BASIC NUMBER THEORY: LECTURE 18

WENHAN DAI

An introduction to complex multiplication

We first introduce elliptic functions.

Definition 1. Let $L = [\omega_1, \omega_2] \subseteq \mathbb{C}$ be a lattice. An *elliptic function* for L is a function $f(z)$ on $\mathbb{C}$ such that

(1) f is meromorphic on $\mathbb{C}$, and
(2) (Doubly-periodicity) $f(z+\omega) = f(z)$ for any $\omega \in L$.

Example 2. The most basic example of elliptic function is Weierstrass $\wp$-function

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Theorem 3. *Some properties on Weierstrass $\wp$-function.*

(1) *$\wp(z)$ is an elliptic function whose singularities exactly consists of double poles of the points of L.*
(2) *It satisfies the equation*
$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),$$
where
$$g_2(L) = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4}, \quad g_3(L) = 140 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^6}.$$
(3) *If $z, w, z+w \notin L$, then*
$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right).$$

A Crush Proof. Since $\wp(z)$ is even and doubly-periodic, we have $\wp'(z)$ odd and doubly-periodic. For $r > 2$, define

$$G_r(L) = \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^r},$$

and then

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+1}(L) z^{2n}.$$

Then

$$\wp'(z)^2 - 4\wp(z)^3 - 60G_4(L)\wp(z) - 140G_6(L)$$

is holomorphic with constant term 0. □

Date: December 29, 2020.

Remark 4. By Theorem 3(2), $\mathbb{C}/L$ is not only topologically a complex torus but also carries an algebraic structure. Consider the map (set-theoretically)

$$W : \mathbb{C}/L \longrightarrow \mathbb{P}^2, \quad z \longmapsto (\wp(z) : \wp'(z) : 1).$$

Then W identifies $\mathbb{C}/L$ as a cubic curve E of $\mathbb{P}^2$, which is an elliptic curve as well. If f is meromorphic on $\mathbb{C}$, and for each $\omega \in L$, $f(z+\omega) = f(z)$, then f can be identified with a meromorphic function on E. Hence $f \in \mathbb{C}(E) := \mathbb{C}(\wp(z), \wp'(z))$.

Definition 5. The *discriminant* of L is

$$\Delta(L) := g_2(L)^3 - 27g_3(L)^2 \neq 0.$$

And the *j-invariant* of L is

$$j(L) := 1728 \cdot \frac{g_2(L)^3}{\Delta(L)}.$$

Recall that for $f(x) = x^3 + ax + b$, $\mathrm{disc}(f) = -4a^3 - 27b^2$. The number $\Delta(L)$ is closely related to the discriminant of the polynomial $4x^3 - g_2(L)x - g_3(L)$ that appears in the differential equation for $\wp(z)$. In fact, if e_1, e_2 and e_3 are the roots of this polynomial, then one can show that

$$\Delta(L) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2.$$

An important fact is that $\Delta(L)$ never vanishes.

Theorem 6. *The j-invariants classifies lattices up to scalars. That is, $j(L) = j(L')$ if and only if L, L' are homothetic, i.e. $L = \lambda L'$ for some $\lambda \in \mathbb{C}$.*

Proof. Note that

$$g_2(\lambda L) = \lambda^{-4} g_2(L), \quad g_3(\lambda L) = \lambda^{-6} g_3(L).$$

Hence $j(L) = j(\lambda L)$. Conversely, if $j(L) = j(L')$ then one can choose $\lambda \in \mathbb{C}$ such that

$$g_2(L') = \lambda^{-4} g_2(L) = g_2(\lambda L), \quad g_3(L') = \lambda^{-6} g_3(L) = g_3(\lambda L).$$

□

Fact. Assume $L = [1, \tau]$ for simplicity. Then $G_{2n+2}(L) \in \mathbb{C}[g_2(L), g_3(L)]$.

Indeed, $\mathbb{C}[g_2(L), g_3(L)]$ is independent of the choice of L, as

$$\mathbb{C}[g_2(L), g_3(L)] \simeq \bigoplus_{k \geqslant 2} M_K(\mathrm{SL}_2(\mathbb{Z}))$$

by any classical theory of modular forms. Granting this fact, $G_{2n+2}(L') = G_{2n+2}(\lambda L)$ for some $\lambda \in \mathbb{C}$. Then $\wp(z; L') = \wp(z; \lambda L)$. Then $L' = \lambda L$ is the locus of singularities.

For $\tau \in \mathfrak{H}$ lying in the upper half plane, define $j(\tau) := j([1, \tau])$. Then

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j\left(\left[1, \frac{a\tau + b}{c\tau + d}\right]\right) = j([c\tau + d, a\tau + b]) = j([1, \tau]) = j(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Fact. $j(\tau)$ is a modular function. We have

$$j(\tau) = \frac{1}{q} + 744 + q\mathbb{Z}[\![q]\!], \quad q = e^{2\pi i \tau}.$$

Theorem 7. *For $\alpha \in \mathbb{C}\backslash\mathbb{Z}$, the following are equivalent.*

(1) *$\wp(\alpha z)$ is a rational function of $\wp(z)$;*
(2) *$\alpha L \subseteq L$;*
(3) *for an imaginary quadratic K, there exists an order $\mathcal{O} \subseteq K$, such that $\alpha \in \mathcal{O}$ and L is homothetic to a proper fractional $\mathcal{O}$-ideal.*[1]

Proof. (2) $\Leftrightarrow$ (3) is easy. For $E = \mathbb{C}/L$, we can take

$$\mathcal{O} = \mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}.$$

For (1) $\Rightarrow$ (2), by assumption there are polynomials A, B such that

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))} \implies B(\wp(z))\wp(\alpha z) = A(\wp(z)).$$

By checking orders of poles at $z = 0$, we see $\deg B + 1 = \deg A$. Thanks to the double-periodicity, $\alpha\omega \in L$ for any $\omega \in L$, so $\alpha L \subseteq L$.

For (2) $\Rightarrow$ (1), suppose $\alpha L \subseteq L$. Along the multiplicating map $\mathbb{C}/L \xrightarrow{\times\alpha} \mathbb{C}/L$, we see $\wp(\alpha z)$ is an even meromorphic function on $\mathbb{C}/L$. Again, for $\omega \in L$, we compare orders of poles at $z = w$. Then $\wp(\alpha z)$ has a pole of order 2 at $z = w$. Hence $\wp(\alpha z)$ is a rational function in $\wp(z)$. $\square$

Corollary 8. *Let $\mathcal{O}$ be an order of some imaginary quadratic field. Then there is a one-to-one set-theoretical correspondence:*

$$C(\mathcal{O}) \longleftrightarrow \left\{ \begin{array}{c} \textit{homothety classes of lattices with } \mathcal{O} \\ \textit{as full ring of complex multiplications} \end{array} \right\}.$$

Here the right set is the collection of lattices such that $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$.

The following is the main theorem of complex multiplication theory.

Theorem 9. *Let $\mathcal{O}$ be an order of an imaginary quadratic field K. Let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal, which can be regarded as a lattice. Then $j(\mathfrak{a}) \in \mathbb{C}$ is an algebraic integer, and $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$.*

$$\begin{array}{c} K(j(\mathfrak{a})) \\ {\scriptstyle C(\mathcal{O})}\Big(\Big| \\ K \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 10. (1) Suppose $K = \mathbb{Q}(i)$, $\mathcal{O} = \mathbb{Z}[i]$, $\mathfrak{a} = \mathcal{O} = [1, i]$. Note that $i\mathfrak{a} = \mathfrak{a}$. We have

$$j(\mathfrak{a}) = j(i\mathfrak{a}),$$

and

$$g_3(\mathfrak{a}) = g_3(i\mathfrak{a}) = i^{-6} g_3(\mathfrak{a}) = -g_3(\mathfrak{a}) \implies g_3(\mathfrak{a}) = 0.$$

So $j([1, i]) = j(\mathfrak{a}) = 1728$, which is an algebraic integer. Simultaneously, $C(\mathcal{O}) = C(-4)$ is trivial, and the ring class field is $\mathbb{Q}(i, 1728) = \mathbb{Q}(i) = K$.

[1]Caution: $\mathcal{O}$ itself is not a lattice unless $\mathcal{O} = \mathcal{O}_K$.

(2) Suppose $K=\mathbb{Q}(\omega)=\mathbb{Q}(\sqrt{-3})$, $\mathcal{O}=\mathbb{Z}[\omega]$, $\mathfrak{a}=\mathcal{O}=[1,\omega]$, where $\omega=e^{2\pi i/3}$. We have

$$g_2(\mathfrak{a})=g_2(\omega\mathfrak{a})=\omega^{-4}g_2(\mathfrak{a}) \implies g_2(\mathfrak{a})=0 \implies j(\omega)=0.$$

Again, $C(\mathcal{O})=C(-3)$ is trivial.

Example 11. Gauss had found that the value of transcendental number

$$e^{\pi\sqrt{163}}=262537412640768743.99999999999925007259719818\cdots$$

is very close to an integer. To explain this phenomenon via complex multiplication theory, we take $K=\mathbb{Q}(\sqrt{-163})$ so that $h(\mathcal{O}_K)=1$. (Recall that $n=163$ is the largest positive integer such that $h(-4n)=1$.) Consider

$$\mathfrak{a}=\mathcal{O}=\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].$$

By the fact above Theorem 7 we see

$$j(\mathfrak{a})=j\left(\frac{1+\sqrt{-163}}{2}\right)=\frac{1}{q}+744+q\mathbb{Z}[\![q]\!], \quad q=\exp\left(2\pi i\cdot\frac{1+\sqrt{-163}}{2}\right).$$

From this construction,

$$\frac{1}{q}=-e^{\pi\sqrt{163}}.$$

By Theorem 9, as the ring class field of $\mathcal{O}_K$ is $\mathbb{Q}$ itself,

$$j\left(\frac{1+\sqrt{-163}}{2}\right)=-e^{\pi\sqrt{163}}+744+f(-e^{\pi\sqrt{163}})\in\mathbb{Z}, \quad f\in q\mathbb{Z}[\![q]\!].$$

After some estimation argument, it turns out that $e^{\pi\sqrt{163}}$ is very close to an integer.

$\boxed{\text{This is the end of the semester.}}$

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