BASIC NUMBER THEORY: LECTURE 5

WENHAN DAI

Recall that we have constructed a map

$$\Phi : C(D) \longrightarrow \ker \chi / H$$

that sends proper equivalence classes to genera in $\ker \chi$. By definition, note that the image of Φ is exactly the group of all genera, and $\ker \Phi$ is the group of principal genus. It turns out in Theorem 9 of Lecture 4 that

(1) the number of genera equals to the number of elements of order $\leqslant 2$ in $C(D)$, which is $2^{\mu-1}$;[1]
(2) $\ker \Phi = C(D)^2$.

To prove this, we have defined μ assigned characters to induce an isomorphism $(\mathbb{Z}/D\mathbb{Z})^\times / H \cong \{\pm 1\}^\mu$, and it follows that $\ker \chi / H \cong \{\pm 1\}^{\mu-1}$ as $\ker \chi$ is a normal subgroup of index 2 in $(\mathbb{Z}/D\mathbb{Z})^\times$. Also consider the exact sequence

$$0 \to C(D)^2 \to C(D) \xrightarrow{\Phi} \ker \chi / H \to 0.$$

Here $C(D)^2$ maps to 0 in $\ker \chi / H$ and Φ appears to be surjective. Hence $|C(D)/C(D)^2| = 2^{\mu-1}$.

1. Applications of the genus theory

We list out some example of the main theorem of genus theory.

Example 1. Let $n = 41$. Gauss had computed that $h(-4n) = 8$. Our goal is to compute $C(D)$ with assuming this fact. Since 41 is the only odd prime divisor of $D = -4n$ with $n \equiv 1 \bmod 4$, we get $r = 1$ and $\mu = r + 1 = 2$. Hence there are $2^{\mu-1} = 2$ genera in $\ker \chi / H$. By the first isomorphism theorem applying to Φ,

$$C(D)/C(D)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, we use the fact (computed by Gauss) that there are exactly 8 reduced forms with discriminant $D = -4n$:

$$A = x^2 + 41y^2,$$
$$B = 2x^2 + 2xy + 21y^2,$$
$$C = 5x^2 \pm 4xy + 9y^2,$$
$$D = 3x^2 \pm 2xy + 16y^2,$$
$$E = 6x^2 \pm 2xy + 7y^2.$$

Date: October 13, 2020.

[1]For the definition of μ, see Notation 5 in Lecture 4.

Then $|C(D)| = 8$. Recall that $C(D)$ is an abelian group, so the only possibility is that $C(D) \cong \mathbb{Z}/8\mathbb{Z}$.

Definition 2. An integer n is called a *convenient number* if each genus of discriminant $-4n$ consists of a single class.

The reader should be very careful that even if n is a convenient number, its genus can involve infinitely many quadratic forms as a set.

Lemma 3. *Fix some integer n. Let $m > 0$ be another integer such that $(m, 2n) = 1$. Then*

$$\#\{m = f(u,v) \mid f \text{ reduced form of discriminant } -4n,\ (u,v) = 1\} = 2\prod_{p|m}\left(1 + \left(\frac{-n}{p}\right)\right).$$

Proof. This is an exercise. □

Example 4 (Mordell's equation)**.** Historically, the equation $y^2 = x^3 + k$, for $k \in \mathbb{Z}$, is called Mordell's equation due to Mordell's work on it throughout his life. Our goal is to prove that the only solutions of (a variant of) Mordell's equation $x^3 = y^2 + 2$ are $(3, \pm 5)$.

(1) Let $m = a^2 + 2b^2$ be an odd integer. It factors as[2]

$$m = (a + \sqrt{-2}b)(a - \sqrt{-2}b).$$

And $(a + \sqrt{-2}b)^3 = a^3 - 6ab^2 + \sqrt{-2}(3a^b - ab^3)$. Hence

$$m^3 = (a^3 - 6ab^2) + 2(3a^b - ab^3) = x^2 + 2y^2.$$

One can check by Euclidean division algorithm that

$$(a, b) = 1 \implies (a^3 - 6ab^2, 3a^b - ab^3) = 1.$$

So we get an injective map

$$\{m = x^2 + 2y^2 \mid (x, y) = 1\} \longrightarrow \{m^3 = x^2 + 2y^2 \mid (x, y) = 1\}.$$

It can be proved that it is also surjective (not so trivial).

(2) Consider the equation $x^3 = y^2 + 2 = y^2 + 2 \cdot 1^2$ with $(y, 1) = 1$, which forces x to be odd. By Step (1), there is a unique pair (a, b) such that $(a, b) = 1$ and

$$a^3 - 6ab^2 = y, \quad 3a^b - ab^3 = 1.$$

It solves as $b = \pm 1$. Hence $y = \pm 5$ is the only solution.

As a summary, in Example 4 above, we use the trick in Step (1) to reduce the cubic invariant to that of degree one. And then the theory of quadratic form representation applies.

Remark 5. Here comes an aspect of Diophantine geometry. Siegel's theorem states that if a polynomial in n variables defines a smooth affine curve of genus > 0 in $\mathbb{A}^n_{\mathbb{Q}}$, then f has only finitely many integral points.

[2]Note that, instead of computing m^3 directly, this trick is necessary to write m^3 into the form of $x^2 + 2y^2$.

2. The cubic reciprocity

We begin with some elementary observations on the cubic residues. Let p be a prime.

- When $p = 3$, for any $n \in \mathbb{Z}$, either $3 \mid n$ or $p \nmid n$. If $3 \mid n$, then $n^3 \equiv 0 \bmod 3$ and n is a cubic residue of 3; otherwise, by Fermat's little theorem, $n^3 \equiv n \bmod 3$. Hence all integers are cubic residues modulo 3.
- When $p \equiv 2 \bmod 3$, $\mathbb{F}_p^\times$ is a cyclic group of order not dividing by 3. Hence there is no element in it with order 3. Consequently, if $x^3 \equiv 1 \bmod p$ then $x \equiv 1 \bmod p$. Hence we obtain an injective group homomorphism

$$\mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times, \quad x \longmapsto x^3,$$

  which is called *the arithmetic Frobenius modulo* 3. As two groups have the same size, the homomorphism is an isomorphism. In particular, $\mathbb{F}_p^\times \cong (\mathbb{F}_p^\times)^3$. Therefore, when $p \equiv 2 \bmod 3$, all integers are cubic residues of p.
- When $p \equiv 1 \bmod 3$, $\mathbb{F}_p^\times$ is a cyclic group of order dividing by 3. Then the polynomial $x^3 - 1$ splits in $\mathbb{F}_p^\times$.

To summarize, in the second and the third cases above, we have considered the solution of $x^3 - 1 = 0$ in $\mathbb{F}_p^\times$. This is done by considering the splitting types of the polynomial $x^3 - 1$ for different p's. When $p \equiv 2 \bmod 3$, $x^3 - 1$ has a unique linear factor and the remaining quadratic factor is irreducible over $\mathbb{F}_p$. When $p \equiv 1 \bmod 3$, $x^3 - 1$ splits completely into 3 linear factors (which are not necessarily mutually distinct).

Recall that while describing the quadratic reciprocity law, we use the Legendre symbol (or Jacobi symbol)

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \longrightarrow \{1, -1\}$$

to associate the splitting type of a polynomial $x^2 - a$ to ± 1. By observing these phenomena, we gain the following insights. To define a *cubic Legendre symbol* one must take it as

$$\left(\frac{\cdot}{p}\right)_3 : \mathbb{F}_p^\times \longrightarrow \{1, \omega, \omega^2\}$$

where $\omega = e^{2\pi i/3}$ is the nontrivial solution to $x^3 - 1 = 0$, satisfying $\omega^2 + \omega + 1 = 0$. We then define the subring of $\mathbb{C}$ by

$$\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\} \simeq \mathbb{Z}^{\oplus 2}.$$

It is a free $\mathbb{Z}$-module of rank 2. Note that it is not of rank 3 because ω^2 can be expressed as a linear combination of ω and 1. It turns out that $\mathbb{Z}[\omega]$ is an integral domain whose function field is $\mathbb{Q}(\omega) = \mathbb{Q}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Q}\}$. Moreover, $\mathbb{Z}[\omega]$ is equipped with a natural multiplicative norm map

$$N : \mathbb{Z}[\omega] \to \mathbb{Z}_{\geqslant 0}, \quad N(\alpha) := \alpha\overline{\alpha},$$

such that $N(\alpha) = 0$ if and only if $\alpha = 0$, and $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proposition 6. *The ring $\mathbb{Z}[\omega]$ is a Euclidean domain.*

Proof. By definition it is sufficient to show that for all $\alpha, \beta \in \mathbb{Z}[\omega]$ with $\beta \neq 0$, there are $\gamma, \delta \in \mathbb{Z}[\omega]$ such that $\alpha = \beta\gamma + \delta$ and $N(\delta) < N(\beta)$. On the function field, we write

$$\frac{\alpha}{\beta} = r + s\omega, \quad r, s \in \mathbb{Q}.$$

Then there are two integers $r_1, s_1 \in \mathbb{Z}$ that are the nearest to r, s, respectively, i.e., such that $|r_1 - r| \leqslant 1/2$ and $|s_1 - s| \leqslant 1/2$. We take

$$\gamma = r_1 + s_1\omega \in \mathbb{Z}[\omega], \quad \gamma - \frac{\alpha}{\beta} = (r_1 - r) + (s_1 - s)\omega.$$

It can be check that

$$N(\gamma - \frac{\alpha}{\beta}) \leqslant \frac{3}{4} = N(\alpha - \beta\gamma) < N(\beta).$$

This completes the proof. □

Corollary 7. *$\mathbb{Z}[\omega]$ is a principal ideal domain, and hence a unique factorization domain.*

Lemma 8. $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$.

Proof. Resuming on Proposition 6, in the Euclidean domain, α is a unit if and only if $N(\alpha) = 1$. Note that the complex conjugation $\overline{\omega} = \omega^2$. Hence

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2 > 0,$$

which is positive definite. Hence $N(a+b\omega) = 1$ if and only if $(a, b) = (\pm 1, 0),\ (0, \pm 1),\ \pm(1, 1)$. □

Proposition 9 (Classification of primes in $\mathbb{Z}[\omega]$)**.** *Let p be a prime. Then*

1. *If $p = 3$, then $1 - \omega$ is prime in $\mathbb{Z}[\omega]$ and $3 = -\omega^2(1 - \omega)^2$. Namely, 3 factors as $(1 - \omega)^2$ in $\mathbb{Z}[\omega]$ up to association.*[3]
2. *If $p \equiv 1 \bmod 3$, then there is a prime $\pi \in \mathbb{Z}[\omega]$ such that $p = \pi\overline{\pi}$, and the primes π and $\overline{\pi}$ are non-associate in $\mathbb{Z}[\omega]$.*
3. *If $p \equiv 2 \bmod 3$, then p remains prime in $\mathbb{Z}[\omega]$.*

Furthermore, every prime in $\mathbb{Z}[\omega]$ is associate to one of the primes listed in (1)(2)(3) above.

Proof. By definition,

$$\mathbb{Z}[\omega] \simeq \mathbb{Z}[x]/(x^2 + x + 1), \quad \mathbb{Z}[\omega]/(p) \simeq \mathbb{F}_p[x]/(x^2 + x + 1).$$

As a consequence of the second isomorphism above, the appearances of p in $\mathbb{Z}[\omega]$ is exactly described by the appearances of $x^2 + x + 1$ over $\mathbb{F}_p$. (Also recall that we are truly interested in the factorization types of $x^3 - 1 = (x-1)(x^2+x+1)$. Hence we consider the factorizations of $x^2 + x + 1$ over $\mathbb{F}_p[x]$ for variant p.)

(1) $p = 3$. In $\mathbb{F}_3[x]$, $x^2 + x + 1 \equiv (x - 1)^2$, and $\mathbb{Z}[\omega]/(p) \simeq \mathbb{F}_p[x]/(x - 1)^2$.
(2) $p \equiv 1 \bmod 3$. We have seen that $x^2 + x + 1$ splits and has two distinct roots. So $\mathbb{Z}[\omega]/(p)$ is the distinct sum of two fields.
(3) $p \equiv 2 \bmod 3$. We have seen that $x^2 + x + 1$ is irreducible. Hence $\mathbb{F}_p[x]/(x^2 + x + 1)$ is a field.

[3] In a ring R, two elements a, b are called *associate* if there is a unit $u \in R^\times$ such that $a = ub$.

Furthermore, by Corollary 7, for any prime ideal $(p) = p\mathbb{Z}[\omega]$ in the UFD $\mathbb{Z}[\omega]$, it can be written as

$$(p) = \pi_1^{r_1} \cdots \pi_m^{r_m},$$

where $\pi_1, \ldots, \pi_m$ are non-associate primes. The Chinese remainder theorem dictates that

$$\mathbb{Z}[\omega]/(p) \simeq \mathbb{Z}[\omega]/(\pi_1^{r_1}) \oplus \cdots \oplus \mathbb{Z}[\omega]/(\pi_m^{r_m}).$$

Here each direct summand can be isomorphic to one of the integral domains in (1)(2)(3). Conversely, let π be any prime in $\mathbb{Z}[\omega]$, we see $(\pi) \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, say $(p) = p\mathbb{Z}$. Then π appears in the decomposition of p. This completes the proof. □

Lemma 10. *Let (π) be a prime ideal of $\mathbb{Z}[\omega]$ appearing in the decomposition of some prime number p, as in the last paragraph in the proof of Proposition 9 above.*

1. *$\mathbb{Z}[\omega]/(\pi)$ is a finite field of cardinality $N(\pi)$.*
2. *Either $N(\pi) = p$ or $N(\pi) = p^2$. More precisely,*
   - (a) *When $p \equiv 1 \bmod 3$ or $p = 3$, $N(\pi) = p$ and $\mathbb{Z}[\omega]/(\pi) \simeq \mathbb{F}_p$.*
   - (b) *When $p \equiv 2 \bmod 3$, $N(\pi) = p^2$ and $\mathbb{Z}/p\mathbb{Z}$ is the unique subfield of order p of the field $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ of p^2 elements; namely, the following diagram commutes:*

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \hookrightarrow & \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \\ \simeq\downarrow & & \downarrow\simeq \\ \mathbb{F}_p & \hookrightarrow & \mathbb{F}_{p^2}. \end{array}$$

Proof. We only do (2). When $p = 3$, $\pi = 1 - \omega$ and $\mathbb{Z}[\omega]/(p) \simeq \mathbb{Z}[\omega]/(\pi^2)$. Then we get a short exact sequence

$$0 \longrightarrow (\pi)/(\pi^2) \longrightarrow \mathbb{Z}[\omega]/(\pi^2) \longrightarrow \mathbb{Z}[\omega]/(\pi) \longrightarrow 0.$$

$$\simeq$$

A priori we obtain $|\mathbb{Z}[\omega]/(\pi^2)| = p^2$, and hence $|\mathbb{Z}[\omega]/(\pi)| = p$.

Now suppose $p \equiv 1 \bmod 3$. Then

$$\mathbb{Z}[\omega]/(p) \simeq \mathbb{Z}[\omega]/(\pi) \oplus \mathbb{Z}[\omega]/(\overline{\pi}).$$

So that

$$|\mathbb{Z}[\omega]/(\pi^2)| = p^2 \implies |\mathbb{Z}[\omega]/(\pi)| = p.$$

Finally, assume $p \equiv 2 \bmod 3$. We obtain

$$|\mathbb{Z}[\omega]/(\pi^2)| = p^2 \implies \mathbb{Z}[\omega]/(\pi^2) \simeq \mathbb{F}_{p^2}.$$

□

Corollary 11 (Generalized Fermat's little theorem)**.** *Let π be a prime in $\mathbb{Z}[\omega]$ with $\pi \nmid \alpha \in \mathbb{Z}[\omega]$. Then*

$$\alpha^{N(\pi)-1} \equiv 1 \bmod \pi.$$

Proof. This is deduced from Lemma 10 and Lagrange's theorem. □

Now we suppose π is a prime in $\mathbb{Z}[\omega]$ that is not associate to $1-\omega$ (and therefore $3 \mid N(\pi)-1$). Then $\pi \nmid \alpha \in \mathbb{Z}[\omega]$ implies $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$. Hence

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv 1, \omega, \omega^2 \bmod \pi.$$

Note that $1, \omega, \omega^2$ are distinct modπ. Then for each α that is coprime to π,

$$\exists \left(\frac{\alpha}{\pi}\right)_3 \in \{1, \omega, \omega^2\} \text{ such that } \alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \bmod \pi.$$

Also,

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff \exists x \in \mathbb{Z}[\omega] \text{ such that } x^3 \equiv \alpha \bmod \pi.$$

To state the law of cubic reciprocity (next time), we need one final definition: a prime π is called *primary* if $\pi \equiv \pm 1 \bmod 3$. Given any prime π not dividing 3, one can show that exactly two of the six associates $\pm\pi, \pm\omega\pi$ and $\pm\omega^2\pi$ are primary.

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn