Lecture 2

Saturday, August 6, 2022 6:12 PM

山 Sha

山 Shan

§1 Heegner points on $X_0(N)$.

Recall we have open and compact modular curves

$$\begin{array}{ccc} \Gamma_0(N)\backslash\mathcal{H} & =: & Y_0(N)(\mathbb{C}) \\ \cap\!| & & \cap\!| \\ \Gamma_0(N)\backslash\mathcal{H}^* & =: & X_0(N)(\mathbb{C}). \end{array}$$

To each $\tau \in \mathcal{H}$ we have an elliptic curve

$$E_\tau \cong \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$$

and $E_\tau \simeq E_{\tau'} \iff \tau, \tau'$ are in the same $SL_2(\mathbb{Z})$-orbit.

i.e. $SL_2(\mathbb{Z})\backslash\mathcal{H} = Y_0(1)(\mathbb{C}) = \{$ elliptic curves $/\mathbb{C}\}$.

Adding a $\Gamma_0(N)$-level structure we obtain

$$E_\tau \simeq \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau \quad , \quad C_\tau = \frac{\frac{1}{n}\mathbb{Z}+\mathbb{Z}\tau}{\mathbb{Z}+\mathbb{Z}\tau} \simeq \mathbb{Z}/N$$

and $(E_\tau, C_\tau) \cong (E_{\tau'}, C_{\tau'}) \iff \tau, \tau'$ in the same $\Gamma_0(N)$-orbit.

Therefore:

$Y_0(N)(\mathbb{C}) = \{$ elliptic curves $E/\mathbb{C}$ together with

$$Y_0(N)(\mathbb{C}) = \left\{ \begin{array}{l} \text{elliptic curves } E/\mathbb{C} \text{ together with} \\ \text{a cyclic subgp } C \subseteq E \text{ of order } N \end{array} \right\}.$$

$$= \left\{ \underset{\text{cyclic } N\text{-isogeny}}{E \to E'} \right\}.$$

Notice the last moduli interpretation makes sense over $\mathbb{Q}$ and gives a model $Y_0(N)_{/\mathbb{Q}}$. Similarly for $X_0(N)_{/\mathbb{Q}}$

Rem

In general $X_0(N)$ has very few $\mathbb{Q}$-pts. (By Mazur or Faltings when $N \gg 0$)

One may try to construct alg pts of $X_0(N)$ over number fields of small degree. Although we have

$$\mathcal{H}^* \longrightarrow X_0(N) = \Gamma_0(N) \backslash \mathcal{H}^*$$

and there are many alg pts in $\mathcal{H}$. this uniformization map is highly transcendental and doesn't send alg pts to alg pts.

Miracle This may still work when $K =$ im quad !
(to see this we use moduli interpretation)

Recall that the endomorphism ring of $E/\mathbb{C}$ has two cases:

① $\mathrm{End}(E) \simeq \mathbb{Z}$.

② $\mathrm{End}(E) \simeq \mathcal{O} \overset{\text{finite index}}{\subseteq} \mathcal{O}_K \quad K =$ im quadratic field.

Def. In case ② we say E has CM (complex multiplication)

Ex. $E: y^2 = x^3 + n x$ has CM by $K = \mathbb{Q}(i)$

Ex. $E: y^2 = x^3 + nx$ has CM by $K = \mathbb{Q}(i)$
given by $[i](x, y) = (-x, iy)$.

Ex $E: y^2 = x^3 + n$ has CM by $K = \mathbb{Q}(\sqrt{-3})$
$= \mathbb{Q}(\zeta_3)$
given by $[\zeta_3](x, y) = (\zeta_3 x, y)$.

Main Theorem of CM:

$$\left\{ \begin{array}{c} \text{elliptic curves } E/\mathbb{C} \text{ with} \\ \text{CM by } \mathcal{O}_K \end{array} \right\} \xrightarrow{\sim} \left\{ \mathbb{C}/\mathfrak{a} : \mathfrak{a} \in Cl(K) \right\}$$

Each such E is defined over the Hilbert class field
H_K/K, and $Gal(H_K/K) \simeq Cl(K)$ acts by
$\sigma \mapsto \mathfrak{b}_\sigma$

$$j(\mathbb{C}/\mathfrak{a})^\sigma = j(\mathbb{C}/\mathfrak{a}\,\mathfrak{b}_\sigma^{-1})$$

Now we can single out "special pts" on $X_0(N)$ corresponding to CM elliptic curves.

Def. A Heegner pt is a pt
$$x_K = (E \to E') \in X_0(N)(\mathbb{C}).$$
s.t.
$$End(E) = End(E') = \mathcal{O}_K.$$

By theory of CM, we know $x_K \in X_0(N)(H_K)$.

Notice a Heegner pt $x_K \in X_0(N)$ exists

$\Leftrightarrow$ $\exists\, \mathfrak{a}, \mathfrak{b} \in Cl(K)$ s.t.

$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}$ is cyclic of order N

$\Leftrightarrow$. $\mathfrak{b}/\mathfrak{a} \simeq \mathbb{Z}/N$ or $\mathcal{O}_K/\ldots \simeq \mathbb{Z}/N$

$\Leftrightarrow$. $\mathfrak{b}/\mathfrak{a} \simeq \mathbb{Z}/N$. or $\mathcal{O}_K/\mathfrak{a}\mathfrak{b}^{-1} \simeq \mathbb{Z}/N$.

$\Leftrightarrow$ $\exists$ an ideal $\mathcal{N} \leq \mathcal{O}_K$ s.t $\mathcal{O}/\mathcal{N} = \mathbb{Z}/N$.

($\Leftrightarrow$ $\exists$ binary quad form $ax^2+bxy+cy^2$ with disc $= d_K$ $(a,b,c)=1$.

s.t $N = ax^2+bxy+cy^2$ has $\mathbb{Z}$-solutions $(x,y)=1$.

$\Leftrightarrow$ $Nx^2+bxy+cy^2$ has disc d_K.).

i.e $d_K = b^2 - 4Nc$ has solution

Def Say K satisfies Heegner hypothesis for N if every prime $|N$ splits in K.

In this case x_K exists on $X_0(N)$ by choosing a prime $\mathfrak{p}$ above $p|N$ and take $\mathcal{N} = \prod \mathfrak{p}^{\mathrm{ord}_p(N)}$.

Rem. More generally, one can allow $p \| N$ to be ramified in K.

§2 Heegner pts on elliptic curves.

Def. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.

Fix a modular parametrization.

$$X_0(N) \xrightarrow{\varphi} E$$

Sending the cusp $\infty \in X_0(N)$ to $0 \in E$.

We define the Heegner pt on E

$$y_K := \sum \sigma(\varphi(x_K)) \in E(K).$$

$$y_K := \sum_{\sigma \in Gal(H_K/K)} \sigma(\varphi(x_K)) \in E(K).$$

Using the moduli interpretation, one can check that

Prop. $\overline{y_K} = -\underset{\substack{\uparrow \\ \text{sign of func eq.}}}{\varepsilon(E)} \cdot y_K$ in $\dfrac{E(K)}{E(K)_{tor}}$.

So $y_K \in E(\mathbb{Q}) + E(K)_{tor} \iff \varepsilon(E) = -1$.

(in particular $y_K + \overline{y_K} \in E(\mathbb{Q}) \underset{\text{up to torsion}}{\sim} 2y_K$ when $\varepsilon(E) = -1$)

<u>Ex</u> $E = X_0(32) : y^2 = x^3 + 4x$

$K = \mathbb{Q}(\sqrt{-7})$ satisfies Heegner hypothesis for $N = 32$

(2 splits in $\mathbb{Q}(\sqrt{-7})$ as $-7 \equiv 1 \pmod 8$)).

$H_K = K = \mathbb{Q}(\sqrt{-7})$ as $Cl(K) = 1$.

using uniformization $\mathcal{H}^* \longrightarrow E = \Gamma_0(32) \backslash \mathcal{H}^*$

one finds $x_K = y_K = \left(\dfrac{\sqrt{-7} - 1}{2}, \dfrac{\sqrt{-7} + 3}{2} \right) \in E(K)$

In fact y_K has infinite order and $E(K)$ has rk $= 1$

(this agrees with $\varepsilon(E) = +1$, $y_K \notin E(\mathbb{Q}) + E(K)_{tor}$).

Using this construction Heegner was able to prove

Thm (Heegner) $E : y^2 = x^3 - n^2 x$ has $r_{alg} \geq 1$

when $n = \text{prime} \equiv 7 \pmod 8$).

Ex $E : y^2 + y = x^3 - x$ $N = 37$

Ex. $E: y^2 + y = x^3 - x$. $N = 37$.

$k = \mathbb{Q}(\sqrt{-7})$ satisfies Heegner hypothesis for $N = 37$.

$y_K = (0,0) \in E(k)$ has infinite order.

(this agrees with $\varepsilon(E) = -1$. $y_K \in E(\mathbb{Q})$).

§3. Gross-Zagier formula (for $X_0(N)$).

Let E_K be the base change of E to $k/\mathbb{Q}$.
Then $L(E_K, s)$ also satisfies a functional equation.

$$\Lambda(E_K, s) = \varepsilon(E_K) \cdot \Lambda(E_K, 2-s)$$

where $\Lambda(E_K, s) = (2\pi^{-s}\Gamma(s))^{[k:\mathbb{Q}]} N_m(N(E_K))^{\frac{s}{2}} |d_K|^s$

Although $\varepsilon(E)$ can be either $+1$ or -1, the root number over a quad field $k/\mathbb{Q}$ has a simpler formula.

Prop Assume $(N, d_K) = 1$. Then

$\varepsilon(E_K) = \chi_K(-N)$. where $\chi_K : (\mathbb{Z}/|d_K|)^\times \to \{\pm 1\}$.

is the quad character associated to $k/\mathbb{Q}$. $\left(\chi_K = \left(\frac{d_K}{\cdot}\right)\right)$

Cor If k is imaginary quad ($\chi_K(-1) = -1$), then

$$\varepsilon(E_K) = -\prod_{p \text{ inert in } k} (-1)^{\mathrm{ord}_p N}.$$

Then Heegner hypothesis $\Rightarrow \varepsilon(\ ) = -1 \Rightarrow r_{an}(E_K)$ odd

$\Rightarrow y_K \in E(K)$. ?

Naturally, one expects to relate y_K to $L(E_K, s)$.

Thm (Gross-Zagier)

$$L'(E_K, 1) = \frac{\int_{E(\mathbb{C})} \omega \wedge i\bar{\omega}}{|d_K|^{\frac{1}{2}} \left| \frac{\mathcal{O}_K^\times}{\{\pm 1\}} \right|^2} \cdot \langle y_K, y_K \rangle_{NT}$$

Here $\omega \in H^0(E_{/\mathbb{Q}}, \Omega^1)$ s.t. $\varphi^* \omega = f_E(q) \frac{dq}{q}$ $\left(= 2\pi i \, f_E(z) \, dz\right)$
(normalized newform)

Rem $\left(\int_{E(\mathbb{C})} \omega \wedge i\bar{\omega} \right) \cdot \deg \varphi$.

$$= \int_{X_0(N)(\mathbb{C})} 8\pi^2 f(z) \overline{f(z)} \, dx\, dy$$

$$= (f, f) \quad \text{Peterson inner product}$$

So: $$L'(E_K, 1) = \frac{(f, f)}{|d_K|^{\frac{1}{2}} \left| \frac{\mathcal{O}_K^\times}{\{\pm 1\}} \right|^2} \frac{\langle y_K, y_K \rangle_{NT}}{\deg \varphi}.$$

Rem. The definition of y_K depends on the choice of x_K $(\mathcal{N} \subseteq \mathcal{O}_K)$ and $\varphi : X_0(N) \to E$.

but y_K is well-defined up to ± 1 and torsion,
(after fixing φ)

$\dfrac{\langle y_K, y_K \rangle}{\deg \varphi}$ doesn't depend on any choices and is canonical.

Cor. $L'(E_K, 1) \neq 0 \iff \langle y_K, y_K \rangle_{NT} \neq 0$

$\iff y_K$ is infinite order.

$$r_{an}(E_K) = 1 \Rightarrow r_{alg}(E_K) \geq 1.$$

Rem. By comparing GZ formula and BSD formula for E_K we find BSD formula for E_K is equivalent to

$$|\text{Ш}(E_K)|^{\frac{1}{2}} = \frac{[E(K) : \mathbb{Z} y_K]}{\prod_p c_p(E) \cdot |u_K^{\vee}/_{\pm 1}| \cdot c}$$

where $\varphi^{\vee} \Omega_E = c \cdot 2\pi i f(z)\, dz$. ($c$ is the Manin constant)

In particular, one has a precise prediction of $|\text{Ш}(E_K)|$ in terms of Heegner points! e.g.:

$$p \nmid y_K \in E(K) \underset{(\text{true for } p \gg 0)}{\overset{?}{\Longleftrightarrow}} \text{Ш}(E_K)[p^{\infty}] = 0$$

§4. Back to $E/\mathbb{Q}$.

Now we would like to relate E_K back to E.

Def. Let $E^{(K)}/_{\mathbb{Q}}$ be the quadratic twis of $E/_{\mathbb{Q}}$ by K.

i.e. if $E: y^2 = x^3 + Ax + B$

Then $E^{(K)}: d_K y^2 = x^3 + Ax + B$.

Intrinsically, $E^{(K)}$ is the unique elliptic curve $/_{\mathbb{Q}}$ that it becomes isomorphic to E over K, but not over $\mathbb{Q}$.

The $G_{\mathbb{Q}}$-rep $V_p(E^{(K)}) \simeq V_p(E) \otimes \chi_{K/\mathbb{Q}}$.

where $\chi_{K/\mathbb{Q}} : G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q}) \simeq \{\pm 1\}$.

Exercise $L(E_K, s) = L(E, s) \cdot L(E^{(K)}, s)$.

Cor $r_{an}(E_K) = r_{an}(E) + r_{an}(E^{(K)})$.

we also have (compatible with BSD)

Prop $r_{alg}(E_K) = r_{alg}(E) + r_{alg}(E^{(K)})$.

Pf Since $E(K) \otimes \mathbb{Q}$

$$= (E(K) \otimes \mathbb{Q})^{c=+1} \oplus (E(K) \otimes \mathbb{Q})^{c=-1}$$

$$\simeq E(\mathbb{Q}) \otimes \mathbb{Q} \oplus E^{(K)}(\mathbb{Q}) \otimes \mathbb{Q} \qquad \square.$$

Thm If $r_{an}(E) = 1$, then $r_{alg}(E) \geq 1$

and $\dfrac{L'(E,1)}{\Omega(E) R(E)} \in \mathbb{Q}$.

Pf. By a theorem of Waldspurger (next time), we may choose K such that $r_{an}(E^{(K)}) = 0$.

So $r_{an}(E_K) = r_{an}(E) + r_{an}(E^{(K)}) = 1 + 0 = 1$

$\overset{GZ}{\Rightarrow}$ $y_K \in E(K)$ has infinite order

$\overset{\varepsilon(E)=-1}{\longrightarrow}$ $y_K + \bar{y}_K \in E(\mathbb{Q})$ also has infinite order

$\Rightarrow$ $r_{alg}(E) \geq 1$.

The second claim then follows by

The second claim then follows by

$$L'(E_K, 1) = L'(E, 1)\, L(E^{(K)}, 1)$$

and $\dfrac{\int \omega \wedge \bar{\omega}}{|d_K|^{\frac{1}{2}}} \sim_{\mathbb{Q}^\times} \Omega(E)\,\Omega(E^{(K)})$, $\dfrac{L(E^{(K)},1)}{\Omega(E^{(K)})} \in \mathbb{Q}^\times$ $\square$.

Exercise Numerically verify GZ formula for

$$E : y^2 + y = x^3 - x. \qquad K = \mathbb{Q}(\sqrt{-7})$$

§5. Application to Gauss class number problem

Cor If $\varepsilon(E) = -1$, and $y_K + \bar{y}_K \in E(\mathbb{Q})$ is torsion.

Then $r_{an}(E) \geq 3$.

Ex (Gauss elliptic curve)

$$E = 5077a : y^2 + y = x^3 - 7x + 6.$$

Buhler-Gross-Zagier computed its Heegner pt is trivial, thus provides the first example with $r_{an}(E) \geq 3$.

In fact, they prove $r_{an}(E) = r_{alg}(E) = 3$ in this case!

Rem. It is still open to find E with provably correct $r_{an}(E) \geq 4$.

Thm (Goldfeld 1976) If there exists $E/\mathbb{Q}$ with $r_{an}(E) \geq 3$

then

$$h(D) > \underset{\text{effective}}{C_{\varepsilon, E}} \left(\log |D|\right)^{1-\varepsilon} \quad \forall \varepsilon > 0.$$

where D runs over fund disc of im quad fields.

So GZ + Goldfeld solve Gauss (1801) class number problem:

there is an effective way to compute all im quad fields with fixed class number!

Rem. Historically Heegner (1952) first used CM theory to solve Gauss class number 1 problem (Baker-Stark-Heegner Theorem)