# Number Theory

Ikhan Choi

October 1, 2024

# Contents

# Part I

# Elementary number theory

# Chapter 1

# Quadratic reciprocity

## 1.1 Congruence

**1.1** (Computation with binomial theorem)**.**

**1.2** (Fermat's little theorem)**.** and Euler theorem

$$a^p \equiv a \pmod{p}. \qquad a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Wilson's theorem $(n-1)! \equiv -1 \pmod{n}$.

## 1.2 Quadratic residue

**1.3.**

$$x^2 \equiv 0, 1 \pmod{3, 4}$$
$$x^2 \equiv 0, 1, 4 \pmod{5, 8}$$
$$x^2 \equiv 0, 1, 3, 4 \pmod{6}$$
$$x^2 \equiv 0, 1, 2, 4 \pmod{7}$$
$$x^2 \equiv 0, 1, 4, 7 \pmod{9}$$
$$x^2 \equiv 0, 1, 4, 9 \pmod{12}$$

**1.4** (Supplental laws)**.** Let $p$ be an odd prime.

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

(b) $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$.

(c) $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

(d) $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{5}$.

**1.5** (Euler's criterion)**.**

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

**1.6** (Quadratic Gauss sum)**.** Let $p$ be an odd prime. The *quadratic Gauss sum* is

$$\tau_p := \sum_{n=0}^{p-1} \zeta_p^{n^2},$$

where $\zeta_p := e^{2\pi i/p}$ is a primitive $p$th root of unity in any field. Define $p^* := (-1)^{\frac{p-1}{2}} p$.

(a) We have

$$\tau_p = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a.$$

(b) We have

$$\tau_p^2 = p^*.$$

**1.7** (Quadratic reciprocity)**.** Let $\ell$ be an odd prime and consider field extensions $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\tau_\ell)$. Here $L := \mathbb{Q}(\tau_\ell)$ and $K := \mathbb{Q}$.

Let $p$ be an odd prime with $p \neq \ell$. Then, $L_p$ is an unramified extension of $K_p$.(maybe) We are interested in a criterion for $p$ to split in $\mathbb{Q}(\tau_\ell)$. Note that $p$ splits in $\mathbb{Q}(\tau_\ell)$ if and only if the Frobenius homomorphism in $\mathrm{Gal}(l_p/k_p)$ is the identity.

Note that the residue field $k_p = \mathbb{F}_p$ of the local field $K_p = \mathbb{Q}_p$ has $q = p$ elements. Note that $\sigma_q : x \mapsto x^q$ gives rise to a field automorphism of $\mathrm{Gal}(\mathbb{Q}(\tau_\ell)/\mathbb{Q})$, called the *Frobenius automorphism*.

(a) From the Gauss sum, we have

$$\sigma_p(\tau_\ell) = \left(\frac{p}{\ell}\right) \tau_\ell.$$

(b) From the Euler criterion, we have

$$\sigma_p(\tau_\ell) = \left(\frac{\ell^*}{p}\right) \tau_\ell.$$

*Proof.* (a) We have

$$\sigma_p(\tau_\ell) = \sigma_p\left(\sum_{a=0}^{\ell-1} \left(\frac{a}{\ell}\right) \zeta_\ell^a\right) = \sum_{a=0}^{\ell-1} \left(\frac{a}{\ell}\right) \zeta_\ell^{ap} = \sum_{a=0}^{\ell-1} \left(\frac{p}{\ell}\right)\left(\frac{ap}{\ell}\right) \zeta_\ell^{ap} = \left(\frac{p}{\ell}\right) \tau_\ell$$

(b) By the Euler criterion, we have

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

□

## 1.3 Binary quadratic forms

Reduced forms Indefinite forms

Ideal class group

**1.8** (Heegner number)**.** There are only nine numbers

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

## Exercises

**1.9** (Dirichlet theorems by quadratic reciprocity)**.** (a) For $f(x) \in \mathbb{Z}[x]$, there exist infinitely many primes $p$ such that $p \mid f(x)$ for some $x$.

(b) There are infinitely many primes $p$ such that $p \equiv 1 \pmod 4$.

**1.10.** $y^2 = f(x)$

Higher order sides: At least a prime divisor of $f$ with a congruence (e.g. $4k+3$) Quantratic sides: Every prime divisor of $f$ must satisfy a congruence (e.g. $4k+1$)

**1.11** (Primes of the form $x^2 - ny^2$)**.** (It is a very important problem in listing primes in $\mathcal{O}_K$) (Want to describe the surjective homomorphism $\mathrm{Spec}\,\mathbb{Z}[i] \to \mathrm{Spec}\,\mathbb{Z}$)

# Chapter 2

# Multiplicative number theory

## 2.1 Arithmetic functions

## 2.2 Dirichlet theorem

## 2.3 Prime number theorem

# Chapter 3

# Algebraic numbers

## Exercises

**3.1** (Mordell equation with no solutions)**.** $k = 7, -5, -6, 45, 6, 46, -24, -3, -9, -12$.

(a) $y^2 = x^3 + 7$ has no integral solutions.

*Proof.* (a) Taking mod 8, $x$ is odd and $y$ is even. The factorization

$$y^2 + 1 = (x+2)((x-1)^2 + 3),$$

implies the existence of a prime factor $p = 4k+3$ of $y^2+1$, which is impossible, so the equation has no solutions. □

**3.2** (Mordell equation with solutions)**.** (a) $y^2 = x^3 - 2$ has only two solutions.

*Proof.* (a) Taking mod 8, $x$ and $y$ are odd. Consider a ring of algebraic integers $\mathbb{Z}[\sqrt{-2}]$. Write $N = N_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}$. The equation is factorized into

$$x^3 = (y - \sqrt{-2})(y + \sqrt{-2}).$$

Let $\delta$ be a common divisor of $y \pm \sqrt{-2}$. Then $\delta \mid 2\sqrt{-2}$ implies $N(\delta) \mid N(2\sqrt{-2}) = 8$, and since $N(\delta) \mid N(y - \sqrt{-2}) = x^3$ is odd, we have $N(\delta) = 1$ and $\delta$ is a unit. It means that $y \pm \sqrt{-2}$ are relatively prime. Since the units in $\mathbb{Z}[\sqrt{-2}]$ are $\pm 1$, which are all cubes, $y \pm \sqrt{-2}$ are cubes in $\mathbb{Z}[\sqrt{-2}]$.

Let

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a(a^2 - 6b^2) + b(3a^2 - 2b^2)\sqrt{-2},$$

so that $1 = b(3a^2 - 2b^2)$. We can conclude $b = \pm 1$. The possible solutions are $(x, y) = (3, \pm 5)$, which are in fact solutions. □

## Problems

1. Show that if $(x^2 + y^2 + z^2)/(xy + yz + zx)$ is a well-defined integer for integers $x, y, z$, then it is not divided by three.
2. There is no non-trivial integral solution of $x^4 - y^4 = z^2$.

# Part II

# Diophantine equations

# Chapter 4

# Pell equation

## 4.1 Continued fraction

Diophantine approximation, Thue theorem

## 4.2

Ellipse is reduced by finitely many computations.

Especially for hyperbola, here is a strategy to use infinite descent.

(a) Let midpoint to be origin.

(b) Find the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ preserving the image of hyperbola(which would be isomorphic to $\mathbb{Z}$).

(c) Find an impossible region.

(d) Assume a solution and reduce it to the either impossible region or the ground solution.

**Example 4.2.1** (Pell's equation)**.** Consider

$$x^2 - 2y^2 = 1.$$

A generator of hyperbola generating group is $g = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$. It has a ground solution $(1,0)$ and impossible region $1 < x < 3$. If $(a,b)$ is a solution with $a > 0$, then we can find $n$ such that $g^n(a,b)$ is in the region $[1,3)$. The possible case is $g^n(a,b) = (1,0)$.

**Example 4.2.2** (IMO 1988, the last problem)**.** Consider a family of equations

$$x^2 + y^2 - kxy - k = 0.$$

By the vieta jumping, a generator is $g : (a,b) \mapsto (b, kb-a)$. It has an impossible region $xy < 0$ : $x^2+y^2-kxy-k \geq x^2+y^2 > 0$. If $(a,b)$ is a solution with $a > b$, then we can find $n$ such that $g^n(a,b)$ is in the region $xy \leq 0$. Only possible case is $g^n(a,b) = (\sqrt{k}, 0)$ or $g^n(a,b) = (0, -\sqrt{k})$. In ohter words, the equation has a solution iff $k$ is a perfect square.

In general, the transformation $(x,y) \mapsto (y, ky-x)$ preserving the image of hyperbola is not easy to find. A strategy to find it in this problem is called the *Vieta jumping* or *root flipping*. It gets the name by the following reason: If $(a,b)$ is a solution with $a > b$, then a quadratic equation

$$x^2 - kbx + b^2 - k = 0$$

has a root $a$, and the other root is $kb-a$ so that $(b, kb-a)$ is also a solution. The last problem is from the International Mathematical Olympiad 1988, and the Vieta jumping technique was firstly used to solve it.

# Chapter 5

# Local-global principle

## 5.1 $p$-adic numbers

Let $p \in \mathbb{Z}$ be a prime. The ring of the $p$-adic integers $\mathbb{Z}_p$ is defined by the inverse limit:

$$\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

We may define the local field $\mathbb{Q}_p$ as $\operatorname{Frac}\mathbb{Z}_p$, or by the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, where $|\cdot|_p$ is an absolute value on $\mathbb{Q}$ such that $|p^m a|_p = \frac{1}{p^m}$. Then, $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \le 1\}$.

**Example 5.1.1.** Let $p = 5$. Observe

$$\begin{aligned} 3^{-1} &\equiv 2_5 \pmod 5 \\ &\equiv 32_5 \pmod{5^2} \\ &\equiv 132_5 \pmod{5^3} \\ &\vdots \\ &\equiv 1313132_5 \pmod{5^7}. \end{aligned}$$

Therefore, we can write

$$3^{-1} = \overline{132}_5 = 2 + 3p + p^2 + 3p^3 + p^4 + \cdots.$$

Since there is no term of negative power of 5, the number $3^{-1}$ is a 5-adic integer.

**Example 5.1.2.** Let $p = 3$.

$$\begin{aligned} 7 &\equiv 1_3^2 \pmod 3 \\ &\equiv 111_3^2 \pmod{3^3} \\ &\equiv 20111_3^2 \pmod{3^5} \\ &\equiv 120020111_3^2 \pmod{3^9}\cdots. \end{aligned}$$

Therefore, we can write

$$\sqrt{7} = \cdots 120020111_3 = 1 + p + p^2 + 2p^4 + 2p^7 + p^8 + \cdots.$$

Since there is no term of negative power of 2, $\sqrt{7}$ is a 3-adic integer.

**5.1.** (a) The absolute value $|\cdot|_p$ is nonarchimedean: it satisfies $|x+y|_p \le \max\{|x|_p, |y|_p\}$.

(b) Every triangle in $\mathbb{Q}_p$ is isosceles.

(c) $\mathbb{Z}_p$ is a discrete valuation ring: it is local PID.

(d) $\mathbb{Z}_p$ is open and compact. Hence $\mathbb{Q}_p$ is locally compact Hausdorff.

*Proof.* $\mathbb{Z}_p$ is open clearly. Let us show limit point compactness. Let $A \subset \mathbb{Z}_p$ be infinite. Since $\mathbb{Z}_p$ is a finite union of cosets $p\mathbb{Z}_p$, there is $\alpha_0$ such that $A \cap (\alpha_0 + p\mathbb{Z}_p)$ is infinite. Inductively, since

$$\alpha_n + p^{n+1}\mathbb{Z}_p = \bigcup_{1 \le x < p} (\alpha_n + xp^{n+1} + p^{n+2}\mathbb{Z}_p),$$

we can choose $\alpha_{n+1}$ such that $\alpha_n \equiv \alpha_{n+1} \pmod{p^{n+1}}$ and $A \cap (\alpha_{n+1} + p^{n+2}\mathbb{Z}_p)$ is infinite. The sequence $\{\alpha_n\}$ is Cauchy, and the limit is clearly in $\mathbb{Z}_p$. □

## 5.2 Hasse-Minkowski theorem

**Theorem 5.2.1** (Sum of two squares)**.** *A positive integer $m$ can be written as a sum of two squares if and only if $v_p(m)$ is even for all primes $p \equiv 3 \pmod 4$.*

*Let $p$ be a prime with $p \equiv 1 \pmod 4$. Every $p$-adic integer is a sum of two squares of $p$-adic integers.*

# Chapter 6

# Elliptic curves

## 6.1 Elliptic curves over $\mathbb{C}$

$\mathbb{P}^2(\mathbb{C})$

**6.1** (Weierstrass form)**.** Let $K$ be a field. An *elliptic curve* over $K$ is a smooth algebraic curve $E$ of genus one together with a specified base point $O$. There is an embedding $w : E \to \mathbb{P}^2$ such that $O$ is mapped to the infinity $(0 : 1 : 0)$ on the $y$-axis and $w(E)$ is the zero set of $y^2z - x^3 + 27c_4xz^2 + 54c_6z^3$.

**6.2** (Legendre form)**.** $E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is a double cover ramified over the four points $0, 1, \lambda, \infty \in \mathbb{P}^1(\mathbb{C})$.

**6.3** (Invariants of elliptic curves)**.** discriminant, $j$-invariant.

**6.4** (Group law)**.** from tangent lines, from Picard group, from quotient of the complex plane,

**6.5** (Isogenies)**.** If a morphism $E_1 \to E_2$ maps $O_1$ to $O_2$, then it is a group isomorphism. dual isogeny,

**6.6** (Tate modules)**.** Let $K$ be a field of characteristic $p$ and $E$ be an elliptic curve over $K$. The set $E[m]$ of points of order $m$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$, where $m$ is prime to the characteristic of $K$. For a prime $\ell \in \mathbb{Z}$ such that $p \neq 0$, the *$\ell$-adic Tate module* is the group $T_\ell(E) := \lim_{\leftarrow n} E[\ell^n]$. As a $\mathbb{Z}_\ell$-module, we have $T_\ell(E) \cong \mathbb{Z}_\ell^2$ and $T_p(E) \cong 0$ or $\mathbb{Z}_p$ if $p > 0$. Then, we can associated a representation $G_{\overline{K}/K} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $G_{\overline{K}/K} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ by tensoring with $\mathbb{Q}_\ell$.

Let $\mu_{\ell^n}$ be the group of $\ell^n$-th roots of unity in $\overline{K}^\times$. Then, we can also define a Tate module $T_\ell(\mu)$ as the projective limit, and it is a multiplicative subgroup of $\overline{K}^\times$ such that $T_\ell(\mu) \cong \mathbb{Z}_\ell$. Thus the one-dimensional Galois representation $G_{\overline{K}/K} \to \mathrm{Aut}(\mathbb{Z}_\ell) = \mathbb{Z}_\ell^\times$, called the *cyclotomic representation*.

The group of torsion points are homology groups which admit Galois actions. ($E[m]$ and $T_\ell(E)$ can be identified with $H_1(E, \mathbb{Z}/m\mathbb{Z})$ and $H_1(E, \mathbb{Z}_\ell)$.)

**6.7** (Weil pairing)**.**

**6.8** (Endomorphism rings)**.** central simple algebras over $K$ is classified by the Brauer group $\mathrm{Br}(K) = H^2(G_{\overline{K}/K}, \overline{K}^\times)$.

**6.9** (Automorphism groups)**.** The order of $\mathrm{Aut}(E)$ divides 24. $\mathrm{Aut}(E)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/6\mathbb{Z}$ over $\overline{K}$ of characteristic not 2 or 3.

**Step 1.** The Riemann-Roch theorem proves that every curve of genus 1 with a specified base point can be described by the first kind of Weierstrass equation. Explicitly, the first form of Weierstrass equation is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

$$b_2 := a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6.$$

$$y \mapsto y - \frac{1}{2}(a_1x + a_3).$$

$$y^2 = x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}b_6.$$

$$c_4 := b_2^2 - 24b_4, \quad c_6 := -b_2^3 + 36b_2b_4 - 216b_6.$$

$$x \mapsto x - \frac{1}{12}b_2.$$

$$y^2 = x^3 - \frac{1}{48}c_4x - \frac{1}{864}c_6.$$

$$b_8 := a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 = \frac{b_2b_6 - b_4^2}{4}.$$

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728}, \quad j := c_4^3/\Delta.$$

**Theorem 6.1.1.** *Let*

$$E : y^2 = x^3 - Ax - B.$$

*TFAE:*

(a) *A point $(x, y)$ is a singular point of $E$.*

(b) *$y = 0$ and $x$ is a double root of $x^3 - Ax - B$.*

(c) *$\Delta = 0$.*

*Proof.* (1)⇒(2) $\partial_y f = 0$ implies $y = 0$. $f = \partial_x f = 0$ implies $x$ is a double root of $x^3 - Ax - B$. $A$ determines whether $x$ is either cusp of node. □

$\mathbb{C}/\Lambda$

**6.10** (Invariant differential)**.** The invariant differential $\omega$ is a one-form that is invariant under the translation, which is unique up to scalar. If we consider a projective embedding $E \to \mathbb{P}^2$ such that $E(\mathbb{C})$ is given by the equation $y^2 = f(x)$ for a cubic $f \in \mathbb{C}[x]$, then we can set $\omega = dx/y$. This implies that the second coordinate is equal to the first coordinate, the Weierstrass $\wp$-function, in the embedding. (Since $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ is a group homomorphism and $dz$ is the invariant differential on $\mathbb{C}/\Lambda$, we have $dz = \phi^*(dx/y)$, so $(\wp(x) : \wp'(z) : 1)$.)

## 6.2 Elliptic curves over $\mathbb{Q}$

Finitely generatedness:Mordell-Weil, Mazur torsion Integral solutions:Nagell-Lutz, Siegel, Baker's bound

## 6.3 Elliptic curves over $\mathbb{F}_p$