Number Theory

Ikhan Choi

February 29, 2024

Contents

I Quadratic reciprocity 3

1 Congruence 4
- 1.1 . . . 4
- 1.2 Quadratic residue . . . 4

2 6

3 Binary quadratic forms 7
- 3.1 Reduced forms . . . 7
- 3.2 Indefinite forms . . . 7
- 3.3 Ideal class group . . . 7

II Multiplicative number theory 8

4 Arithmetic functions 9

5 Dirichlet's theorem 10

6 Prime number theorem 11

III Quadratic Diophantine equations 12

7 Pell's equation 13
- 7.1 Continued fraction . . . 13
- 7.2 . . . 13

8 p-adic numbers 15
- 8.1 Hensel lemma . . . 15

9 Local-global principle 17
- 9.1 Hasse-Minkowski theorem . . . 17

IV Elliptic curves 18

10 Elliptic curves over $\mathbb{C}$ 19
- 10.1 $\mathbb{P}^2(\mathbb{C})$ . . . 19
- 10.2 $\mathbb{C}/\Lambda$ . . . 20

11 Elliptic curves over $\mathbb{Q}$ **21**
11.1 Finitely generatedness 21
11.2 Integral solutions 21

12 Elliptic curves over $\mathbb{F}_p$ **22**

Part I

Quadratic reciprocity

Chapter 1

Congruence

1.1

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 pth 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 p and q be distinct odd primes. Let L be the splitting field of $x^p - 1$ over $\mathbb{F}_q$. Let $\zeta_p \in L$ be a primitive p-th root of unity. Define $p^* := (-1)^{\frac{p-1}{2}} p$ and write

$$\sqrt{p^*} := \sum_{n=0}^{p-1} \zeta_p^{n^2} \in L.$$

Note that $\sigma_q : L \to L : x \mapsto x^q$ is a field automorphism.

(a) From the Gauss sum, we have

$$\sigma_q(\sqrt{p^*}) = \left(\frac{q}{p}\right) \sqrt{p^*}.$$

(b) From the Euler criterion, we have

$$\sigma_q(\sqrt{p^*}) = \left(\frac{p^*}{q}\right) \sqrt{p^*}.$$

Proof. (a) We have

$$\sigma_q(\sqrt{p^*}) = \sigma_q\left(\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a\right) = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{aq} = \sum_{a=0}^{p-1} \left(\frac{q}{p}\right)\left(\frac{aq}{p}\right) \zeta_p^{aq} = \left(\frac{q}{p}\right) \sqrt{p^*}$$

(b) By the Euler criterion, we have

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

□

Exercises

1.8 (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 $p \equiv 1 \pmod 4$.

1.9. $y^2 = f(x)$

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. $4k+1$)

1.10 (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 $\operatorname{Spec}\mathbb{Z}[i] \to \operatorname{Spec}\mathbb{Z}$)

Problems

1. Show that if $\frac{x^2+y^2+z^2}{xy+yz+zx}$ is an integer, then it is not divided by three.
2. There is no non-trivial integral solution of $x^4 - y^4 = z^2$.

Chapter 2

Chapter 3

Binary quadratic forms

3.1 Reduced forms

3.2 Indefinite forms

3.3 Ideal class group

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

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

Exercises

3.2 (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. $\square$

3.3 (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 δ 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 δ is a unit. It means that $y \pm \sqrt{-2}$ are relatively prime. Since the units in $\mathbb{Z}[\sqrt{-2}]$ are ± 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. $\square$

Part II

Multiplicative number theory

Chapter 4

Arithmetic functions

Chapter 5

Dirichlet’s theorem

Chapter 6

Prime number theorem

Part III

Quadratic Diophantine equations

Chapter 7

Pell's equation

7.1 Continued fraction

Diophantine approximation, Thue theorem

7.2

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 7.2.1 (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 7.2.2 (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 8

p-adic numbers

8.1 Hensel lemma

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 8.1.1. 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

$$3^{-1} = \overline{13}2_5 = 2 + 3p + p^2 + 3p^3 + p^4 + \cdots.$$

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

Example 8.1.2. 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.

8.1. (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 α_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 α_{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 $\mathbb{Z}_p$. $\square$

Chapter 9

Local-global principle

9.1 Hasse-Minkowski theorem

Theorem 9.1.1 (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.

Part IV

Elliptic curves

Chapter 10

Elliptic curves over $\mathbb{C}$

10.1 $\mathbb{P}^2(\mathbb{C})$

10.1 (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 $y^2z - x^3 + 27c_4xz^2 + 54c_6z^3$.

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

10.3 (Invariants of elliptic curves). discriminant, j-invariant.

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

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

10.6 (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 *ℓ-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 μ_{ℓ^n} be the group of ℓ^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 $H_1(E, \mathbb{Z}_\ell)$.)

10.7 (Weil pairing).

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

10.9 (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

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

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

$$y \mapsto y - \frac{1}{2}(a_1 x + a_3).$$

$$y^2 = x^3 + \frac{1}{4}b_2 x^2 + \frac{1}{2}b_4 x + \frac{1}{4}b_6.$$

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

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

$$y^2 = x^3 - \frac{1}{48}c_4 x - \frac{1}{864}c_6.$$

$$b_8 := a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2 = \frac{b_2 b_6 - b_4^2}{4}.$$

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

Theorem 10.1.1. *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. □

10.2 $\mathbb{C}/\Lambda$

10.10 (Invariant differential)**.** The invariant differential ω 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 $(\wp(x) : \wp'(z) : 1)$.)

Chapter 11

Elliptic curves over $\mathbb{Q}$

11.1 Finitely generatedness

Mordell-Weil, Mazur torsion

11.2 Integral solutions

Nagell-Lutz, Siegel, Baker's bound

Chapter 12

Elliptic curves over $\mathbb{F}_p$