Contents

1 Elliptic curves **2**
1.1 Reduction of Weierstrass equations 2

2 Algebraic integer **4**
2.1 Quadratic integer 4
2.2 Integral basis 4
2.3 Fractional ideals 5
2.4 Frobenius element 6
2.5 Quadratic Dirichlet character 6

3 Diophantine equations **7**
3.1 Quadratic equation on a plane 7
3.2 The Mordell equations 8

4 The local-global principle **9**
4.1 The local fields 9
4.2 Hensel's lemma 10
4.3 Sums of two squares 10

5 Algebra problems **11**
5.1 Linear algebra 11
5.2 Groups 11
5.3 Rings 11
5.4 Galois theory 12

1 Elliptic curves

1.1 Reduction of Weierstrass equations

In this subsection, we want to investigate the important constants of elliptic curves such as c_4, c_6, Δ, j by calculating equations with hands.

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

Step 2. *Elimination of xy and y.* Factorize the left hand side

$$y\,(y + a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6.$$

By translation

$$\boxed{x \mapsto x, \qquad y \mapsto y - \tfrac{1}{2}(a_1x + a_3)}$$

we have

$$\begin{aligned} y^2 - (\tfrac{1}{2}(a_1x + a_3))^2 &= x^3 + a_2x^2 + a_4x + a_6, \\ y^2 &= x^3 + (\tfrac{1}{4}a_1^2 + a_2)x^2 + (\tfrac{1}{2}a_1a_3 + a_4)x + (\tfrac{1}{4}a_3^2 + a_6), \\ y^2 &= x^3 + \frac{1}{4}(a_1^2 + 4a_2)x^2 + \frac{1}{2}(a_1a_2 + 2a_4)x + \frac{1}{4}(a_3^2 + 4a_6). \end{aligned}$$

Introduce new coefficients b to write it as

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

By scaling

$$\boxed{x \mapsto x, \qquad y \mapsto \tfrac{1}{2}y}$$

we get

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

Step 3. *Elimination of x^2.* By translation

$$\boxed{x \mapsto x - \tfrac{1}{12}b_2}$$

we have

$$\begin{aligned}y^2 = 4\left(x^3 - 3\cdot\frac{1}{12}b_2x^2 + 3\cdot\frac{1}{12^2}b_2^2x - \frac{1}{12^3}b_2^3\right)\\ +b_2\left(x^2 - 2\cdot\frac{1}{12}b_2x + \frac{1}{12^2}b_2^2\right)\\ +2b_4\left(x - \frac{1}{12}b_2\right)\\ +b_6,\end{aligned}$$

so

$$\begin{aligned}y^2 &= 4x^3 + \left(4\cdot 3\cdot\frac{1}{12^2}b_2^2 - 2\cdot\frac{1}{12}b_2^2 + 2b_4\right)x + \left(-4\cdot\frac{1}{12^3}b_2^3 + \frac{1}{12^2}b_2^3 - 2\cdot\frac{1}{12}b_2b_4 + b_6\right)\\ &= 4x^3 + \frac{1}{12}\left(-b_2^2 + 24b_4\right)x + \frac{1}{216}\left(b_2^3 - 36b_2b_4 + 216b_6\right).\end{aligned}$$

Write it as

$$y^2 = 4x^3 - \frac{1}{12}c_4x - \frac{1}{216}c_6.$$

We want to match the coefficients of y^2 and x^3 but also want the coefficients of c_4x and c_6 to be integers. Iterative scaling implies

$$\begin{aligned}x \mapsto \tfrac{1}{6}x: &\qquad 216y^2 = 4x^3 - 3c_4x - c_6\\ y \mapsto \tfrac{1}{36}y: &\qquad y^2 = 24x^3 - 18c_4x - 6c_6\\ x \mapsto \tfrac{1}{6}x: &\qquad 9y^2 = x^3 - 27c_4x - 54c_6\\ y \mapsto \tfrac{1}{3}y: &\qquad y^2 = x^3 - 27c_4x - 54c_6.\end{aligned}$$

Thus, we get the famous third form of Weierstrass equation:

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{3}$$

Theorem 1.1. *Let*

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

TFAE:

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

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

(3) $\Delta = 0$.

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. □

2 Algebraic integer

2.1 Quadratic integer

Theorem 2.1. *Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for a square-free d.*

Theorem 2.2. *Let d be a square-free.*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z} & , d \equiv 2, 3 \pmod 4 \\ \mathbb{Z} + \dfrac{1+\sqrt{d}}{2}\mathbb{Z} & , d \equiv 1 \pmod 4 \end{cases}$$

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} 4d & , d \equiv 2, 3 \pmod 4 \\ d & , d \equiv 1 \pmod 4 \end{cases}$$

Example 2.1.

$$\Delta_{\mathbb{Q}(i)} = -4, \quad \Delta_{\mathbb{Q}(\sqrt{2})} = 8, \quad \Delta_{\mathbb{Q}(\gamma)} = 5, \quad \Delta_{\mathbb{Q}(\omega)} = -3$$

where $\gamma := \frac{1+\sqrt{5}}{2}$ and $\omega = \zeta_3$.

Theorem 2.3. *Let $\theta^3 = hk^2$ for h, k square-free's.*

$$\mathcal{O}_{\mathbb{Q}(\theta)} = \begin{cases} \mathbb{Z} + \theta\mathbb{Z} + \dfrac{\theta^2}{k}\mathbb{Z} & , m \not\equiv \pm 1 \pmod 9 \\ \mathbb{Z} + \theta\mathbb{Z} + \dfrac{\theta^2 \pm \theta k + k^2}{3k}\mathbb{Z} & , m \equiv \pm 1 \pmod 9 \end{cases}$$

Corollary 2.4. *If θ^3 is a square free integer, then*

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

2.2 Integral basis

Theorem 2.5. *Let $\alpha \in K$. $Tr_K(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathcal{O}_K$. $N_K(\alpha) \in \mathbb{Z}$ if and only if $\alpha \in \mathcal{O}_K$.*

Theorem 2.6. *Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of K over $\mathbb{Q}$. If $\Delta(\omega_1, \cdots, \omega_n)$ is square-free, then $\{\omega_1, \cdots, \omega_n\}$ is an integral basis.*

Theorem 2.7. *Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of K over $\mathbb{Q}$ consisting of algebraic integers. If $p^2 \mid \Delta$ and it is not an integral basis, then there is a nonzero algebraic integer of the form*

$$\frac{1}{p}\sum_{i=1}^{n} \lambda_i \omega_i.$$

2.3 Fractional ideals

Theorem 2.8. *Every fractional ideal of K is a free $\mathbb{Z}$-module with rank $[K : \mathbb{Q}]$.*

Proof. This theorem holds because $K/\mathbb{Q}$ is separable and $\mathbb{Z}$ is a PID. $\square$

2.4 Frobenius element

Consider an abelian extension L/K. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. Since L/K is Galois, the followings do not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$.

Lemma 2.9. *The following sequence of abelian groups is exact:*

$$0 \longrightarrow I(\mathfrak{P}|\mathfrak{p}) \longrightarrow D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \longrightarrow 0,$$

where $k(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$ and $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ are residue fields.

The Frobenius element is defined as an element of $D(\mathfrak{P}|\mathfrak{p})/I(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, which is a cyclic group.

Definition 2.1. For an unramified prime $\mathfrak{p} \subset \mathcal{O}_K$ so that $I(\mathfrak{P}|\mathfrak{p})$ is trivial, the Frobenius element $\phi(\mathfrak{P}|\mathfrak{p}) \in \mathrm{Gal}(L/K)$ is defined by

$$\phi_{\mathfrak{P}|\mathfrak{p}}(\mathfrak{P}) = \mathfrak{P}, \quad \text{and} \quad \phi_{\mathfrak{P}|\mathfrak{p}}(x) \equiv x^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}} \quad \text{for} \quad x \in \mathcal{O}_L.$$

The first condition is equivalent to $\phi_{\mathfrak{P}|\mathfrak{p}} \in D(\mathfrak{P}|\mathfrak{p})$. In fact, the Frobenius element is in fact a generator of the cyclic group $D(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ by the Galois theory of finite fields.

Remark. Fermat's little theorem states

$$\phi_{\mathfrak{P}|\mathfrak{p}}(x) \equiv x \pmod{\mathfrak{p}}, forx \in \mathcal{O}_K,$$

which means $\phi_{\mathfrak{P}|\mathfrak{p}}$ fixes the field $\mathcal{O}_K/\mathfrak{p}$ so that $\phi_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$.

2.5 Quadratic Dirichlet character

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D and $L = \mathbb{Q}(\zeta_D)$ be the cyclotomic field for $\zeta_D = e^{\frac{2\pi i}{D}}$.

$$\begin{array}{ccccccc} D(\mathfrak{P}/p) & \subset & \mathrm{Gal}(L/\mathbb{Q}) & \cong & (\mathbb{Z}/D\mathbb{Z})^\times & & L = \mathbb{Q}(\zeta_D) \\ & & \big\downarrow q & & \big\downarrow \chi_K = (\frac{D}{\cdot}) & & \\ D(\mathfrak{p}/p) & \subset & \mathrm{Gal}(K/\mathbb{Q}) & \cong & \{\pm 1\} & & K = \mathbb{Q}(\sqrt{D}). \end{array}$$

For $p \nmid D$ so that p is unramified, let $\sigma_p := (\zeta_D \mapsto \zeta_D^p) \in \mathrm{Gal}(L/\mathbb{Q})$. Then, what is $\sigma_p|_K$ in $\mathrm{Gal}(K/\mathbb{Q})$. In other words, for $\sigma_p(\zeta_D) = \zeta_D^p$ which is true: $\sigma_p(\sqrt{D}) = \pm\sqrt{D}$?

Note that σ satisfies the condition to be the Frobenius element: $\sigma_p = \phi_{\mathfrak{P}|p}$. Therefore, $q(\phi_{\mathfrak{P}|p}) = \phi_{\mathfrak{p}|p} = \sigma_p|_K$ is also a Frobenius element. There are only two cases:

(1) If $f = |D(\mathfrak{p}/p)| = 1$, then $\sigma|_K$ is the identity, so $\chi_K(p) = 1$

(2) If $f = |D(\mathfrak{p}/p)| = 2$, then $\sigma|_K$ is not trivial, so $\chi_K(p) = -1$

Artin reciprocity: $(\mathbb{Z}/D\mathbb{Z})^\times$ is extended to I_K^S.

3 Diophantine equations

3.1 Quadratic equation on a plane

Ellipse is reduced by finitely many computations.

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

(1) Let midpoint to be origin.

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

(3) Find an impossible region.

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

Example 3.1 (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 3.2 (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.

3.2 The Mordell equations

(The reciprocity laws let us learn not only which prime splits, but also which prime factors a given polynomial has.)

$$y^2 = x^3 + k$$

There are two strategies for the Mordell equations:

- $x^2 - 2x + 4$ has a prime factor of the form $4k + 3$
- $x^3 = N(y - a)$ for some a.

First case: $k = 7, -5, -6, 45, 6, 46, -24, -3, -9, -12$.

Example 3.3. Solve $y^2 = x^3 + 7$.

Proof. Taking mod 8, x is odd and y is even. Consider

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4).$$

Since

$$x^2 - 2x + 4 = (x - 1)^2 + 3,$$

there is a prime $p \equiv 3 \pmod 4$ that divides the right hand side. Taking mod p, we have

$$y^2 \equiv -1 \pmod p,$$

which is impossible. Therefore, the equation has no solutions. □

Example 3.4. Solve $y^2 = x^3 - 2$.

Proof. Taking mod 8, x and y are odd. Consider a ring of algebraic integers $\mathbb{Z}[\sqrt{-2}]$. We have

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

For a common divisor δ of $y \pm \sqrt{-2}$, we have

$$N(\delta) \mid N((y - \sqrt{-2}) - (y + \sqrt{-2})) = N(2\sqrt{-2}) = |(2\sqrt{-2})(-2\sqrt{-2})| = 8.$$

On the other hand,

$$N(\delta) \mid x^3 \equiv 1 \pmod 2,$$

so $N(\delta) = 1$ and δ is a unit. Thus, $y \pm \sqrt{-2}$ are relatively prime. Since the units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1, which are cubes, $y \pm \sqrt{-2}$ are cubics 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. □

4 The local-global principle

4.1 The local fields

Let $f \in \mathbb{Z}[x]$.

Does $f = 0$ have a solution in $\mathbb{Z}$?

Does $f = 0$ have a solution in $\mathbb{Z}/(p^n)$ for all n?

Does $f = 0$ have a solution in $\mathbb{Z}_p$?

In the first place, here is the algebraic definition.

Definition 4.1. Let $p \in \mathbb{Z}$ be a prime. The ring of the p-adic integers $\mathbb{Z}_p$ is defined by the inverse limit:

$$\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{F}_{p^n} \longrightarrow \cdots \longrightarrow \mathbb{Z}/(p^3) \longrightarrow \mathbb{Z}/(p^2) \longrightarrow \mathbb{F}_p.$$

Definition 4.2. $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$.

Secondly, here is the analytic definition.

Definition 4.3. Let $p \in \mathbb{Z}$ be a prime. Define a absolute value $|\cdot|_p$ on $\mathbb{Q}$ by $|p^m a|_p = \frac{1}{p^m}$. The local field $\mathbb{Q}_p$ is defined by the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Definition 4.4. $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Example 4.1. Observe

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

Therefore, we can write

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

for $p = 5$. Since there is no negative power of 5, 3^{-1} is a p-adic integer for $p = 5$.

Example 4.2.

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

Therefore, we can write

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

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

There are some pathological and interesting phenomena in local fields. Actually note that the values of $|\cdot|_p$ are totally disconnected.

Theorem 4.1. *The absolute value $|\cdot|_p$ is nonarchimedean: it satisfies $|x+y|_p \leq \max\{|x|_p, |y|_p\}$.*

Proof. Trivial. $\square$

Theorem 4.2. *Every triangle in $\mathbb{Q}_p$ is isosceles.*

Theorem 4.3. *$\mathbb{Z}_p$ is a discrete valuation ring: it is local PID.*

Proof. asdf $\square$

Theorem 4.4. *$\mathbb{Z}_p$ 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

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

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 $\mathbb{Z}_p$. $\square$

4.2 Hensel's lemma

Theorem 4.5 (Hensel's lemma)**.** *Let $f \in \mathbb{Z}_p[x]$. If f has a simple solution in $\mathbb{F}_p$, then f has a solution in $\mathbb{Z}_p$.*

Proof. asdf $\square$

Remark. Hensel's lemma says: for X a scheme over $\mathbb{Z}_p$, X is smooth iff $X(\mathbb{Z}_p) \twoheadrightarrow X(\mathbb{F}_p)$....???

Example 4.3. $f(x) = x^p - x$ is factorized linearly in $\mathbb{Z}_p[x]$.

4.3 Sums of two squares

Theorem 4.6 (Euler)**.** *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 $p \equiv 3 \pmod 4$.*

Lemma 4.7. *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.*

5 Algebra problems

5.1 Linear algebra

(1) Show that normal nilpotent matrix equals zero.

(2) Show that two matrices AB and BA have same nonzero eigenvalues whose both multiplicities are coincide blabla...

(3) Show that if A is a square matrix whose characteristic polynomial is minimal then a matrix commuting A is a polynomial in A.

(4) Show that if two by two integer matrix is a root of unity then its order divides 12.

5.2 Groups

(1) Show that a finite symmetric group has two generators.

(2) Show that a group G is abelian if $|G| = p^2$ for a prime p.

(3) Show that a group G is abelian if it has a surjective cube map.

(4) Let G be a finite group of order n and p the smallest prime divisor of n. Show that a subgroup of G of index p is normal in G.

(5) Find all n such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

(6) Show that a nontrivial normalizer of a p-group meets its center out of identity.

(7) Show that a proper subgroup of a finite p-group is a proper subgroup of its normalizer. In particular, every finite p-group is nilpotent.

(8) Show that a finite group G satisfying $\sum_{g\in G} \operatorname{ord}(g) \le 2n$ is abelian.

(9) Show that the order of a group with trivial automorphism group is either 1 or 2.

(10) Find all homomorphic images of A_4 up to isomorphism.

(11) Show that in a group of order 105 is a single Sylow p-subgroup for $p = 5, 7$.

(12) Show that the number of Sylow p-subgroups of $\mathrm{SL}_3(\mathbb{F}_p)$ is $(p^2 + p + 1)(p + 1)$.

5.3 Rings

(1) Show that the complement of a saturated monoid in a commutative ring is a union of prime ideals.

5.4 Galois theory

(1) Show that the Galois group of a quintic over $\mathbb{Q}$ having exactly three real roots is isomorphic to S_5.