Modular Curves and the CM points on Modular Curves

In our last three lectures, we introduced the notion of a CM elliptic curve, an explicit description of a CM elliptic curve defined over the complex numbers (lattice $\mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$, where τ is an imaginary quadratic number), and some properties of CM elliptic curves (they are defined over number fields and they have everywhere potentially good reduction).

In this lecture, I want to introduce some central problems in modern arithmetic geometry where CM elliptic curves played a critical role in the study of.

1 Rational Points on Algebraic Curves

One origin of number theory and arithmetic geometry is the study of Diophantine problems, namely the study of integral solutions to polynomial equations. Integral roots of polynomials correspond to rational points on an algebraic variety, and the starting point of this problem is to study the set of K-points on an algebraic curve defined over some non-algebraically closed field K.

The most famous example of this problem is Fermat's last theorem, in which it states that the only integral solutions to $x^n + y^n = z^n$ are the ones satisfying $xyz = 0$ for any $n > 2$. The proof of this theorem relies on the study of elliptic curves and modular curves which we will define today. To talk about rational points on algebraic curve, we start with the set of rational points on an elliptic curve defined over $\mathbb{Q}$.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$ and we want to study the set of points $(x, y) \in E(\mathbb{Q})$. From the group law on E, we know that $E(\mathbb{Q})$ is an abelian group.

Theorem 1.1 (Mordell–Weil theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

By the fundamental theorem of finitely generated abelian groups, the group $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E_{tors}(\mathbb{Q})$ where r is a non-negative integer called the rank of E and $E_{tors}(\mathbb{Q})$ is a finite abelian group called the torsion subgroup of E. We have a relatively good understanding on the group $E_{tors}(\mathbb{Q})$ thanks to the following theorem of Mazur.

Theorem 1.2 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:*

$$\mathbb{Z}/N\mathbb{Z} \quad \textit{with } 1 \leq N \leq 10 \textit{ or } N = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \textit{with } 1 \leq N \leq 4.$$

Further, each of these groups occurs as $E_{tors}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

But the rank of an elliptic curve is much more mysterious. We don't know whether the rank for the set of elliptic curves defined over $\mathbb{Q}$ is bounded and we don't have an algorithm which guarantees to compute the rank of an arbitrary elliptic curve $E/\mathbb{Q}$.

The most important conjecture regarding the rank of an elliptic curve is the Birch and Swinnerton-Dyer conjecture which predicts that the rank of $E(\mathbb{Q})$ is determined by the L-function of E which contains the information of the number of points on the reductions of E at all primes. This conjecture is wide open, especially for E without complex multiplication.

One topic we will discuss today is a method to construct rational points (called *Heegner points*) on an elliptic curve using the theory of complex multiplication. These points were used in the work of Gross–Zagier and Kolyvagin which proved some cases of the BSD conjecture.

2 Congruence Subgroups and Modular Curves

Let N be a positive integer. Consider the reduction homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

This map is in fact surjective with kernel the subgroup of $\mathrm{SL}_2(\mathbb{Z})$, referred to as the *principal congruence subgroup of level N*,

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Definition 2.1. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is called a congruence subgroup of level N.

Besides the principal congruence subgroups, the most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Note that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$.

Definition 2.2. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. The modular curve $Y(\Gamma)$ is the quotient $\Gamma \setminus \mathbb{H}$ and the modular curve $X(\Gamma)$ is its compactification $X(\Gamma) = \Gamma \setminus \mathbb{H}^*$. The orbits of the points $\mathbb{Q} \cup \{\infty\}$ under the Γ-action are called the cusps of $X(\Gamma)$.

The modular curves $X(\Gamma)$ are compact Riemann surfaces. Moreover, for Γ being $\Gamma(N)$, $\Gamma_1(N)$, or $\Gamma_0(N)$ the curves $Y(\Gamma(N))$ (denoted as $Y(N)$), $Y_1(\Gamma(N))$ (denoted as $Y_1(N)$), and $Y(\Gamma_0(N))$ (denoted as $Y_0(N)$) have modular interpretations. Here, we discuss the case of $Y_0(N)$ as an example.

Consider pair (E, C) where E is an elliptic curve defined over $\mathbb{C}$ and C is a cyclic subgroup of E of order N. The set of $\mathbb{C}$-points on $Y_0(N)$ are in bijection with pairs (E, C) up to equivalence condition $(E_1, C_1) \sim (E_2, C_2)$ where there exists an isomorphism $\phi : E_1 \to E_2$ such that $\phi(C_1) = C_2$. Equivalently, a $\mathbb{C}$-point on $Y_0(N)$ corresponds to a pair of elliptic curves (E, E') together with a degree N isogeny $E \to E'$. To each $\tau \in \mathbb{H}$, this pair of elliptic curves is $(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \mathbb{C}/(\mathbb{Z} + \mathbb{Z}N\tau))$ and the isogeny is $z \mapsto Nz$.

The modular curve $X(1)$ has a model over $\mathbb{Q}$, i.e. $\mathbb{P}^1_{\mathbb{Q}}$ and its function field is $\mathbb{Q}(j)$. The curve $X_0(N)$ also has a model over $\mathbb{Q}$, meaning there exists an irreducible polynomial $f(x) \in \mathbb{Q}(j)[x]$ such that the curve $X/\mathbb{Q}$ whose function field is isomorphic to $\mathbb{Q}(j)[x]/f(x)$ satisfies $X \otimes \mathrm{Spec}\ \mathbb{C} \simeq X_0(N)$. In fact this polynomial $f(x)$ is exactly the polynomial $\Phi_N(x, \tau) \in \mathbb{Q}(j(\tau))[x]$ from Lecture 3.

Theorem 2.3 (Modularity Theorem, Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor)**.** *Let E be an elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N there exists a surjective morphism over $\mathbb{Q}$ from the modular curve $X_0(N)/\mathbb{Q}$ to the elliptic curve E,*

$$X_0(N) \to E.$$

The modularity theorem was conjectured by Shimura–Taniyama–Weil and it was the key ingredient in the proof of Fermat's Last Theorem.

3 Rational Points on Modular Curves and CM Elliptic Curves

Let E be an elliptic curve defined over a field K. For any positive integer m which is coprime to the characteristic of K, let $E[m]$ denote the m-torsion subgroup of E,

$$E[m] = \{P \in E(\overline{K}) : mP = O\}, \quad \text{and recall} \quad E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2.$$

Then $E[m]$ is a scheme defined over K and the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$ by acting on the $\overline{K}$-points of E. This action gives a Galois representation

$$\phi_m : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

If an elliptic curve E/K has an order N cyclic subgroup $C \subset E[N]$ fixed by the $\mathrm{Gal}(\overline{K}/K)$ action, then the pair (E, C) gives rise to a K-point on $X_0(N)$. If further the action of $\mathrm{Gal}(\overline{K}/K)$ restricts on C is the trivial action, then it gives rise to a K-point on $X_1(N)$. A $\mathbb{C}$-point on $Y_1(N)$ corresponds to a pair (E, P) where $E/\mathbb{C}$ is an elliptic curve and P is point of order N on E. A major part of Mazur's theorem on the structure of the torsion subgroup $E_{tors}(\mathbb{Q})$ is to prove the non-existence of $\mathbb{Q}$-points on $X_1(N)$ which are not cusps for $N \geq 13$.

We can use CM elliptic curves to construct points on modular curves whose defining field is of low degree over $\mathbb{Q}$.

Let $\alpha : E \to E$ be an endomorphism of E defined over K. Then the map $\alpha : E[m] \to E[m]$ commutes with the $\mathrm{Gal}(\overline{K}/K)$ action. This forces the image of ϕ_m to be an **abelian subgroup** of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ when E is a CM elliptic curve with all of its endomorphisms defined over K. This image is much smaller than the typical behavior of a non-CM elliptic curve defined over a number field.

Theorem 3.1 (Serre)**.** *Let K be a number field and let E/K be an elliptic curve without complex multiplication.*

1. $\phi_{\ell^\infty}(\mathrm{Gal}(\overline{K}/K))$ *is of finite index in* $\mathrm{Aut}(E[\ell^\infty])$ *for all primes ℓ;*
2. $\phi_{\ell^\infty}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{Aut}(E[\ell^\infty])$ *for all but finitely many primes ℓ.*

Thus, the m-torsion points of a CM elliptic curve E/K is defined over a number field L with relatively low degree over K. Using this fact, we deduce that CM elliptic curves give rise to points on modular curves whose defining field is of relatively low degree. Moreover, we can use CM elliptic curves to construct explicit points on modular curves for which we can analyze their defining fields.

4 Heegner Points

The set of Heegner points on $Y_0(N)(\mathbb{C})$ are points corresponding to a pair of elliptic curves (E, E') such that $\mathrm{End}(E) \simeq \mathrm{End}(E') \simeq \mathcal{O}$ where O is an order in an imaginary quadratic field.

Given an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ where d is the discriminant of the field $K = \mathbb{Q}(\sqrt{d})$. Let c be the index of $\mathcal{O}$ in $\mathcal{O}_K$ and then $D = dc^2$ is the discriminant of $\mathcal{O}$. The order $\mathcal{O}$ is determined by its discriminant. Given a positive integer N, if the equation $D = B^2 - 4NC$ has integer solutions $B, C \in \mathbb{Z}$ satisfying $\gcd(N, B, C) = 1$, then there exists proper fractional $\mathcal{O}$-ideals α, β such that under an embedding $K \hookrightarrow \mathbb{C}$, the images of α, β are lattices with a cyclic degree N isogeny between their corresponding elliptic curves.

For fixed $\mathcal{O}$ and N, the set of Heegner points is fixed under the action of $\mathrm{Aut}(\mathbb{C})$. They are algebraic points defined over $K(j(\tau))$ where $j(\tau)$ is the j-invariant of an elliptic curve with CM by $\mathcal{O}$.

Recall from the modularity theorem, given an elliptic curve $E/\mathbb{Q}$, there exists $X_0(N)$ which admits a surjective map $\pi : X_0(N) \to E$ over $\mathbb{Q}$. Thus, for an order $\mathcal{O}$ such that we can construct Heegner points $P_1, \cdots, P_{h(\mathcal{O})}$ on $X_0(N)$, we can consider the point $P = \pi(P_1) + \cdots + \pi(P_{h(\mathcal{O})})$ on E which is defined over K. The work of Gross–Zagier related the height of P with the L-function of E, giving a way to construct a rational point of infinite order for elliptic curves whose L-function satisfies certain conditions.