# 1 Overview

The topic of the course is complex multiplication, a beautiful theory developed in the 19–th century with many arithmetic applications. This theory tells us something about the values of certain modular functions at certain points.

**Definition 1.** A *modular function* is a holomorphic function $f\colon \mathfrak{H} \to \mathbb{C}$ satisfying that

$$f\Big(\frac{az+b}{cz+d}\Big) = f(z) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \text{ and } z \in \mathbb{C},$$

where

- $\mathfrak{H}$ is the Poincaré upper half-plane $\{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$, and
- $\Gamma$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

*Remark.* We will only use the following congruence subgroups:

$$\begin{aligned} \Gamma_0(N) &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \Big\}, \\ \Gamma_1(N) &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \Big\}, \\ \Gamma(N) &= \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \Big\}. \end{aligned}$$

Also, sometimes we consider modular functions having values in $\mathbb{P}^1(\mathbb{C})$ (i.e., with poles) or even in $E(\mathbb{C})$ for some elliptic curve $E$.

**Example 2.** The following are examples of modular functions:

(1) The $j$–invariant $j\colon\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \to \mathbb{C}$ is an analytic isomorphism and generates the ring of modular functions on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$.

(2) The $\lambda$–function $\lambda\colon \Gamma(2)\backslash\mathfrak{H} \to \mathbb{C} \setminus \{ 0, 1 \}$ is an analytic isomorphism related to $j$ by

$$j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

It also satisfies the equations

$$\lambda = 16\frac{\eta(z/2)^8\,\eta(2z)^{16}}{\eta(z)^{24}} \quad \text{and} \quad 1-\lambda = \frac{\eta(z/2)^{16}\,\eta(2z)^8}{\eta(z)^{24}},$$

where

$$\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n) \quad \text{if } q = e^{2\pi i z} \quad \text{(Dedekind eta function).}$$

(The $q$–expansion of $\eta(z)$ together with the previous formulae for $\lambda$ and $1-\lambda$ show that, indeed, $\lambda$ does not take the values 0 or 1.)

(3) The Siegel units: we have a modular function $U_N \colon \Gamma_0(N)\backslash\mathfrak{H} \to \mathbb{C}^\times$ given by

$$U_N = \frac{\Delta(Nz)}{\Delta(z)}, \quad \text{where } \Delta(z) = \eta(z)^{24}.$$

(4) Modular parametrizations: every elliptic curve $E/\mathbb{Q}$ of conductor $N$ admits a non-constant analytic map $\Phi_E \colon \Gamma_0(N)\backslash\mathfrak{H} \to E(\mathbb{C})$ (modularity theorem).

## 1.1 The main theorem

**Definition 3.** A *CM point* of $\mathfrak{H}$ is a point $\tau \in \mathfrak{H}$ which satisfies a quadratic equation over $\mathbb{Q}$, so that $\tau = a + b\sqrt{d}$ for some $a, b, d \in \mathbb{Q}$ with $d < 0$ and $b > 0$.

**Theorem 4.** *Let $\tau \in \mathfrak{H} \cap \mathbb{Q}(\sqrt{d})$ (for some $d < 0$) and let $f$ be a modular function. If the $q$–expansion of $f$ has coefficients in $\mathbb{Q}$, then $f(\tau)$ is algebraic and is defined over an abelian extension of $\mathbb{Q}(\sqrt{d})$.*

This theorem suggests that we might be able to generate almost all abelian extensions of a quadratic imaginary fields (i.e., explicit class fields) from the values of modular functions.

**Example 5.** The CM values of $j(z)$ are called *singular moduli*. Consider a quadratic imaginary field $K$ with $D = \operatorname{disc}(K)$, $D < 0$, and class number $h(K) = 1$. Then the CM point

$$\tau_D = \frac{D + \sqrt{D}}{2}$$

satisfies that $j(\tau_D) \in \mathbb{Z}$.

Table 1 shows all these singular moduli. One can observe several patterns: all the numbers in the second column are perfect cubes and have many small prime factors but not all (no 7 or 13); in contrast the numbers in the third column are *almost* perfect squares (except for a factor of $D$) and includes the prime 7 but no 5. This kind of patterns were explained by the work of Gross and Zagier.

Writing

$$(j(\tau_D), j(\tau_D) - 1728) = (x^3, Dy^2),$$

we obtain an integral solution to the equation

$$x^3 - Dy^2 = 1728.$$

| $D$ | $j(\tau_D)$ | $j(\tau_D) - 1728$ |
|---|---|---|
| $-3$ | $0$ | $-2^6 3^3$ |
| $-4$ | $2^6 3^3$ | $0$ |
| $-7$ | $-3^3 5^3$ | $-3^6 7$ |
| $-8$ | $2^6 5^3$ | $2^7 7^2$ |
| $-11$ | $-2^{15}$ | $-2^6 7^2 11$ |
| $-19$ | $-2^{15} 3^3$ | $-2^6 3^6 19$ |
| $-43$ | $-2^{18} 3^3 5^3$ | $-2^6 3^8 7^2 43$ |
| $-67$ | $-2^{15} 3^3 5^3 11^3$ | $-2^6 3^6 7^2 31^2 67$ |
| $-163$ | $-2^{18} 3^3 5^3 23^3 29^3$ | $-2^6 3^6 7^2 11^2 19^2 127^2 163$ |

Table 1: Singular moduli for quadratic imaginary fields with class number 1.

These kind of numbers seem to *contradict* the ABC conjecture. Of course this is not really the case because we only have a finite number of quadratic imaginary fields with class number 1.

**Example 6.** In the spirit of the last observation in the previous example, Granville and Stark proved that a strong version of the ABC conjecture implies that $h(D)$ grows asymptotically like

$$\frac{\sqrt{|D|}}{\log(|D|)}$$

as $D \to -\infty$. In particular, the Dirichlet $L$–function $L(\chi_D, s)$ has no Siegel zeros.

## 1.2 More applications

Let $D$ be a negative discriminant as before. We have the following associated data:

(1) a quadratic order $\mathcal{O}_D = \mathbb{Z}[(D + \sqrt{D})/2]$;

(2) the class group $\mathrm{Cl}(D) = \mathrm{Pic}(\mathcal{O}_D)$, and

(3) a ring class field $H_D$ such that, if $K = \mathbb{Q}(\sqrt{D})$,

$$\mathrm{Gal}(H_D/K) = \mathrm{Cl}(D)$$

by class field theory. Furthermore, if we write $D = D_0 c^2$, where $D_0$ is a fundamental discriminant (square-free) and $c$ is the conductor of the order, then $H_D$ is unramified outside $c$.

**Proposition 7.** *If $f$ is a modular function for some group $\Gamma$ with rational $q$–expansion, then $f(\tau_D)$ is defined over an abelian extension $L$ of $H_D$ satisfying that*

(1) *$L$ is unramified outside the level $N$ of $\Gamma$ and*
(2) $[L : H_D] \le [\mathrm{SL}_2(Z) : \Gamma]$.

**Proposition 8.** *In the situation of proposition 7, if $f(\mathfrak{H})$ is contained in $V(\mathbb{C})$ for an algebraic variety $V$ (such as $\mathbb{A}^1$, $\mathbb{A}^1 \setminus \{1\}$ or an elliptic curve $E$), then*

$$f(\tau_D) \in V(\mathscr{O}_L[N^{-1}]).$$

**Example 9.**

(1) $j(\tau_D) \in \mathscr{O}_L$.
(2) $\lambda(\tau_D)$ is a solution to

$$(x^2 - x + 1)^3 - 2^{-8} j(\tau_D) x^2 (x-1)^2 = 0$$

and so $\lambda(\tau_D) \in \mathscr{O}_L[1/2]^\times$. Exercise: $1 - \lambda(\tau_D) \in \mathscr{O}_L[1/2]^\times$. The pair $(\lambda(\tau_D), 1 - \lambda(\tau_D))$ is then a solution to the 2–unit equation in $L$.
(3) $U_N(\tau_D) \in \mathscr{O}_L[1/N]^\times$ (and often even $U_N(\tau_D) \in \mathscr{O}_L^\times$). These units are called *elliptic units*. There is an interesting analogy summarized in table 2.

| $\mathbb{Q}$ | $K$ (imaginary quadratic) |
|---|---|
| Circular units $1 - \zeta_N$ | Elliptic units $U_N(\tau_D)$ |
| Class number formula:<br>$L'(\chi, 1) \leftrightarrow \log(1 - \zeta_N)$<br>for an even Dirichlet character $\chi$ | Kronecker limit formula:<br>$L'(\psi, 1) \leftrightarrow \log(U_N(\tau_D))$<br>for a finite-order Hecke character $\psi$ |
| Work of Thaine, Rubin<br>(Iwasawa main conjecture) | Work of Coates–Wiles, Rubin<br>(Iwasawa main conjecture) |

Table 2: Analogy between the theory over $\mathbb{Q}$ and over $K$.

**Theorem 10 (Coates–Wiles, Rubin).** *Let $A/\mathbb{Q}$ be an elliptic curve with CM. If the Hasse–Weil L–function of $A$ satisfies that $L(A,1) \neq 0$, then $A(\mathbb{Q}) < \infty$ (Coates–Wiles) and $\text{Ш}(A/\mathbb{Q}) < \infty$ (Rubin).*

Remarkably, CM theory has applications towards the proof of the BSD conjecture for general elliptic curves (not just those with CM). Consider an elliptic curve $E/\mathbb{Q}$ and a modular parametrization $\Phi_E \colon \Gamma_0(N)/\mathfrak{H} \to E(\mathbb{C})$. Choosing an appropriate $D$, we get $\Phi_E(\tau_D) \in E(H_D)$. Define

$$P_D = \sum_{\mathrm{disc}(\tau) = D} \Phi_E(\tau) \in E(K).$$

**Theorem 11 (Gross–Zagier).** *In the situation above and if $D$ is perfect square modulo $N$, then*

$$L'(E,1) \sim \mathrm{ht}_{\mathrm{NT}}(P_D).$$

*In particular, $P_D$ has infinite order precisely when $L'(E,1) \neq 0$.*

**Theorem 12 (Kolyvagin).** *If $P_D$ has infinite order, then $E(K)$ is generated by $P_D$ and $Ш(E/K) < \infty$.*

**Corollary 13.** *If $\mathrm{ord}_{s=1}(L(E,s)) \leq 1$, then*

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1}(L(E,s)) \quad \textit{and} \quad Ш(E/\mathbb{Q}) < \infty.$$

These are essentially the best known results towards a proof of the BSD conjecture, and they would not be available without the theory of complex multiplication.