BASIC NUMBER THEORY: LECTURE 4

WENHAN DAI

1. Genus theory of Gauss (continued)

Recap. Suppose $f = ax^2+bxy+cy^2$ and $g = a'x^2+b'xy+c'y^2$ such that $D(f) = D(g) = D$ and $(a, a', (b+b')/2) = 1$. Recall that the *Dirichlet composition* of f and g is defined as

$$F(x, y) = aa'x^2 + Bxy + Cy^2,$$

where B is a unique constant modulo $2aa'$ such that $B \equiv b \bmod 2a$, $B \equiv b' \bmod 2a'$, and $B \equiv D \bmod 4aa'$, and $C = (B^2 - D)/4aa'$ is determined by B.

Proposition 1. (1) *The direct composition $F(x, y)$ is also a ppdf of discriminant D.*

(2) *The Dirichlet composition is the direct decomposition of*

$$f(x, y) \sim ax^2 + Bxy + a'Cy^2, \quad (x, y) \mapsto (x + \frac{B-b}{2a}y, y)$$

and

$$g(x, y) \sim a'x^2 + Bxy + aCy^2, \quad (x, y) \mapsto (x + \frac{B-b'}{2a'}y, y).$$

Proof. (1) It suffices to check the primitivity. This is given by the following: for each prime p, if $p \nmid f(x_0, y_0)$ and $p \nmid g(x_0, y_0)$, then $p \nmid F(X, Y) = f(x_0, y_0)g(x_0, y_0)$ for some X, Y determined by $f(x_0, y_0)$ and $g(x_0, y_0)$.

(2) We compute that

$$(ax^2 + Bxy + a'Cy^2)(a'x^2 + Bxy + aCy^2) = aa'X^2 + BXY + CY^2,$$

where by comparison on coefficients,

$$X = xz + 0 + 0 + Cyw, \quad Y = 0 + axw + a'yz + Byw.$$

Hence $a_1b_2-a_2b_1 = a$ and $a_1c_2-a_2c_1 = a'$. By definition, $F(x, y)$ is a direct composition. □

2. Form class group

Recall that we have already defined the class number $h(D)$ to be the number of proper equivalence classes of ppdfs with discriminant D. It can be interpreted as the order of some class group $C(D)$.

Definition 2 (Form class group)**.** Let $0 > D \equiv 0, 1 \bmod 4$. We set-theoretically define

$$C(D) := \{\text{ppdf of discriminant } D\}/\sim,$$

where $\sim$ denotes the proper equivalence.

Date: October 9, 2020.

The set $C(D)$ turns out to be an abelian group. It is called the *form class group*.

Theorem 3. *The Dirichlet composition induces an abelian group structure on $C(D)$. Moreover, the principal form is the identity, and the opposite (i.e. the group inverse) of $f(x) = ax^2 + bxy + cy^2$ is $f'(x) = ax^2 - bxy + cy^2$.*

Proof. Omitted. The verifications to the well-definite and the group structure are postponed to the similar theorem about the ideal class group. □

In the upcoming context we always denote f' the opposite of f in $C(D)$ (as a representative of proper equivalence class). Via the proper equivalence induced by $(x, y) \mapsto (y, -x)$, we have

$$ax^2 - bxy + cy^2 \sim cx^2 + bxy + ay^2.$$

By choosing $B = b$ and say $F(x, y) = acx^2 + bxy + y^2$, it is properly equivalent to a principal form. More precisely,

- if b is even,
$$F(x, y) \sim y^2 + (ac - \frac{b^2}{4})x^2, \quad (x, y) \mapsto (x, y - \frac{b}{2}x);$$
- if b is odd,
$$F(x, y) \sim y^2 - xy + \frac{1 - (b^2 - 4ac)}{4}x^2, \quad (x, y) \mapsto (x, y - \frac{b+1}{2}x).$$

For some numerical reason (or some deep reason which we will discuss later), people noticed that elements of order $\leqslant 2$ are truly important in $C(D)$.

Lemma 4. *Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced ppdf. Then f has order $\leqslant 2$ in $C(D)$ if and only if either of $b = 0$, $a = b$ or $a = c$ holds.*

Proof. Note that f has order $\leqslant 2$, i.e. f is either a principal form or an involution, if and only if $ax^2 + bxy + cy^2 \sim ax^2 - bxy + cy^2$. Suppose f has order $\leqslant 2$. Then by definition,

- if f is reduced, then $b = 0$;
- if f is non-reduced, then $a = c$ or $a = b$.

Conversely, if $b = 0$ then the relation $ax^2 + bxy + cy^2 \sim ax^2 - bxy + cy^2$ is trivial. In case where $a = b$ (resp. $a = c$), the proper equivalence is induced by the change of variables $(x, y) \mapsto (x - y, y)$ (resp. $(x, y) \mapsto (y, -x)$) in $\mathrm{SL}_2(\mathbb{Z})$. □

Recall that in Theorem 9 of Lecture 2, we have seen that each proper equivalence class of ppdfs with a fixed determinant can be represented by a unique reduced form. Hence the elements of $C(D)$ can be represented by different reduced forms, and $h(D) = \#C(D)$. Here comes a list of some elements for fixed determinants with small absolute values.

D	$C(D)$	Reduced forms	$\#\{$order $\leqslant 2$ elements$\}$
-20	$\mathbb{Z}/2\mathbb{Z}$	$x^2 + 5y^2,\ 2x^2 + 2xy + 3y^2$	2
-56	$\mathbb{Z}/4\mathbb{Z}$	$x^2 + 14y^2,\ 2x^2 + 7y^2,\ 3x^2 \pm 2xy + 5y^2$	2
-108	$\mathbb{Z}/3\mathbb{Z}$	$x^2 + 27y^2,\ 4x^2 \pm 2xy + 7y^2$	1
-256	$\mathbb{Z}/4\mathbb{Z}$	$x^2 + 64y^2,\ 4x^2 + 4xy + 17y^2,\ 5x^2 \pm 2xy + 13y^2$	2

Notation 5. Let $0 > D \equiv 0, 1 \bmod 4$. Define

$$r := \#\{\text{distinct odd primes dividing } D\}.$$

Also define

$$\mu = \begin{cases} r, & D \equiv 1 \bmod 4, \\ r, & D = -4n,\ n \equiv 3 \bmod 4, \\ r+1, & D = -4n,\ n \equiv 1, 2 \bmod 4, \\ r+1, & D = -4n,\ n \equiv 4 \bmod 8, \\ r+2, & D = -4n,\ n \equiv 0 \bmod 8. \end{cases}$$

With these notations, we deduce a result in counting the elements of order $\leqslant 2$ in form class groups.

Proposition 6. *Let $0 > D \equiv 0, 1 \bmod 4$. Then the form class group $C(D)$ has exactly $2^{\mu-1}$ elements of order $\leqslant 2$.*

Proof. We only do half of the proof to show the idea of counting work. The remaining cases are done by similar arguments (see Exercises). Let $D = -4n$ with $n \equiv 1 \bmod 4$. Assume $f(x, y) = ax^2 + 2bxy + cy^2$ with $D(f) = 4(b^2 - ac)$ and $n = ac - b^2$ is a reduced form. Then saying f has order $\leqslant 2$ is equivalent to $b = 0$ or $a = 2b$ or $a = c$.

- If $b = 0$, then $n = ac$ with $(a, c) = 1$ (as f is in particular primitive), may assume $a \leqslant c$. Then r is the number of distinct prime divisors for n, and there are 2^{r-1} different ways to determine a, and hence c.
- If $a = 2b$, then $b(2c - b) = n$ (note that $2c - b \geqslant 3b$). As $n \equiv 1 \bmod 4$, c is odd. Then there are 2^{r-1} ways to choose c, and a, b are determined by c and n.
- If $c = a$, then $(a + b)(a - b) = n$ (note that $a + b \leqslant 3(a - b)$). Since $n \equiv 1 \bmod 4$ and a is odd, we see there are 2^{r-1} selections.

The arguments for remaining cases are omitted. □

3. Genus theory of Gauss revisiting

As in Lemma 5(1) in Lecture 3, let H be the subgroup in $\ker \chi$ represented by principal forms. We define the map between sets

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

sending classes to genera. Recall that a genus of some coset aH is defined to be the set of *all quadratic forms of discriminant D* representing all values in aH. We infer by definition that to determine a genus of some coset H' of H, it suffices to determine all reduced forms (and hence all proper equivalence classes) with discriminant D that represent values in H'.

Lemma 7. *Φ is a group homomorphism.*

Proof. We can check that if

$$f(x, y) \mapsto H', \quad g(x, y) \mapsto H'',$$

and if F is the direct composition of f and g, then F represents values in $H'H''$. □

Corollary 8. *Let $0 > D \equiv 0, 1 \bmod 4$. Then*

(1) *All genera of forms of discriminant D consist of the same number of classes.*
(2) *The number of genera of forms of discriminant D is a power of* 2.

Proof. (1) This is basically because all fibers of a homomorphism have the same number of elements.

(2) As Φ is a group homomorphism, all genera form a subgroup of $\ker\chi/H \simeq \{\pm 1\}^m$ (for some integer m). For a principal form f with $f(x,0)=x^2$, it represents all quadratic residues modulo D. Hence H contains a subgroup $((\mathbb{Z}/D\mathbb{Z})^\times)^2$. On the other hand, $\ker\chi$ is a subgroup of $(\mathbb{Z}/D\mathbb{Z})^\times$, hence $\ker\chi/H$ embeds into $(\mathbb{Z}/D\mathbb{Z})^\times/((\mathbb{Z}/D\mathbb{Z})^\times)^2$. Therefore, any element of $\ker\chi/H$ has order $\leqslant 2$.

□

Theorem 9. (1) *The number of genera equals $2^{\mu-1}$, which is the same as the number of elements of order $\leqslant 2$ in $C(D)$.*
(2) *The group of all principal genera, i.e. the genera containing the principal forms, is isomorphic to $C(D)^2$.*

Proof. Let $p_1,\dots,p_r$ be all odd prime factors of D. Due to the quadratic reciprocity law (cf. Proposition 2(2) in Lecture 3), we define the following characters:

$$\chi_i(a) := \left(\frac{a}{p_i}\right), \quad i=1,2,\dots,r;$$

and

$$\delta(a) := (-1)^{\frac{a-1}{2}}, \quad \varepsilon(a) := (-1)^{\frac{a^2-1}{8}}, \quad 2\nmid a.$$

Note that $\chi_i(a)=1$ if and only if a is a quadratic residue modulo p_i. The *assigned characters* is the following series of μ characters, where μ is defined in Notation 5.

- $D\equiv 1 \bmod 4$: $\mu=r$, and the assigned characters are $\chi_1,\dots,\chi_r$.
- $D=-4n$: the μ assigned characters are

$$\begin{cases} \text{none}, & n\equiv 3 \bmod 4,\\ \delta, & n\equiv 1 \bmod 4,\\ \delta\varepsilon, & n\equiv 2 \bmod 4,\\ \varepsilon, & n\equiv 4 \bmod 8,\\ \delta, & n\equiv 6 \bmod 8,\\ \delta,\varepsilon, & n\equiv 0 \bmod 8. \end{cases}$$

Consider the group homomorphism defined by

$$\begin{aligned} \psi : (\mathbb{Z}/D\mathbb{Z})^\times &\longrightarrow \{\pm 1\}^\mu \\ [a] &\longmapsto \text{the } \mu\text{-tuple of evaluation of assigned characters at } [a]. \end{aligned}$$

Claim. ψ is surjective and $\ker\psi = H$.

The proof of the claim is a course assignment. Granting the claim, we see

$$\ker\chi/H \simeq \{\pm 1\}^{\mu-1},$$

because $\ker\chi \subseteq (\mathbb{Z}/D\mathbb{Z})^\times$ is of index 2. Recall that for an odd prime p, if $[p]\in\ker\chi$, then D is a quadratic residue mod p, i.e. $\left(\frac{D}{p}\right)=1$. Hence there exists a ppdf f such that $f(x_0, y_0) = p$ for some $x_0, y_0 \in \mathbb{Z}$. Consequently, for the pre-composition with this isomorphism,

$$\Phi : C(D) \twoheadrightarrow \ker \chi / H \simeq \{\pm 1\}^{\mu - 1}$$

is surjective. So $C(D)^2 \subseteq \ker \Phi$, and

$$|C(D)/C(D)^2| = \#\{\text{elements of order } \leqslant 2\}.$$

Hence we obtain a short exact sequence

$$0 \to C(D)^2 \to C(D) \to \ker \chi / H \to 0.$$

This is sufficient to show that $\ker \Phi = C(D)^2$, which is exactly isomorphic to the group of principal genera. $\square$

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