(2|\theta| + 1\right) + |b|.$$

Hence there are finitely many choices for a_n. Since $a_{n-1} = c_n$, we have there are finitely many choices for c_n. Since $b_n^2 - 4a_n c_n = b^2 - 4ac$, we have there are finitely many choices for b_n. Let θ_n's be the complete quotients to θ. Then $\theta = \frac{\theta_{n+1}p_n+p_{n-1}}{\theta_{n+1}q_n+q_{n-1}}$. Let $\theta = \frac{\phi}{\phi'}$. Then $\begin{bmatrix} \phi \\ \phi' \end{bmatrix} \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} \begin{bmatrix} \theta_{n+1} \\ 1 \end{bmatrix}$. Since $f(\theta, 1) = 0$ and $f_n(x, y) = f(p_n x + p_{n-1}y, q_n x + q_{n-1}y)$, we have

$$f_n(\theta_{n+1}, 1) = f(p_n\theta_{n-1} + p_{n-1}, q_n\theta_{n+1} + q_{n-1}) = f(\phi, \phi') = a\phi^2 + b\phi\phi' + c\phi'^2 = \phi'^2 f(\theta, 1) = 0.$$

Since there are finitely many choices a_n, b_n, c_n, there are finitely many f_n. Since $(\theta_n, 1)$'s are roots of f_n, there are finitely many possible θ_n's. So there exists m, l such that $\theta_{l+m} = \theta_l$. Then

$$\begin{aligned} \theta &= [a_0, \dots, a_{l-1}, \theta_l] = [a_0, \dots, a_{l-1}, a_l, \dots, a_{l+m-1}, \theta_{l+m}] \\ &= [a_0, \dots, a_{l-1}, a_l, \dots, a_{l+m-1}, \theta_l] = [a_0, \dots, a_{l-1}, \overline{a_l, \dots, a_{l+m-1}}]. \end{aligned}$$

Thus, θ has periodic continued fraction. □

Definition 5.13. We say θ is *purely periodic* if

$$\theta = [\overline{a_0, \dots, a_n}].$$

Remark. Goal: Given $d \in \mathbb{N}$ not a perfect square. Compute the continued fractional of $\sqrt{d}$. We first compute the continued fractional of $\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor$, which is purely periodic.

Theorem 5.14. *The continued fraction expansion of the real quadratic irrational number θ is purely periodic if and only if $\theta > 1$ and $-1 < \bar{\theta} < 0$.*

Proof. "$\Leftarrow$". Assume $\theta > 1$ and $-1 < \bar{\theta} < 0$. As usual, define $\theta_{i+1} = \frac{1}{\theta_i - a_i}$. Then $\overline{\theta_{i+1}} = \frac{1}{\overline{\theta_i} - a_i}$. Note by assumption, $-1 < \overline{\theta_0} < 0$. Assume $-1 < \overline{\theta_n} < 0$. Since $a_n \geqslant 1$ for $n \in \mathbb{Z}_{\geqslant 0}$, we have $\overline{\theta_n} - a_n < -1$. So $-1 < \overline{\theta_{n+1}} < 0$. Thus, $-1 < \overline{\theta_i} < 0$ for $i \in \mathbb{Z}^{\geqslant 0}$. Then $-1\overline{\theta_i} = a_i + \frac{1}{\overline{\theta_{i+1}}} < 0$. So $0 < -a_i - \frac{1}{\overline{\theta_{i+1}}} < 1$, i.e., $a_i < -\frac{1}{\overline{\theta_{i+1}}} < a_i + 1$. Hence $a_i = \left\lfloor -\frac{1}{\overline{\theta_{i+1}}} \right\rfloor$. Since θ is quadratic irrational, θ is eventually periodic and so for some $0 < j < k$, $\theta_j = \theta_k$. Then $\overline{\theta_j} = \overline{\theta_k}$. So $a_{j-1} = \left\lfloor -\frac{1}{\overline{\theta_j}} \right\rfloor = \left\lfloor -\frac{1}{\overline{\theta_k}} \right\rfloor = a_{k-1}$. Then $\theta_{j-1} = a_{j-1} + \frac{1}{\theta_j} = a_{k-1} + \frac{1}{\theta_k} = \theta_{k-1}$. Thus, if $\theta_j = \theta_k$, then $\theta_{j-1} = \theta_{k-1}$. Repeating this j times gives $\theta_0 = \theta_{k-j}$. Then

$$\theta = \theta_0 = [a_0, \ldots, a_{k-j-1}, \theta_{k-j}] = [a_0, \ldots, a_{k-j-1}, \theta_0] = [\overline{a_0, a_1, \ldots, a_{k-j+1}}].$$

"$\Rightarrow$". Assume θ is purely periodic, say $\theta = [\overline{a_0, \ldots, a_n}]$ with $a_j \in \mathbb{N}$ for $j = 0, \ldots, n$. Then $\theta > a_0 \geqslant 1$. Since $\theta = [a_0, \ldots, a_{n-1}, \theta] = \frac{\theta p_{n-1} + p_{n-2}}{\theta q_{n-1} + q_{n-2}}$, θ is a root of $f(x) = q_{n-1}x^2 + (q_{n-2} - p_{n-1})x^2 - p_{n-2} = 0$. Let $\bar{\theta}$ be another root of f. Then it remains to show $-1 < \bar{\theta} < 0$. Note $f(0) = -a_{n-2} < 0$ and

$$\begin{aligned} f(-1) &= q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} = a_{n-1}q_{n-2} + q_{n-3} - q_{n-2} + a_{n-1}p_{n-2} + p_{n-3} - p_{n-2} \\ &= (q_{n-2} + p_{n-2})(a_{n-1} - 1) + q_{n-3} + p_{n-3} \geqslant q_{n-3} + p_{n-3} > 0. \end{aligned}$$

By intemediate zero theorem, $-1 < \bar{\theta} < 0$. □

Lemma 5.15. Let $\frac{p_n}{q_n}$ be the n^{th} convergent of the continued fraction representation $\theta \in \mathbb{R} \setminus \mathbb{Q}$. If $a, b \in \mathbb{Z}$ with $1 \leqslant b < q_{n+1}$, then $|q_n\theta - p_n| < |b\theta - a|$.

Proof. Consider the system of equations $\begin{cases} p_n\alpha + p_{n+1}\beta &= a \\ q_n\alpha + q_{n+1}\beta &= b \end{cases}$. Since $p_nq_{n+1} - p_{n+1}q_n = (-1)^{n+1}$, we have a unique solution to equations above

$$\begin{cases} \alpha &= (-1)^{n+1}(aq_{n+1} - bp_{n+1}) \in \mathbb{Z} \\ \beta &= (-1)^{n+1}(bp_n - aq_n) \in \mathbb{Z} \end{cases}.$$

If $\alpha = 0$, then $aq_{n+1} = bp_{n+1}$. Since $\gcd(p_{n+1}, q_{n+1}) = 1$, we have $q_{n+1} \mid b$, contradicted by $b < q_{n+1}$. So $\alpha \neq 0$. If $\beta = 0$, then $bp_n = aq_n$ and $a = p_n\alpha$ and $b = q_n\alpha$. So $|b\theta - a| = |\alpha||q_n\theta - p_n| \geqslant |q_n\theta - p_n|$. Hence we have the result if $\beta = 0$. Assume now $\beta \neq 0$. Claim. β and α have opposite sign. If $\beta < 0$, then $q_n\alpha = b - q_{n+1}\beta > 0$. Since $b \geqslant 1$ and $q_i \geqslant 0$ for $i \geqslant 0$, $\alpha > 0$. If $\beta > 0$, since $b < q_{n+1}$, $b < \beta q_{n+1}$. Then $q_n\alpha = b - \beta q_{n+1} < 0$. So $\alpha < 0$. Recall θ lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$. Then $\left(\theta - \frac{p_n}{q_n}\right)\left(\theta - \frac{p_{n+1}}{q_{n+1}}\right) < 0$. Since $q_i > 0$ for $i \in \mathbb{Z}_{\geqslant 0}$, $(q_n\theta - p_n)(q_{n+1}\theta - p_{n+1}) < 0$. So $q_n\theta - p_n$ and $q_{n+1}\theta - p_{n+1}$ are of opposite sign. Thus, $\alpha(q_n\theta - p_n)$ and $\beta(q_{n+1}\theta - p_{n+1})$ have the same sign. Since $\alpha \neq 0$,

$$\begin{aligned} |b\theta - a| &= |(q_n\alpha + q_{n+1}\beta)\theta - (p_n\alpha + p_{n+1}\beta)| = |\alpha(q_n\theta - p_n) + \beta(q_{n+1}\theta - p_{n+1})| \\ &= |\alpha(q_n\theta - p_n)| + |\beta(q_{n+1}\theta - p_{n+1})| \geqslant |\alpha||q_n\theta - p_n| \geqslant |q_n\theta - p_n|. \end{aligned}$$ □

Theorem 5.16. *If* $1 \leqslant b \leqslant q_n$, *then* $\left|\theta - \frac{p_n}{q_n}\right| \leqslant \left|\theta - \frac{a}{b}\right|$, *i.e., Continued fractions give the best approximations.*

Proof. Suppose $\left|\theta - \frac{p_n}{q_n}\right| > \left|\theta - \frac{a}{b}\right|$. Then $|q_n\theta - p_n| = q_n\left|\theta - \frac{p_n}{q_n}\right| > \left|\theta - \frac{a}{b}\right| = |b\theta - a|$, contradicted by Lemma 5.15. □

Lemma 5.17. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$. If $\frac{a}{b} \in \mathbb{Q}$ with $b \in \mathbb{N}$ and $\gcd(a, b) = 1$ such that $\left|\theta - \frac{a}{b}\right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a convergent $\frac{p_n}{q_n}$ for some n.

Proof. Assume $\frac{a}{b}$ is not a convergent. We know q_n's form an increasing sequence. So there exists $n \geqslant 0$ such that $1 \leqslant b = q_n < q_{n+1}$. Then $|q_n\theta - p_n| \leqslant |b\theta - a| = b\left|\theta - \frac{a}{b}\right| < b\frac{1}{2b^2} = \frac{1}{2b}$. So $\left|\theta - \frac{p_n}{q_n}\right| \leqslant \frac{1}{2q_n b}$. Since $\frac{a}{b}$ is not a convergent, $bp_n - aq_n \neq 0$. So $1 \leqslant |bp_n - aq_n|$. Then

$$\frac{1}{bq_n} \leqslant \left|\frac{bp_n - aq_n}{bq_n}\right| = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leqslant \left|\frac{p_n}{q_n} - \theta\right| + \left|\theta - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}.$$

So $b < q_n$, a contradiction. □

Theorem 5.18. *If (p, q) is a positive solution to $x^2 - dy^2 = 1$, then $\frac{p}{q}$ is a convergent of the continued fraction expresion of $\sqrt{d}$.*

Proof. Since $1 = p^2 - dq^2 = (p - q\sqrt{d})(p + q\sqrt{d})$ and $p + q\sqrt{d} > 0$, $p > q\sqrt{d}$. Then

$$0 < \frac{p}{q} - \sqrt{d} = \frac{p - q\sqrt{d}}{q} = \frac{p^2 - dq^2}{q(p + q\sqrt{d})} = \frac{1}{q(p + q\sqrt{d})} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{\sqrt{d}}{2q\sqrt{d}} = \frac{1}{2q^2}.$$

Since $\gcd(p, q) = 1$, by Lemma 5.17, $\frac{p}{q}$ is a convergent. □

Lemma 5.19. Let $d > 0$ not be a perfect square. Write $\sqrt{d} = [a_0, a_1, a_2, \cdots]$. Define s_k and t_k by $s_0 = 0, t_0 = 1$, $s_{k+1} = a_k t_k - s_k$, and $t_{k+1} = \frac{d - s_{k+1}^2}{t_k}$ for $k \in \mathbb{Z}_{\geqslant 0}$. Then $s_k, t_k \in \mathbb{Z}$ with $t_k \neq 0$, $t_k \mid (d - s_k^2)$ and $\theta_k = \frac{s_k + \sqrt{d}}{t_k}$ for $k \in \mathbb{Z}_{\geqslant 0}$.

Proof. $k = 0$ is clear. Assume the result holds for k. Since $a_k \in \mathbb{Z}$, $s_{k+1} \in \mathbb{Z}$. Suppose $t_{k+1} = 0$. Then $d = s_{k+1}^2$, which is a contradicted by d is not a perfect square. So $t_{k+1} \neq 0$. Since $t_{k+1} = \frac{d - s_{k+1}^2}{t_k} = \frac{d - s_k^2}{t_k} + (2a_k s_k - a_k^2 t_k) \in \mathbb{Z}$, $t_{k+1} \mid (d - s_{k+1}^2)$. Note

$$\theta_{k+1} = \frac{1}{\theta_k - a_k} = \frac{t_k}{(s_k + \sqrt{d}) - t_k a_k} = \frac{t_k}{\sqrt{d} - s_{k+1}} = \frac{t_k(s_{k+1} + \sqrt{d})}{d - s_{k+1}^2} = \frac{s_{k+1} + \sqrt{d}}{t_{k+1}}.$$ □

Theorem 5.20. *Let $d \in \mathbb{N}$ not be a perfect square. Then $\sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor > 1$ and $-1 < -\sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor < 0$. So $\sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor$ is purely periodic.*

Proof. Since $a_0 = \left\lfloor\sqrt{d} + \lfloor d\rfloor\right\rfloor = 2\left\lfloor\sqrt{d}\right\rfloor$,

$$\begin{aligned}\sqrt{d} &= -\left\lfloor\sqrt{d}\right\rfloor + \left(\sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor\right) = -\left\lfloor\sqrt{d}\right\rfloor + \left[2\left\lfloor\sqrt{d}\right\rfloor, \overline{a_1, \ldots, a_{r-1}, a_0}\right] \\ &= -\left\lfloor\sqrt{d}\right\rfloor + 2\left\lfloor\sqrt{d}\right\rfloor + \frac{1}{\text{stuff}} = \left\lfloor\sqrt{d}\right\rfloor + \frac{1}{\text{stuff}} = \left[\left\lfloor\sqrt{d}\right\rfloor, \overline{a_1, \ldots, a_{r-1}, 2\left\lfloor\sqrt{d}\right\rfloor}\right].\end{aligned}$$ □

Theorem 5.21. *Let $\theta_0 = \left\lfloor\sqrt{d}\right\rfloor + \sqrt{d}$,, then $t_i = 1$ if and only if $i = jr$ for some $j \geqslant 0$.*

Proof. Assume

$$\theta = \sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor = [\overline{a_0, \ldots, a_{r-1}}] = [a_0, \overline{a_1, \ldots, a_{r-1}, a_0}] = [a_0, a_1, \overline{a_2, \ldots, a_{r-2}, a_0, a_1}] = \cdots,$$

where r is chosen to be the smallest integer such that we have this type of expression for θ. Then

$$\begin{aligned}\theta_i &= [a_i, a_{i+1}, \cdots] = [a_i, \ldots, a_{Nr-1}, \overline{a_0, \ldots, a_{r-1}}] = [a_{i-(N-1)r}, \ldots, a_{r-1}, \overline{a_0, \ldots, a_{r-1}}] \\ &= [a_{i-(N-1)r}, \ldots, a_{r-2}, \overline{a_{r-1}, a_0, \ldots, a_{r-2}}] = [\overline{a_{i-(N-1)r}, \ldots, a_{i-(N-2)r-1}}],\end{aligned}$$

is purely periodic as well. Since $\theta = \theta_0 = \theta_r = \theta_{2r} = \cdots$ with $\theta_i \neq \theta_0$ for $i = 1, \ldots, r-1$, we have $\theta_0 = \theta_i$ if and only if $i = rm$ for some $m \geqslant 0$. Let $s_0 = \left\lfloor\sqrt{d}\right\rfloor$, $t_0 = 1$, $\theta_0 = \sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor$, $s_{i+1} = a_i t_i - s_i$ for $i \in \mathbb{N}$ and $t_{i+1} = \frac{d - s_{i+1}^2}{t_i}$ for $i \in \mathbb{N}$. So similarly, we have $\theta_i = \frac{s_i + \sqrt{d}}{t_i}$ for $i \geqslant 0$. Then for $j \in \mathbb{N}$, $\frac{s_{jr} + \sqrt{d}}{t_{jr}} = \theta_{jr} = \theta_0 = \sqrt{d} + \left\lfloor\sqrt{d}\right\rfloor$. So $\mathbb{Z} \ni s_{jr} - t_{jr}\left\lfloor\sqrt{d}\right\rfloor = (t_{jr} - 1)\sqrt{d}$. Hence $t_{jr} = 1$. Suppose $t_i = 1$ for some other index i. Then $\theta_i = s_i + \sqrt{d}$. Since θ_i is purely periodic, $-1 < s_i - \sqrt{d} < 0$, i.e., $\sqrt{d} - 1 < s_i < \sqrt{d}$. So $s_i = \left\lfloor\sqrt{d}\right\rfloor$. Hence $\theta_i = \left\lfloor\sqrt{d}\right\rfloor + \sqrt{d} = \theta_0$, a contradiction. Exercise: show $t_i \neq -1$ for $i \geqslant 0$. ☐

Corollary 5.22. Let $\theta_0 = \sqrt{d}$,, then $t_i = 1$ if and only if $i = jr$ for some $j \geqslant 0$.

Example 5.23. Find the quadratic irrational given by $\theta = \lfloor 8, \overline{1, 16}\rfloor = 8 + \frac{1}{x}$, where $x = [\overline{1, 16}]$. Since $x = [1, 16, x] = 1 + \frac{1}{16 + \frac{1}{x}}$, we have $x^{-2} + 16x^{-1} - 16 = 0$. Solve this for x^{-1} and take the positive part, $x^{-1} = -8 + \sqrt{80}$. Then $\theta = 8 + x^{-1} = 8 + (-8 + \sqrt{80}) = \sqrt{80}$.

Theorem 5.24. *Let $d > 0$ not be a perfect square. Then $x^2 - dy^2 = 1$ has infinitely many integer solution.*

Proof. By Dirichlet (1842), for $Q \in \mathbb{R}_{>1}$, there exist $p, q \in \mathbb{Z}$ with $1 \leqslant q < Q$ such that $\left|q\sqrt{d} - p\right| \leqslant \frac{1}{Q}$. Then

$$\left|p + q\sqrt{d}\right| = \left|p - q\sqrt{d} + 2q\sqrt{d}\right| \leqslant \left|p - q\sqrt{d}\right| + 2q\sqrt{d} \leqslant \frac{1}{Q} + 2q\sqrt{d} < 3q\sqrt{d} < 3Q\sqrt{d}.$$

So $\left|p^2 - q^2 d\right| = \left|p - q\sqrt{d}\right|\left|p + q\sqrt{d}\right| < \frac{1}{Q}3Q\sqrt{d} = 3\sqrt{d}$. We can show there are infinitely many pairs (p, q) such that $\left|p^2 - q^2 d\right| < 3\sqrt{d}$. Since $3\sqrt{d}$ is finite, there exist N such that the Pell's equation $x^2 - dy^2 = N$ has infinitely many solutions. Among these infinitely many solutions, there is a pair of congruence class (α, β) such that infinitely many (x, y)'s satisfy $\begin{cases} x \equiv \alpha \pmod{N} \\ y \equiv \beta \pmod{N} \end{cases}$. Let (p, q) and (p', q') satisfy the Pell's equation and $\begin{cases} p \equiv p' \equiv \alpha \pmod{N} \\ q \equiv q' \equiv \beta \pmod{N} \end{cases}$. Then

$$(pp' - dqq')^2 - d(pq' - qp')^2 = (pp')^2 + d^2(qq')^2 - d(pq')^2 - d(qp')^2 = (p^2 - dq^2)(p'^2 - dq'^2) = N^2.$$

Set $\widetilde{x} = pp' - dqq'$ and $\widetilde{y} = pq' - qp'$. Then

$$\widetilde{x} = pp' - dqq' \equiv p^2 - dq^2 \pmod{N} \equiv N \pmod{N} \equiv 0 \pmod{N},$$

and

$$\widetilde{y} = pq' - qp' = pq' - p'q' + p'q' - qp' = (p - p')q' + (q' - q)p' \equiv 0 \pmod N.$$

So $N \mid \widetilde{x}$ and $N \mid \widetilde{y}$. Set $x = \frac{\widetilde{x}}{N} \in \mathbb{Z}$ and $y = \frac{\widetilde{y}}{N} \in \mathbb{Z}$. Since $\widetilde{x}^2 - d\widetilde{y}^2 = N^2$, we have $x^2 - dy^2 = 1$. So we have a solution. Exercise: show $(x, y) \neq (\pm 1, 0)$. Then we get distinct solutions. Given a nontrivial solution (u, v) to $x^2 - dy^2 = 1$. Then $(u^2 + dv^2)^2 - d(2uv)^2 = (u^2 - dv^2) = 1$. So $(u^2 + dv^2, 2uv)$ is another solution. Repeat to get infinitely many solution. □

Theorem 5.25. *Let $\frac{p_k}{q_k}$ be the k^{th} convergents of $\theta = \sqrt{d}$. Then $p_k^2 - dq_k^2 = (-1)^{k+1} t_{k+1}$, where $t_{k+1} > 0$ for $k \geqslant 0$.*

Proof. Write $\sqrt{d} = [a_0, a_1, \ldots, a_k, \theta_{k+1}]$ and $\theta = \frac{\theta_{k+1} p_k + p_{k-1}}{\theta_{k+1} q_k + q_{k-1}}$. Substitute $\theta_{k+1} = \frac{s_{k+1} + \sqrt{d}}{t_{k+1}}$, we have $\sqrt{d} = \frac{\frac{s_{k+1}+\sqrt{d}}{t_{k+1}} p_k + p_{k-1}}{\frac{s_{k+1}+\sqrt{d}}{t_{k+1}} q_k + q_{k-1}}$, i.e., $\sqrt{d} = \frac{s_{k+1} p_k + \sqrt{d} p_k + t_{k+1} p_{k-1}}{s_{k+1} q_k + \sqrt{d} q_k + t_{k+1} q_{k-1}}$, i.e., $\sqrt{d}(s_{k+1} q_k + t_{k+1} q_{k-1} - p_k) = s_{k+1} p_k + t_{k+1} p_{k-1} - dq_k \in \mathbb{Z}$. So

$$\begin{cases} s_{k+1} q_k + t_{k+1} q_{k-1} &= p_k \\ s_{k+1} p_k + t_{k+1} p_{k-1} &= dq_k \end{cases}.$$

Then $p_k^2 - dq_k^2 = t_{k+1}(p_k q_{k-1} - p_{k-1} q_k) = (-1)^{k+1} t_{k+1}$. Facts: $\frac{p_{2k}}{q_{2k}}$ converges to θ from below. $\frac{p_{2k+1}}{q_{2k+1}}$ converges to θ from above. Since $\frac{p_{2k}}{q_{2k}} < \sqrt{d} < \frac{p_{2k+1}}{q_{2k+1}}$ for $k \geqslant 0$, for $k \geqslant 0$, $\begin{cases} p_k^2 - dq_k^2 < 0, \forall 2 \mid k \\ p_k^2 - dq_k^2 > 0, \forall 2 \nmid k \end{cases}$. Then $\frac{p_k^2 - dq_k^2}{p_{k-1}^2 - dq_{k-1}^2} < 0$, i.e., $\frac{(-1)^{k+1} t_{k+1}}{(-1)^k t_k} < 0$, i.e., $\frac{t_{k+1}}{t_k} > 0$ for $k \geqslant 0$. Since $t_0 = 1 > 0$, we have $t_k > 0$ for $k \geqslant 0$. □

Example 5.26. We have $\sqrt{15} = [3, \overline{1, 6}]$. The convergents are $\frac{3}{1}, \frac{4}{1}, \frac{27}{7}, \frac{31}{8}, \cdots$. Then $p_0^2 - dq_0^2 = 3^2 - 15 \cdot 1^2 = -6$, $p_1^2 - dq_1^2 = 4^2 - 15 \cdot 1^2 = 1$, $p_2^2 - dq_2^2 = 27^2 - 15 \cdot 7^2 = -6$, $p_3^2 - dq_3^2 = 31^2 - 15 \cdot 8^2 = 1$, $t_1 = t_3 = 6$ and $t_2 = t_4 = 1$.

Theorem 5.27. *Let $\frac{p_k}{q_k}$ be the convergents of the continued fractions expansions of $\sqrt{d}$ and let n be the length of the expansion.*

(a) If $2 \mid n$, then all possible solutions of $x^2 - dy^2 = 1$ are given by $\begin{cases} x &= p_{kn-1} \\ y &= q_{kn-1} \end{cases}, k \in \mathbb{N}$.

(b) If $2 \nmid n$, then all possible solutions of $x^2 - dy^2 = 1$ are given by $\begin{cases} x &= p_{2kn-1} \\ y &= q_{2kn-1} \end{cases}, k \in \mathbb{N}$.

Proof. By previous theorem, $p_j^2 - dq_j^2 = (-1)^{j+1} t_{j+1}$ with $t_{j+1} > 0$. To be a solution, we must have $2 \mid j + 1$. Then we get a solution if $t_{j+1} = 1$. Since n is the length of the expansion, $t_{j+1} = 1$ if and only if $j + 1 = nk$ for some $k \in \mathbb{N}$, i.e., $j = nk - 1$. If $2 \nmid n$, since $2 \mid j + 1$, we have $2 \mid k$. If $2 \mid n$, no conclusion on k. □

Example 5.28. Consider $x^2 - 7y^2 = 1$. Note $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$. Since $n = 4$, solutions are $\begin{cases} x &= p_{4k-1} \\ y &= q_{4k-1} \end{cases}, \forall k \in \mathbb{N}$. Note the $\frac{p_i}{q_i}'s$ are $\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}, \frac{37}{14}, \frac{45}{17}, \frac{82}{31}, \frac{127}{48}, \cdots$. Then $p_3^2 - 7 * q_3^2 = 8^2 - 7 * 3^2 = 1$, $p_7^2 - 7 * q_7^2 = 127^2 - 7 * 48^2 = 1, \cdots$.

Definition 5.29. The unique solution (x_0, y_0) of $x^2 - dy^2 = 1$ in which x, y have their smallest positive value is called the *fundamental solution*, i.e., if (x', y') is another solution, then $0 < x_0 < x'$ and $0 < y_0 < y'$.

Theorem 5.30. *The fundamental solution (x, y) exists. If $2 \mid n$, $\begin{cases} x_0 &= p_{n-1} \\ y_0 &= p_{n-1} \end{cases}$. If $2 \nmid n$, $\begin{cases} x_0 &= p_{2n-1} \\ y_0 &= p_{2n-1} \end{cases}$.*

Theorem 5.31. *Let (x_0, y_0) be fundamental solution of $x^2 - dy^2 = 1$. Then every pair of integers (x_n, y_n) defined by $x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ is also a solution.*

Proof. Exercise: $x_n - y_n\sqrt{d} = (x_0 - y_0\sqrt{d})^n$. Since $x_0, y_0 > 0$, we have $x_n, y_n > 0$ for $n \in \mathbb{N}$. Since $x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (x_0 + y_0\sqrt{d})^n(x_0 - y_0\sqrt{d})^n = (x_0^2 - y_0^2 d)^n = 1^n = 1$, (x_n, y_n) is a solution. □

Example 5.32. Consider $x^2 - 35y^2 = 1$. The fundamental solution is $\begin{cases} x_0 = 6 \\ y_0 = 1 \end{cases}$. Since $(6 + \sqrt{35})^2 = 71 + 12\sqrt{35}$, $(71, 12)$ is a solution. Since $(6 + \sqrt{35})^3 = 846 + 143\sqrt{35}$, $(846, 143)$ is a solution.

Theorem 5.33. *Let (x_1, y_1) be fundamental solution of $x^2 - dy^2 = 1$. Then every positive solution is given by (x_n, y_n), where x_n, y_n are determined by $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.*

Proof. Assume (u, v) is a positive solution that is not of this form. Since $x_1 + y_1\sqrt{d} > 1$, we have $x_n + y_n\sqrt{d} \to \infty$. Then there exist $n \in \mathbb{N}$ such that

$$(x_1 + y_1\sqrt{d})^n = x_n + y_n\sqrt{d} < u + v\sqrt{d} < x_{n+1} + y_{n+1}\sqrt{d} = (x_n + y_n\sqrt{d})(x_1 + y_1\sqrt{d}).$$

Then

$$(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) < (u + v\sqrt{d})(x_n - y_n\sqrt{d}) < (x_n + y_n\sqrt{d})(x_1 + y_1\sqrt{d})(x_n - y_n\sqrt{d}).$$

Since $x_n^2 - y_n^2 = 1$, we have $1 < (u + v\sqrt{d})(x_n - y_n\sqrt{d}) < x_1 + y_1\sqrt{d}$. Define r, s by $1 < r + s\sqrt{d} = (u + v\sqrt{d})(x_n - y_n\sqrt{d})$. Then $r = x_n u - y_n vd$ and $s = x_n v - y_n u$. Then $r^2 - ds^2 = (x_n^2 - dy_n^2)(u^2 - dv^2) = 1$. Since $1 = (r + s\sqrt{d})(r - s\sqrt{d})$ and $1 < r + s\sqrt{d}$, we have $0 < r - s\sqrt{d} < 1$. Then $2r = (r + s\sqrt{d}) + (r - s\sqrt{d}) > 1 + 0 = 1$. So $r > 0$. Also, since $2s\sqrt{d} = (r + \sqrt{d}) - (r - s\sqrt{d}) > 1 - 1 = 0$, $s > 0$. Since $1 < r + s\sqrt{d} < x_1 + y_1\sqrt{d}$ and $r > 0$, we have $s > 0$, a contradiction. □

5.0.1 Quadratic fields

Consider the quadratic number field $\mathcal{K} = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. This is a Galois extension of $\mathbb{Q}$, i.e.,there are two automorphisms, the identity and the conjugation map $\sigma : \mathcal{K} \to \mathcal{K}$ given by $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. Clearly $\sigma^2 = 1$ and $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}) = \{1, \sigma\}$. Let $\alpha = a + b\sqrt{d}$. Note $\sigma(\alpha) = \alpha$ if and only if $b = 0$, i.e., if and only if $\alpha \in \mathbb{Q}$. We say that $\mathcal{K}$ is real or complex quadratic according to $d > 0$ or $d < 0$. The element $\alpha = a + b\sqrt{d} \in \mathcal{K}$ is a root of the quadratic polynomial $p_\alpha(X) = X^2 - 2aX + a^2 - db^2 \in \mathbb{Q}[X]$. Its second root $\overline{\alpha} = a - b\sqrt{d}$ is called the conjugate of α.

Definition 5.34. Let d be square free. Let $K = \mathbb{Q}(\sqrt{d})$. Define

$$\begin{aligned} \mathrm{N} : (\mathcal{K}, \times) &\to (\mathbb{Q}, \times) \\ a + b\sqrt{d} &\mapsto (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d \end{aligned}$$

and

$$\begin{aligned} \mathrm{Tr} : (\mathcal{K}, +) &\to (\mathbb{Q}, +) \\ a + b\sqrt{d} &\mapsto (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \end{aligned}$$

and

$$\begin{aligned} \mathrm{disc} : \mathcal{K} &\to \mathbb{Q} \\ a + b\sqrt{d} &\mapsto 4db^2. \end{aligned}$$

Theorem 5.35. N *is a multiplicative group homomorphism.* Tr *is an additive group homomorphism.*

Definition 5.36. $\mathrm{N}|_{\mathcal{O}_\mathcal{K}} : \mathcal{O}_\mathcal{K} \smallsetminus \{0\} \to \mathbb{Z} \smallsetminus \{0\}$ with $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. To ease notation, we assume $d \equiv 2, 3 \pmod 4$, such that $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{d}]$.

Remark. Goal: understand $\mathbb{Z}[\sqrt{d}]^\times$.

Lemma 5.37. $\alpha \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $\mathrm{N}(\alpha) = \pm 1$.

Proof. Suppose there exists $\beta \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha\beta = 1$. Then $1 = \mathrm{N}(1) = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. So $\mathrm{N}(\alpha) \mid 1$. Hence $\mathrm{N}(\alpha) = \pm 1$. Suppose $\mathrm{N}(\alpha) = \pm 1$. Let $\alpha = a + b\sqrt{d}$. Then $\pm 1 = \mathrm{N}(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d})$. If $(a+b\sqrt{d})(a-b\sqrt{d}) = 1$, then $(a+b\sqrt{d})^{-1} = a - b\sqrt{d}$. If $(a+b\sqrt{d})(a-b\sqrt{d}) = -1$, then $(a + b\sqrt{d})^{-1} = -(a - b\sqrt{d})$. □

Theorem 5.38. *The solutions to Pell's equations are*

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})} \cong G_2 \times \left(x_1 + y_1\sqrt{d}\right)^\mathbb{Z},$$

where (x_1, y_1) is the fundamental solution. and $G_2 = \{\pm 1\}$ is an order 2 group. Note

$$(x_1 + y_1\sqrt{d})^{-n} = \left(\frac{1}{x_1 + y_1\sqrt{d}}\right)^n = (x_1 - y_1\sqrt{d})^n = x_n - y_n\sqrt{d}.$$

Example 5.39. Consider $\mathbb{Q}(\sqrt{7})$. Then $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{7}]$. To find units in $\mathbb{Z}[\sqrt{7}]$, we want to study $x^2 - 7y^2 = 1$. Note $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$, $p_0 = a_0 = 2$, $q_0 = 1$, $p_1 = a_1 a_0 + 1 = 3$, $q_1 = a_1 = 1$, $p_2 = a_2 p_1 + p_0 = 3 + 2 = 5$, $q_2 = a_2 q_1 + q_0 = 1 + 1 = 2$, $p_3 = a_3 p_2 + p_1 = 5 + 3 = 8, q_3 = a_3 q_2 + q_1 = 2 + 1 = 3, \cdots$. So $(p_{4-1}, q_{4-1}) = (p_3, q_3) = (8, 3)$ is a solution.

Theorem 5.40. *Let $d > 0$ be not square and $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. If $\mathrm{N}(\alpha) = 1$, then is a Pell's equation. If $\mathrm{N}(\alpha) = -1$, then you want a solution to $x^2 - dy^2 = -1$.*

Fact 5.41.

$$\mathcal{O}^\times_\mathcal{K} \cong G_2 \times (x_1 + y_1\sqrt{d})^\mathbb{Z}.$$

$\mathrm{N} : \mathcal{O}^\times_\mathcal{K} \to G_2$. The solution to Pell's equation is kernel of this. If $d \equiv 3 \pmod 4$, there are no units of norm -1.

Remark. We want to solve the fermat equation for $n = 3$. Equivalently, we can show there is no nontrivial solution to $\alpha^3 + \beta^3 + \gamma^3 = 0$. We will show this how no solution is in $\mathbb{Q}(\sqrt{-3})$.

Remark. We say the units for $\mathbb{Q}(\sqrt{d})$, we actually say the units for $\mathbb{Z}(\sqrt{d})$.

Theorem 5.42. *Let $d < 0$ be square-free. The field $\mathbb{Q}(\sqrt{d}) = \mathcal{K}$ has units ± 1 and these are the only units except $d = -1, -3$. The units for $\mathbb{Q}(i)$ are $\pm 1, \pm i$. The units for $\mathbb{Q}(\sqrt{-3})$ are $\pm 1, \frac{1\pm\sqrt{-3}}{2}, \frac{-1\pm\sqrt{-3}}{2}$.*

Proof. Let $\alpha \in \mathcal{O}_{\mathcal{K}}$ with $\mathrm{N}(\alpha) = \pm 1$. The integral basis is $\begin{cases} \{1, \sqrt{d}\} & d \not\equiv 1 \pmod 4 \\ \left\{1, \frac{1+\sqrt{d}}{2}\right\} & d \equiv 1 \pmod 4 \end{cases}$.

(a) If $d \not\equiv 1 \pmod 4$, then $\alpha = x + y\sqrt{d}$. Then $\mathrm{N}(\alpha) = x^2 - dy^2$. Since $d < 0$, we have $\mathrm{N}(\alpha) > 0$ and then $\mathrm{N}(\alpha) \neq -1$ in this case. For $d < -1$, $x^2 - dy^2 \geqslant -dy^2 \geqslant 2y^2$. The only solutions to $x^2 - dy^2 = 1$ are $x = \pm 1$ and $y = 0$, i.e., the only units are $\alpha = \pm 1$. If $d = -1$, then $x^2 + y^2 = 1$. This only has solutions $x = \pm 1, y = 0$ and $x = 0, y = \pm 1$, i.e., the only units for $\mathbb{Q}(\sqrt{-1})$ are $\alpha = \pm 1, \pm\sqrt{-1}$.

(b) If $d \equiv 1 \pmod 4$, then $\alpha = x' + y'\frac{1+\sqrt{d}}{2} = \frac{(2x'+y')+y'\sqrt{d}}{2}$. If y' is even, then same case as previous one and we get some units ± 1. If y' is odd, then $2x' + y'$ is odd and write $\alpha = \frac{x+y\sqrt{d}}{2}$ with x, y odd. So $\mathrm{N}(\alpha) = \frac{x^2-dy^2}{4}$. Since $d < 0$, $\mathrm{N}(\alpha) > 0$, so $\mathrm{N}(\alpha) \neq -1$ in this case. If $d < -3$, since $x^2 - dy^2 \geqslant 1 - d > 4$, there are no solution to $\frac{x^2-dy^2}{4} = 1$ with odd x, y. If $d = -3$, $\frac{x^2+3y^2}{4} = 1$ with x, y odd, i.e., $x^2 + 3y^2 = 4$ with x, y odd. The only solutions are $(1, \pm 1)$ and $(-1, \pm 1)$, i.e., the only units are $\alpha = \frac{1\pm\sqrt{-3}}{2}, \frac{-1\pm\sqrt{-3}}{2}$. Thus, we have units for $\mathbb{Q}(\sqrt{-3})$ are $\alpha = \pm 1, \frac{1\pm\sqrt{-3}}{2}, \frac{-1\pm\sqrt{-3}}{2}$. ☐

Remark. Let $\omega = \frac{-1+\sqrt{-3}}{2}$. Then the units of $\mathbb{Q}(\sqrt{-3})$ are $\pm 1,\ \pm\omega,\ \pm\omega^2$. Note $1 + \omega + \omega^2 = 0$, and $\omega^3 = 1$.

We aren't actually working with quadratic fields to look at fermat big theorem, it just happens that $\mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{-3})$. Over $\mathbb{Q}(\xi_p)$, $z^p = x^p + y^p = (x + y)(x + \xi_p y) \cdots (x + \xi_p^{p-1} y)$.

Definition 5.43. An element $\alpha \in \mathcal{O}_{\mathcal{K}}$ is a *prime* if it is not a unit and it is divisible only by units and its associates.

Theorem 5.44. *Let $\alpha \in \mathcal{O}_{\mathcal{K}}$. If $\mathrm{N}(\alpha) = \pm p$ for a rational prime, then α is prime.*

Proof. Suppose $\alpha \in \mathcal{O}_{\mathcal{K}}$ satisfies $\mathrm{N}(\alpha) = \pm p$ and $\alpha = \beta\gamma$. Then $\pm p = \mathrm{N}(\alpha) = \mathrm{N}(\beta\gamma) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma)$. So $\mathrm{N}(\beta) = \pm 1$ and $\mathrm{N}(\gamma) = \pm p$, or $\mathrm{N}(\beta) = \pm p$ and $\mathrm{N}(\gamma) = \pm 1$. So either β or γ is a unit. Hence β or γ is associate of α. Thus, α is only divisible by units or associates. Therefore, α is prime. ☐

Theorem 5.45. *Every element $\alpha \in \mathcal{O}_{\mathcal{K}}$ can be factored into primes.*

Proof. Let $\alpha \in \mathcal{O}_{\mathcal{K}}$. If α is prime, we are done. If not, we can write $\alpha = \beta_1\beta_2$ with β_1, β_2 not associate of α. If $\beta_1\beta_2$ are both prime, we are done. If not, factor the one that is not prime (possibly both). Then $\alpha = \beta_1\beta_2^{(1)}\beta_2^{(2)}$. Keeping doing this, write $\alpha = \beta_1 \cdots, \beta_n$. Since β_i's are not associates of α, they are not units, either. If there is no prime factorization, you get something like this for any n. Then $|\mathrm{N}(\alpha)| = |\prod_{i=1}^n \mathrm{N}(\beta_i)| = \prod_{i=1}^n |\mathrm{N}(\beta_i)|$. So we can just choose n such that $|\mathrm{N}(\alpha)| < 2^n$, a contradiction. ☐

Definition 5.46. We say $\mathbb{Q}(\sqrt{d})$ has *unique factorization* if $\mathcal{O}_\mathcal{K}$ is a UFD, i.e., all elements in $\mathcal{O}_\mathcal{K}$ that are not 0 or units can be factored uniquely into primes up to order and associates.

Definition 5.47. We say $\mathbb{Q}(\sqrt{d})$ is an *Euclidean Domain* if $\mathcal{O}_\mathcal{K}$ is an Euclidean domain, i.e., given $\alpha, \beta \in \mathcal{O}_\mathcal{K}$ with $\beta \neq 0$, there exist $\gamma, \delta \in \mathcal{O}_\mathcal{K}$ such that $\alpha = \beta\gamma + \delta$ with $\gamma = 0$ or $|\mathrm{N}(\delta)| < |\mathrm{N}(\gamma)|$.

Theorem 5.48. *Every Euclidean domain $\mathbb{Q}(\sqrt{d})$ has unique factorization.*

Theorem 5.49. *The field $\mathbb{Q}(\sqrt{d})$ for $d = -1, -2, -3, -7, 2, 3$ is Euclidean.*

Proof. Let $\mathcal{K} = \mathbb{Q}(\sqrt{m})$. Let $\alpha, \beta \in \mathcal{O}_\mathcal{K}$ with $\beta \neq 0$. Write $\frac{\alpha}{\beta} = u + v\sqrt{m}$ with $u, v \in \mathbb{Q}$. Choose x, y as close as possible to u, v, respectively. Then $0 \leqslant |u - x| \leqslant \frac{1}{2}$ and $0 \leqslant |v - y| \leqslant \frac{1}{2}$. Set $\gamma = x + y\sqrt{m} \in \mathcal{O}_\mathcal{K}$ and $\delta = \alpha - \beta\gamma \in \mathcal{O}_\mathcal{K}$. Since

$$\mathrm{N}(\delta) = \mathrm{N}(\alpha - \beta\gamma) = \mathrm{N}\big(\frac{\alpha}{\beta} - \gamma)\big)\,\mathrm{N}(\beta) = \mathrm{N}(u - x + (v - y)\sqrt{m})\,\mathrm{N}(\beta) = \big((u - x)^2 - m(v - y)^2\big)\,\mathrm{N}(\beta),$$

we have $|\mathrm{N}(\delta)| = \big|(u - x)^2 - m(v - y)^2\big||\mathrm{N}(\beta)|$. Observe

$$\begin{cases} -\frac{m}{4} \leqslant (u - x)^2 - m(v - y)^2 \leqslant \frac{1}{4} & m > 0 \\ 0 \leqslant (u - x)^2 - m(v - y)^2 \leqslant \frac{1}{4} - \frac{m}{4} & m < 0 \end{cases}.$$

If $m = 2, 3, -1, -2$, then $|\mathrm{N}(\delta)| < |\mathrm{N}(\beta)|$, which implies the corresponding $\mathbb{Q}(\sqrt{m})$ is Euclidean.
Let $m = -3$ or -7. Leave u, v as above. Choose s as close as possible to $2v$ and r such that $r \equiv s \pmod 2$ and as close to $2u$ as possible. Then $0 \leqslant |2v - s| \leqslant \frac{1}{2}$ and $0 \leqslant |2u - r| \leqslant 1$. Since $m \equiv 1 \pmod 4$, $\gamma = \frac{r + s\sqrt{m}}{2} \in \mathcal{O}_\mathcal{K}$. Set $\delta = \alpha - \beta\gamma \in \mathcal{O}_\mathcal{K}$. Since

$$\mathrm{N}(\delta) = \mathrm{N}(\alpha - \beta\gamma) = \mathrm{N}(\frac{\alpha}{\beta} - \gamma))\,\mathrm{N}(\beta) = \mathrm{N}(u - \frac{r}{2} + (v - \frac{s}{2})\sqrt{m})\,\mathrm{N}(\beta) = ((u - \frac{r}{2})^2 - m(v - \frac{s}{2})^2)\,\mathrm{N}(\beta),$$

we have $|\mathrm{N}(\delta)| \leqslant \big|\frac{1}{4} - \frac{m}{16}\big||\mathrm{N}(\beta)| < |\mathrm{N}(\beta)|$. □

Theorem 5.50. *Let $\mathcal{K} = \mathbb{Q}(\sqrt{m})$ have unique factorization. Then any prime π in $\mathbb{Q}(\sqrt{m})$ corresponds to exactly one rational prime p such that $\pi \mid p$.*

Proof. Since $\mathrm{N}(\pi) = \pi\overline{\pi} \in \mathbb{Z}$, we have $\pi \mid \mathrm{N}(\pi)$. Let n be the smallest positive rational integer divisible by π. Claim. n is prime in $\mathbb{Q}(\sqrt{m})$. If not, write $n = n_1 n_2$ with $n_1, n_2 \neq \pm 1$. Then $\pi \mid n = n_1 n_2$. Since $n_1, n_2 \neq \pm 1$, $\pi \mid n_1$ or $\pi \mid n_2$, a contradiction since $n_1 < n$ and $n_2 < n$. Hence, n is our n. Let q be a rational prime and $p \neq q$ such that $\pi \mid q$. Then $\pi \mid 1 = px + qy$ for some x, y, a contradiction since 1 is not a prime. □

Theorem 5.51. *Let $\mathcal{K} = \mathbb{Q}(\sqrt{m})$ have unique factorization.*

(a) Any rational prime p is either a prime π in $\mathcal{K}$ or the product of two prime π_1, π_2 not necessarily distinct of $\mathcal{K}$.

(b) The totality of primes π, π_1, π_2 obtained in (a) from p, together with associates constitute all the primes in $\mathbb{Q}(\sqrt{m})$.

(c) An odd rational prime p satisfying $\gcd(p, m) = 1$ is a product $\pi_1\pi_2$ of two primes π_1, π_2 of $\mathcal{K}$ if and only if? $\left(\frac{m}{p}\right) = 1$. Furthermore, if $p = \pi_1\pi_2$, then π_1 and π_2 are not associate, but π_1 and $\overline{\pi_2}$ are associate (as are $\overline{\pi_1}$ and π_2).

(d) If $\gcd(2,m)=1$*, then 2 is the associate of a square of a prime if* $m\equiv 3 \pmod 4$*, 2 is prime if* $m\equiv 5 \pmod 8$*, and 2 is a product of distinct primes if* $m\equiv 1 \pmod 8$*.*

(e) Any rational prime p *that divides* m *is the associate of the square of a prime in* $\mathbb{Q}(\sqrt{m})$*.*

Proof. (a) Suppose p is prime π in $\mathcal{K}$, then we are done. Suppose p is not prime in $\mathcal{K}$. Then $p=\pi\beta$ for some π prime and $\beta\in\mathcal{O}_{\mathcal{K}}$ with $\beta\neq\pm 1$. So $p^2=\mathrm{N}(p)=\mathrm{N}(\pi\beta)=\mathrm{N}(\pi)\,\mathrm{N}(\beta)$. Also, since $\mathrm{N}(\pi)\in\mathbb{Z}\smallsetminus\{1\}$ and $\mathrm{N}(\beta)\in\mathbb{Z}\smallsetminus\{1\}$, $\mathrm{N}(\beta)=\pm p$. So β is prime. Thus, p is the product of two primes.

(b) Given any prime π, the previous theorem says it divides a unique rational prime p. Now apply (a).

(c) Let p be a rational prime such that $2\nmid p$, $p\nmid m$ and $\left(\frac{m}{p}\right)=1$. Then there exists x such that $x^2\equiv m \pmod p$, i.e., $p\mid x^2-m$ if and only if $p\mid(x+\sqrt{m})(x-\sqrt{m})$. Suppose p is prime in $\mathcal{K}$, then $p\mid x-\sqrt{m}$ or $p\mid x+\sqrt{m}$. Without loss of generality, assume $p\mid x+\sqrt{m}$.

(1) If $m\not\equiv 1 \pmod 4$, then there exist a,b such that $p(a+b\sqrt{m})=x+\sqrt{m}$. Then $pb=1$, a contradiction.

(2) If $m\equiv 1 \pmod 4$, then there exist a,b such that $p\left(a+b\frac{1+\sqrt{m}}{2}\right)=x+\sqrt{m}$, i.e., $pa+p\frac{b}{2}+p\frac{b}{2}\sqrt{m}=x+\sqrt{m}$. So $p\frac{b}{2}=1$, which is a contradiction since $p\nmid 2$.

Hence, p is not a prime (in $\mathcal{K}$). By the proof of part (a), p is the product of two prime π_1,π_2 with $\pi_1=a+b\sqrt{m}$ and $a^2-mb^2=\mathrm{N}(\pi_1)=\pm p$. Then $\pi_2=\frac{p}{\pi_1}=\frac{p}{a+b\sqrt{m}}=\pm(a-b\sqrt{m})$. So $\overline{\pi}_2=\pm(a+b\sqrt{m})$, which is an associate of π. Since $\frac{\pi_1}{\pi_2}=\pm\frac{a+b\sqrt{m}}{a-b\sqrt{m}}=\pm\left(\frac{(2a)^2+m(2b)^2}{4p}+\frac{8ab\sqrt{m}}{4p}\right)\notin\mathcal{O}_{\mathcal{K}}$ (Exercise), which means $\frac{\pi_1}{\pi_2}$ is certainly not a unit. For example, $5=(2+i)(2-i)$. But 2 is not odd, $1+i=i(1-i)$ and $2=(1+i)(1-i)$.

(d) Assume $m\equiv 3 \pmod 4$. Then $(m-\sqrt{m})(m+\sqrt{m})=m^2-m=2\frac{m^2-m}{2}$. If is a prime, then $2\mid m-\sqrt{m}$ or $2\mid m+\sqrt{m}$. So $\frac{m+\sqrt{m}}{2}\in\mathcal{O}_{\mathcal{K}}$ or $\frac{m-\sqrt{m}}{2}\in\mathcal{O}_{\mathcal{K}}$. Since $2\nmid m$ and $m\not\equiv 1 \pmod 4$, these are actually not in $\mathcal{O}_{\mathcal{K}}$. Hence, 2 is not prime. By the proof of part (a), there exist x,y such that $x+y\sqrt{m}\mid 2$ and $x^2-my^2=\mathrm{N}(x+y\sqrt{m})=\pm 2$. So $2=\pm(x-y\sqrt{m})(x+y\sqrt{m})$, where $x-y\sqrt{m}$ and $x+y\sqrt{m}$ are primes. We want $x-y\sqrt{m}$ and $x+y\sqrt{m}$ to be associate and then 2 will be square of a prime up to associate. Exercise: show the last part of the following

$$\frac{x-y\sqrt{m}}{x+y\sqrt{m}}=\pm\frac{x^2+my^2-2xy\sqrt{m}}{x^2-my^2}=\pm\left(\frac{x^2+my^2}{2}-xy\sqrt{m}\right)\in\mathcal{O}_{\mathcal{K}}.$$

Similarly, $\frac{x+y\sqrt{m}}{x-y\sqrt{m}}=\pm\left(\frac{x^2+my^2}{2}+xy\sqrt{m}\right)\in\mathcal{O}_{\mathcal{K}}$. So $\frac{x+y\sqrt{m}}{x-y\sqrt{m}}$ and its inverse are in $\mathcal{O}_{\mathcal{K}}$. Hence $\frac{x+y\sqrt{m}}{x-y\sqrt{m}}\in\mathcal{O}_{\mathcal{K}}^{\times}$. Thus, $x-y\sqrt{m}$ and $x+y\sqrt{m}$ are associate. Assume $m\equiv 1 \pmod 4$. Suppose 2 is not a prime. By the proof of part (a), there exist x,y of the same parity such that $\frac{x+y\sqrt{m}}{2}\,\Big|\,2$, and $\mathrm{N}\left(\frac{x+y\sqrt{m}}{2}\right)=\pm 2$. Then $x^2-my^2=\pm 8$. If x,y are both even, write $x=2x_0,\ y=2y_0$. Then $x_0^2-my_0^2=\pm 2$. Since $m\equiv 1 \pmod 4$, we have $x_0^2-my_0^2$ is odd or multiple of 4, a contradiction. So x and y are both odd. Hence $x^2\equiv y^2\equiv 1 \pmod 8$. Then $1-m\equiv x^2-my^2\equiv 0 \pmod 8$. So $m\equiv 1 \pmod 8$. Thus, if $m\equiv 5 \pmod 8$, then 2 is a prime in $\mathcal{K}$. Assume $m\equiv 1 \pmod 8$. Then

$\frac{1-\sqrt{m}}{2}\frac{1+\sqrt{m}}{2} = \frac{1-m}{4} = 2\frac{1-m}{8}$. Since $2 \mid \frac{1\pm\sqrt{m}}{2}$, we have 2 is not a prime. By the proof of part (d), there exist x, y both odd such that $\frac{x+y\sqrt{m}}{2}\frac{x-y\sqrt{m}}{2} = \mathrm{N}\left(\frac{x+y\sqrt{m}}{2}\right) = \pm 2$. Since x, y are both odd, $\pm\frac{\frac{x+y\sqrt{m}}{2}}{\frac{x-y\sqrt{m}}{2}} = \pm\frac{x+y\sqrt{m}}{x-y\sqrt{m}} = \pm\left(\frac{x^2+my^2}{8} + \frac{xy\sqrt{m}}{4}\right) \notin \mathcal{O}_{\mathcal{K}}$. Thus, $\frac{x-y\sqrt{m}}{2}$ and $\frac{x+y\sqrt{m}}{2}$ are not associates. Therefore, 2 is a product of two non-associate primes.

(e) Let p be a rational prime divisor of m. If $p = |m|$, then $p = \pm\sqrt{m}\sqrt{m}$. Since the norm of m is prime p, $\sqrt{m}$ is prime. If $p < |m|$, then $\sqrt{m}\sqrt{m} = m = p\frac{m}{p}$. Since $\frac{\sqrt{m}}{p} \notin \mathcal{O}_{\mathcal{K}}$, we have $p \nmid \sqrt{m}$ in $\mathcal{K}$. So p is not prime in $\mathcal{K}$. By the proof of part (a), there exists some prime π with $\mathrm{N}(\pi) = \pm p$ such that $\pi \mid p$. Since $\pi \mid \sqrt{m}\sqrt{m}$, we have $\pi \mid \sqrt{m}$. So $\pi^2 \mid m$. Since m is square-free, $p \mid\mid m$. So $\pi \not\Big| \frac{m}{p}$? Thus, $\pi^2 \mid p$. ☐

Remark (Diophantine Equation)**.** Let $\alpha \in \mathcal{O}_{\mathcal{K}}$ with $\mathrm{N}(\alpha) = \pm p$. Since $\mathrm{N}(\overline{\alpha}) = \pm p$, we have $\overline{\alpha}$ is prime. If $m \not\equiv 1 \pmod 4$, write $\alpha = x + y\sqrt{m}$. Then $\pm p = \mathrm{N}(\alpha) = \alpha\overline{\alpha} = x^2 - my^2$. If $m \equiv 1 \pmod 4$, write $\alpha = \frac{x+y\sqrt{m}}{2}$. Then we get a solution to $x^2 - my^2 = \pm 4p$. Suppose $\mathbb{Q}(\sqrt{m})$ has unique factorization. Let p be a rational prime with $\gcd(p, 2m) = 1$ and $\left(\frac{m}{p}\right) = 1$. (By Theorem 5.51(c), since m is odd, use $\gcd(p, 2m)$ to make sure p is odd prime.) Then if $m \not\equiv 1 \pmod 4$, we get a solution to one of the equation $x^2 - my^2 = \pm p$; if $m \equiv 1 \pmod 4$, we get a solution to one of the equation $x^2 - my^2 = \pm 4p$.

5.0.2 The field $\mathbb{Q}(\sqrt{-3})$

Example 5.52. Find primes in $\mathbb{Q}(\sqrt{-3})$. Factor $2, 3, 5, 7, \cdots$ in $\mathbb{Q}(\sqrt{-3})$. Let $m = -3$. Then $2m = -6$. Find p such that $\gcd(p, 2m) = 1$ or $\gcd(p, 6) = 6$. Since $\left(\frac{-3}{p}\right) = \begin{cases} -1 & \text{if } p = 3k+2 \\ 1 & \text{if } p = 3k+1 \end{cases}$, we have rational primes of the form $p = 3k + 2$ are primes in $\mathbb{Q}(\sqrt{-3})$, and rational primes of the form $p = 3k + 1$ factor in prime product $\pi_1\pi_2$ uniquely up to associates in $\mathbb{Q}(\sqrt{-3})$, where

$$\begin{cases} \pi_1 &= \frac{a_p+b_p\sqrt{-3}}{2} \\ \pi_2 &= \frac{a_p-b_p\sqrt{-3}}{-2} \end{cases}.$$

We can show 2 is not prime by contradiction. Consider $p = 3$. Since $3 = \frac{3+\sqrt{-3}}{2}\frac{3-\sqrt{-3}}{2}$, $3 = \sqrt{-3}\sqrt{-3}$ and $\sqrt{-3}$ are prime, we have $\sqrt{-3} \sim \frac{3+\sqrt{-3}}{2}$, where $\sim$ denote "associate". Or since $\frac{3+\sqrt{-3}}{2} = \sqrt{-3}\frac{1-\sqrt{-3}}{2}$ and $\frac{1-\sqrt{-3}}{2} \in \mathcal{O}_{\mathcal{K}}^{\times}$, we have $\sqrt{-3} \sim \frac{3+\sqrt{-3}}{2}$. We have that 6 units in $\mathbb{Q}(\sqrt{-3})$ are $\pm 1, \frac{1\pm\sqrt{-3}}{2}, \frac{-1\pm\sqrt{-3}}{2}$. Write from now on $\theta = \sqrt{-3}$. Set $w = \frac{-1+\sqrt{-3}}{2}$. Then θ has 6 associates $\pm(1-w),\ \pm(1-w^2),\ \pm(w-w^2),\ \pm\theta$.

Lemma 5.53. Every integer in $\mathcal{K} = \mathbb{Q}(\theta)$ is congruent to 0 or $-1, 1$ modulo θ.

Proof. Let $\frac{a+b\theta}{2} \in \mathcal{O}_{\mathcal{K}}$. Then a, b are of the same parity. So $\frac{b+a\theta}{2} \in \mathcal{O}_{\mathcal{K}}$. Since $\theta^2 = -3$, we have $\frac{a+b\theta}{2} = \frac{b+a\theta}{2}\theta + 2a \equiv 2a \pmod\theta$. Note $2a \equiv 0, \pm 1 \pmod 3$. Since $\theta \mid 3$, $\frac{a+b\theta}{2} \equiv 2a \equiv 0, \pm 1 \pmod\theta$. ☐

Lemma 5.54. Let $\mathcal{K} = \mathbb{Q}(\theta)$. Let $\xi, \eta \in \mathcal{O}_{\mathcal{K}}$, not divisible by θ.

(a) If $\xi \equiv 1 \pmod\theta$, then $\xi^3 \equiv 1 \pmod{\theta^4}$.

(b) If $\xi \equiv -1 \pmod{\theta}$, then $\xi^3 \equiv -1 \pmod{\theta^4}$.

(c) If $\xi^3 + \eta^3 \equiv 0 \pmod{\theta}$, then $\xi^3 + \eta^3 \equiv 0 \pmod{\theta^4}$.

(d) If $\xi^3 - \eta^3 \equiv 0 \pmod{\theta}$, then $\xi^3 - \eta^3 \equiv 0 \pmod{\theta^4}$.

Proof. (a) If $\xi \equiv 1 \pmod{\theta}$, we can write $\xi = 1 + \beta\theta$ for some $\beta \in \mathcal{O}_{\mathcal{K}}$. Since $\theta^2 = -3$ and $\theta^4 = 9$, we have

$$\xi^3 = (1+\beta\theta)^3 = 1 + 3\beta\theta - 9\beta^2 + \beta^3\theta^3 \equiv 1 + 3\beta\theta + \beta^3\theta^3 \equiv 1 + \theta^3(\beta^3 - \beta) \pmod{\theta^4}.$$

Since $\beta^3 - \beta = \beta(\beta-1)(\beta+1)$, we have $\theta \mid \beta(\beta-1)(\beta+1)$ by Lemma 5.53. So $\xi^3 \equiv 1 \pmod{\theta^4}$.

(b) If $\xi \equiv -1 \pmod{\theta}$, then $-\xi \equiv 1 \pmod{\theta}$. Then by part (a), $-\xi^3 \equiv (-\xi)^3 \equiv 1 \pmod{\theta^4}$. So $\xi^3 \equiv -1 \pmod{\theta^4}$.

(c) Since $\theta \mid \xi(\xi-1)(\xi+1)$, we have $\xi^3 \equiv \xi \pmod{\theta}$. Similarly, $\eta^3 \equiv \eta \pmod{\theta}$. If $\xi^3 + \eta^3 \equiv 0 \pmod{\theta}$, then $\xi + \eta \equiv 0 \pmod{\theta}$, i.e., $\xi \equiv -\eta \pmod{0}$. If $\xi \equiv -1 \pmod{\theta}$, then $\eta \equiv 1 \pmod{\theta}$. So $\xi^3 \equiv -1 \pmod{\theta^4}$ and $\eta^3 \equiv 1 \pmod{\theta^4}$. Hence $\xi^3 + \eta^3 \equiv -1 + 1 \equiv 0 \pmod{\theta^4}$. Similarly, we have the cases $\xi \equiv 0 \pmod{\theta}$ and $\xi \equiv 1 \pmod{\theta}$

(d) Play the same game to get the result. □

Lemma 5.55. Let $\mathcal{K} = \mathbb{Q}(\theta)$. Let $\alpha, \beta, \gamma \in \mathcal{O}_{\mathcal{K}}$ such that $\alpha^3 + \beta^3 + \gamma^3 = 0$. If $\gcd(\alpha, \beta, \gamma) = 1$, then θ divides one of them.

Proof. Suppose θ divides none of them. Then $\alpha, \beta, \gamma \equiv \pm 1 \pmod{\theta}$. So $0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\theta^4}$. Then θ^4 must divide $3,\ 1,\ -1$ or -3. But $\theta^4 = 9$, which is a contradiction. □

Lemma 5.56. Let $\mathcal{K} = \mathbb{Q}(\theta)$. Let $\alpha, \beta, \gamma \in \mathcal{O}_{\mathcal{K}} \setminus \{0\}$ such that $\theta \nmid \alpha\beta\gamma$. Let ϵ_1, ϵ_2 be units and $r \in \mathbb{N}$ such that $\alpha^3 + \epsilon_1\beta^3 + \epsilon_2(\theta^r\gamma)^3 = 0$. Then $\epsilon_1 = \pm 1$ and $r \geqslant 2$.

Proof. Since $\alpha, \beta \in \mathcal{O}_{\mathcal{K}} \setminus \{0\}$, we have $\alpha, \beta \equiv \pm 1 \pmod{\theta}$. By previous Lemma 5.54(a) and (b), $\alpha^3, \beta^3 \equiv \pm 1 \pmod{\theta^4}$. Since $r > 0$, we have $0 \equiv \alpha^3 + \epsilon_1\beta^3 \equiv \pm 1 \pm \epsilon_1 \pmod{\theta^3}$. Since ϵ is one of $\pm 1, \pm w, \pm w^2$, we have $\pm 1 \pm \epsilon_1$ is one of $2, 0, -2, \pm(1 \pm w), \pm(1 \pm w^2)$ with all possible sign combinations. Since $1 - w$ and $1 - w^2$ are associates of θ and $\theta^2 = -3$ is prime, we have θ^3 cannot divide them. Also, $1 + w = -w^2 \in \mathcal{O}_{\mathcal{K}}^{\times}$ and $1 + w^2 = -w \in \mathcal{O}_{\mathcal{K}}^{\times}$, so θ^3 cannot divide them. Since $\mathrm{N}(\pm 2) = 4$ and $\mathrm{N}(\theta^3) = 27$, we have $\mathrm{N}(\theta^3) \nmid \mathrm{N}(\pm 2)$. So $\theta^3 \nmid \pm 2$. Hence the only possibility is $\pm 1 \pm \xi_1 = 0$. So $\epsilon_1 = \pm 1$. Since $\theta \mid \theta^3$ and $\alpha^3 + \epsilon_1\beta^3 \equiv 0 \pmod{\theta^3}$, we have $\alpha^3 + \beta^3 \equiv 0 \pmod{\theta}$ and $\alpha^3 - \beta^3 \equiv 0 \pmod{\theta}$. Since $\theta \mid \alpha(\alpha-1)(\alpha+1)$, we have $\alpha^3 \equiv \alpha \pmod{\theta}$. Similarly, $\beta^3 \equiv \beta \pmod{\theta}$. By Lemma 5.54(c), $\alpha^3 + \epsilon_1\beta^3 \equiv 0 \pmod{\theta^4}$. Then $\epsilon_2(\theta^r\gamma)^3 \equiv 0 \pmod{\theta^4}$. So $\theta^4 \mid \epsilon_2(\theta^r\gamma)^3$. Thus, $r \geqslant 2$. □