BASIC NUMBER THEORY: LECTURE 3

WENHAN DAI

Recap. Last time, we have defined the class number $h(D)$ associated to a given discriminant. This is the class number associated to the quadratic forms. We will then define the class number associated to the ideals.

1. Elementary genus theory

Definition 1. The *Jacobi symbol* is defined to be

$$\left(\frac{M}{m}\right)=\prod_{i=0}^{r}\left(\frac{M}{p_i}\right)^{t_i},\quad 2\nmid m=p_1^{t_1}\cdots p_r^{t_r},\quad (M,m)=1.$$

Proposition 2. *The Jacobi symbol enjoys the following properties.*

(1) (*Multiplication*)

$$\left(\frac{MN}{m}\right)=\left(\frac{M}{m}\right)\left(\frac{N}{m}\right),\quad \left(\frac{M}{mn}\right)=\left(\frac{M}{m}\right)\left(\frac{M}{n}\right).$$

(2) (*Quadratic reciprocity*)

$$\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}},\quad \left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}},$$

and

$$\left(\frac{M}{m}\right)\left(\frac{m}{M}\right)=(-1)^{\frac{M-1}{2}\cdot\frac{m-1}{2}}.$$

Proof. It is straightforward to check by definition and the quadratic reciprocity law. $\square$

Lemma 3. *Suppose $0\neq D\equiv 0,1 \bmod 4$. Then there exists a unique character (a group homomorphism) $\chi:(\mathbb{Z}/D\mathbb{Z})^\times\to\{\pm1\}$ such that*

$$\chi([p])=\left(\frac{D}{p}\right),\quad p\nmid 2D,$$

and

$$\chi([-1])=\begin{cases}1, & D>0;\\ -1, & D<0.\end{cases}$$

Here $[n]$ denotes the image of odd prime n along the group homomorphism $\mathbb{Z}\to(\mathbb{Z}/D\mathbb{Z})^\times$.

Proof. On Proposition 2, it suffices to prove that when $D\equiv 0,1 \bmod 4$ and m,n are odd integers such that $m\equiv n \bmod D$, then

$$(m,D)=(n,D)=1\implies\left(\frac{D}{m}\right)=\left(\frac{D}{n}\right).$$

We split the proof for this assertion in two cases.

Date: September 29, 2020.

(i) $D \equiv 1 \bmod 4$. By the quadratic reciprocity,

$$\left(\frac{D}{m}\right)\left(\frac{m}{D}\right) = (-1)^{\frac{(m-1)(D-1)}{4}} = 1 = \left(\frac{D}{n}\right)\left(\frac{n}{D}\right).$$

We then infer that

$$\left(\frac{D}{m}\right) = \left(\frac{m}{D}\right), \quad \left(\frac{D}{n}\right) = \left(\frac{n}{D}\right).$$

For $D < 0$,

$$\begin{aligned}\left(\frac{D}{m}\right) &= \left(\frac{-1}{m}\right)\left(\frac{-D}{m}\right) = (-1)^{\frac{m-1}{2}}\left(\frac{-D}{m}\right) \\ &= (-1)^{\frac{m-1}{2}\cdot(\frac{-D+1}{2}+1)}\left(\frac{m}{-D}\right) = \left(\frac{m}{-D}\right).\end{aligned}$$

And similarly,

$$\left(\frac{D}{n}\right) = \left(\frac{n}{-D}\right).$$

Thus, it is sufficient to prove for $D > 0$, in which case

$$m \equiv n \bmod D \implies \left(\frac{m}{D}\right) = \left(\frac{n}{D}\right)$$

and therefore

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

(2) $D \equiv 0 \bmod 4$. Suppose $D = 2^r D'$ for $2 \nmid D'$ and $r \geqslant 2$. In particular we have $m \equiv n \bmod 4$, so we may suppose $D' \equiv 1 \bmod 4$ (otherwise replace D' with $-D'$). By congruence relations,

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

If $r \geqslant 3$, then $m^2 \equiv n^2 \bmod 16$ and then

$$\left(\frac{2}{m}\right) = \left(\frac{2}{n}\right).$$

Otherwise $r = 2$, for which it is easy to check the equality.

The uniqueness of χ simply comes from the fact that $(\mathbb{Z}/D\mathbb{Z})^\times$ is a multiplicative cyclic group which is generated by some odd prime $[p]$. We are left to check the value for $\chi([-1])$. This is an exercise of the course. $\square$

Definition 4. Suppose $D \in \mathbb{Z}_{<0}$ is an integer that $D \equiv 0, 1 \bmod 4$. The *principal form* of discriminant D is defined as

$$\begin{cases} x^2 - \dfrac{D}{4}y^2, & D \equiv 0 \bmod 4; \\ x^2 + xy + \dfrac{1-D}{4}y^2, & D \equiv 1 \bmod 4. \end{cases}$$

Lemma 5. *Let f be a quadratic form of discriminant D.*

1. *The values in $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by principal forms of discriminant D form a subgroup $H < \ker\chi$.*
2. *The values in $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by f form a coset of H in $\ker\chi$.*

Proof. We first check that the values in $(\mathbb{Z}/D\mathbb{Z})^\times$ represented by quadratic forms lie in $\ker\chi$. Let $(m,D)=1$. Then m is represented by a form g of discriminant D. We may write $m = d^2m'$ for m' square-free. Suppose m' is represented by g (or equivalently, $\left(\frac{D}{m'}\right) = \left(\frac{D}{m}\right) = 1$ by Lemma 6 in Lecture 2). Hence D is a quadratic residue modulo m'. This shows that $\chi([m]) = \chi([m']) = 1$ when m' is odd.

(1) When $D=-4n$, the corresponding principal forms are read as x^2+ny^2. The set of these forms are closed under multiplication, because
$$(x^2+ny^2)(a^2+nb^2) = (ax+by)^2 + n(ay-bx)^2.$$
When $D\equiv 1 \bmod 4$, the corresponding principal forms are read as $x^2+xy+\frac{1-D}{4}y^2$. Note that $[4]\in(\mathbb{Z}/D\mathbb{Z})^\times$ because if $D=4k+1$ say, then $[4]\cdot[4k^2]=[4k]\cdot[4k]=[-1]\cdot[-1]=[1]$, namely 4 is invertible modulo D. Also,
$$4\left(x^2+xy+\frac{1-D}{4}y^2\right) = (2x+y)^2 - Dy^2 = z^2 - Dw^2.$$
This proves the group law of the set of representable values in $(\mathbb{Z}/D\mathbb{Z})^\times$.

(2) We first assert that given $0\neq m\in\mathbb{Z}$ and a primitive form f, then f properly represents at least one integer that is coprime to m. To prove this, note that from the primitivity, $\gcd(f(0,1), f(1,0), f(1,1)) = \gcd(c,a,a+b+c) = 1$. Thus for any prime number p, it is coprime to at least one of $f(0,1)$, $f(1,0)$, and $f(1,1)$. So the assertion holds for primes, and hence for the general integer m by Chinese remainder theorem.
   - Let $D=-4n$. Taking $m=D$ in the assertion and fix $f\sim ax^2+bxy+cy^2$ with $(a,D)=1$, $(a,b,c)=1$, and $b=2b'$. Then $a\in(\mathbb{Z}/D\mathbb{Z})^\times$, and
   $$a(ax^2+bxy+cy^2) = (ax+b'y)^2+ny^2.$$
   The right hand side is a principal form that represents a subgroup of H by (1). Then f takes values in the coset $[a]^{-1}H$ in $(\mathbb{Z}/D\mathbb{Z})^\times$.
   - The case for $D\equiv 1 \bmod 4$ is left as an exercise.

So we finish the proof of Lemma 5. $\square$

Definition 6. Let $H'=aH$ be a coset of H in $\ker\chi$. Define the *genus of H'* to be the set of all quadratic forms of discriminant D representing the values of H' modulo D. A *principal genus* is the genus that contains the principal form.

Theorem 7. *Fix $0>D\equiv 0,1 \bmod 4$. Let $p\nmid D$ be an odd prime. Then for each coset H' in $\ker\chi$, $[p]\in H'$ if and only if p can be represented by a reduced form of discriminant D in the genus of H'.*

Example 8. In the present examples, all principal genera contain a single element.

(1) For $f=x^2+6y^2$, we see $D(f)=-24$ and
$$p=x^2+6y^2 \iff p\equiv 1,7 \bmod 24.$$
It can be verified that $H=\{[1],[7]\}$ is a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z},\times)$ of $\ker\chi$ in $(\mathbb{Z}/24\mathbb{Z})^\times \simeq (\mathbb{Z}/8\mathbb{Z},\times)$.

(2) Similarly,
$$p = x^2 + 10y^2 \iff p \equiv 1, 9, 11, 29 \bmod 40.$$
Also,
$$H = \{[1], [9], [11], [29]\} \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \times)$$
$$\leqslant \ker \chi \leqslant (\mathbb{Z}/40\mathbb{Z})^\times \simeq (\mathbb{Z}/16\mathbb{Z}, \times).$$

(3) Again,
$$p = x^2 + 13y^2 \iff p \equiv 1, 9, 17, 25, 29, 49 \bmod 52,$$
and
$$H = \{[1], [9], [17], [25], [29], [49]\} \simeq (\mathbb{Z}/6\mathbb{Z}, \times)$$
$$\leqslant \ker \chi \leqslant (\mathbb{Z}/52\mathbb{Z})^\times \simeq (\mathbb{Z}/24\mathbb{Z}, \times).$$
Here $[49]$ is a generator of order 6 in H.

Historically, Fermat and Euler had discovered that
$$p, q \equiv 3, 7 \bmod 20 \implies pq = x^2 + 5y^2,$$
and
$$p \equiv 3, 7 \bmod 20 \implies 2p = x^2 + 5y^2.$$
The question would be more attractive while comparing the first relation with that $p = x^2 + 5y^2$ if and only if $p \equiv 1, 9 \bmod 20$.

2. Genus theory of Gauss

Definition 9. Let f, g be primitive positive definite forms of discriminant D. Their *composition* is defined as a new ppdf F that
$$F(B_1(x, y; z, w), B_2(x, y; z, w)) = f(x, y)g(z, w),$$
where
$$B_i(x, y; z, w) := a_i xz + b_i xw + c_i yz + d_i yw, \quad i = 1, 2.$$

Exercise 10. Check that on Definition 9,
$$a_1b_2 - a_2b_1 = \pm f(1, 0), \quad a_1c_2 - a_2c_1 = \pm g(1, 0).$$

We remark that if both signatures in Exercise 10 are $+1$, the composition is called a *direct composition* by Gauss. We then introduce a more explicit computation for the composition by following Dirichlet's approach.

Lemma 11. *Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$. Suppose*
$$(a, \frac{a + a'}{2}, \frac{b + b'}{2}) = 1, \quad D(f) = D(g) = D.$$
Then there exists a unique $B \bmod 2aa'$ such that

(1) *$B \equiv b \bmod 2a$,*
(2) *$B \equiv b' \bmod 2a'$, and*
(3) *$B^2 \equiv D \bmod 4aa'$.*

Proof. Note that

$$(1) \iff a'B \equiv a'b \bmod 2aa', \quad (2) \iff aB \equiv ab' \bmod 2aa'.$$

Summing up (1)(2), we get

$$(B-b')(B-b) = B^2 - (b'+b)B + b'b \equiv 0 \bmod 4aa'.$$

Also,

$$(3) \iff \frac{b+b'}{2}B \equiv \frac{bb'+D}{2} \bmod 2aa'.$$

Claim. Suppose $\gcd(p_1, \ldots, p_r, m) = 1$, then the system of equations

$$p_i B \equiv q_i \bmod m, \quad i = 1, \ldots, r$$

have a unique solution $B \bmod m$ if and only if $p_i q_j \equiv p_j q_i \bmod m$.

For the proof of the claim, note that $\gcd(p_1, \ldots, p_r, m) = 1$ implies that $B \bmod m$ is uniquely determined. The "only if" part is obvious, and the "if" part will be a course assignment. □

Definition 12. The *direct composition* of $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ is defined as

$$F(x,y) = aa'x^2 + Bxy + Cy^2, \quad C = \frac{B^2 - D}{4aa'},$$

where B is the unique constant modulo $2aa'$ given by Lemma 11.

Proposition 13. *The direct composition $F(x,y)$ is also a ppdf of discriminant D.*

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