TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 5, May 2018, Pages 3721–3743
http://dx.doi.org/10.1090/tran/7053
Article electronically published on December 14, 2017

HEEGNER POINTS ON MODULAR CURVES

LI CAI, YIHUA CHEN, AND YU LIU

Abstract. In this paper, we study the Heegner points on more general modular curves other than $X_0(N)$, which generalizes Gross' work "Heegner points on $X_0(N)$". The explicit Gross-Zagier formula and the Euler system property are stated in this case. Using such a kind of Heegner points, we construct certain families of quadratic twists of $X_0(36)$, with the ranks of Mordell-Weil groups being zero and one respectively, and show that the 2-part of their BSD conjectures hold.

Contents

1. Introduction

Let $\phi = \sum_{n=1}^{\infty} a_n q^n$ be a newform of weight 2, level $\Gamma_0(N)$, normalized such that $a_1 = 1$. Let K be an imaginary quadratic field of discriminant D and χ a (primitive) ring class character over K of conductor c, i.e., a character of $\mathrm{Pic}(\mathcal{O}_c)$ where $\mathcal{O}_c$ is the order $\mathbb{Z} + c\mathcal{O}_K$ of K. Let $L(s, \phi, \chi)$ be the Rankin-Selberg convolution of ϕ and χ. Assume the Heegner condition:

(1) $(c, N) = 1$.
(2) Any prime $p|N$ is either split in K or ramified in K with $\mathrm{ord}_p(N) = 1$ and $\chi([\mathfrak{p}]) \neq a_p$, where $\mathfrak{p}$ is the unique prime ideal of $\mathcal{O}_K$ above p and $[\mathfrak{p}]$ is its class in $\mathrm{Pic}(\mathcal{O}_c)$.

Under this condition, the sign of $L(s, \phi, \chi)$ is -1 and Gross studies the Heegner points on $X_0(N)$ in [7]. It's well known that $X_0(N)(\mathbb{C})$ parameterizes the pairs (E, C), with E an elliptic curve over $\mathbb{C}$ and C a cyclic subgroup of E of order N. By the Heegner condition, there exists a proper ideal $\mathcal{N}$ of $\mathcal{O}_c$ such that $\mathcal{O}_c/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. For any proper ideal $\mathfrak{a}$ of $\mathcal{O}_c$, let $P_{\mathfrak{a}} \in X_0(N)$ be the point representing $(\mathbb{C}/\mathfrak{a}, \mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a})$, which is defined over the ring class field H_c, the abelian extension of K with Galois group $\mathrm{Pic}(\mathcal{O}_c)$ given by class field theory. Such points are called Heegner points over K of conductor c and only depend on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_c)$.

Received by the editors May 31, 2016, and, in revised form, August 18, 2016 and August 21, 2016.

2010 *Mathematics Subject Classification.* Primary 11G05, 11G07.

The first author was supported by the Special Financial Grant from the China Postdoctoral Science Foundation 2014T70067.

Let $J_0(N)$ be the Jacobian of $X_0(N)$. The cusp $[\infty]$ on $X_0(N)$ defines a morphism over $\mathbb{Q}$ from $X_0(N)$ to $J_0(N)$ given by $P \mapsto [P-\infty]$. Let P_χ be the point

$$P_\chi = \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O}_c)} [P_{\mathfrak{a}} - \infty] \otimes \chi([\mathfrak{a}]) \in J_0(N)(H_c) \otimes_{\mathbb{Z}} \mathbb{C}$$

and let P_χ^ϕ be the ϕ-isotypical component of P_χ. Under the Heegner condition, Cai-Shu-Tian [3] give an explicit form of Gross-Zagier formula which relates the height of P_χ^ϕ to $L'(1,\phi,\chi)$. In fact, they give an explicit form of Gross-Zagier formula in the general Shimura curve case.

Let the data (ϕ, K, χ) be as above, and generalize the Heegner condition to the following one $(*)$:

(i) $(c, N) = 1$,
(ii) if a prime $p|N$ is inert in K, then $\mathrm{ord}_p N$ is even; if $p|N$ is ramified in K, then $\mathrm{ord}_p N = 1$ and $\chi([\mathfrak{p}]) \neq a_p$, where $\mathfrak{p}$ is the unique prime ideal of $\mathcal{O}_K$ above p and $[\mathfrak{p}]$ is its class in $\mathrm{Pic}(\mathcal{O}_c)$.

Under these assumptions, we can write $N = N_0 N_1^2$, with $p|N_1$ if and only if p is inert. Given an embedding $K \hookrightarrow M_2(\mathbb{Q})$ such that $K \cap M_2(\mathbb{Z}) = K \cap R_0(N_0) = \mathcal{O}_c$, where

$$R_0(N_0) = \left\{ A \in M_2(\mathbb{Z}) \middle| A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N_0} \right\}.$$

We will consider the order R of $M_2(\mathbb{Z})$ given by $R = \mathcal{O}_c + N_1 R_0(N_0)$. Define

$$\Gamma_K(N) = R^\times \cap \mathrm{SL}_2(\mathbb{Z}) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{array}{l} A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N_0} \\ A \bmod N_1 \in R/N_1 R \end{array} \right\}.$$

Now we have to consider the modular curve $X_K(N) = \Gamma_K(N) \backslash \mathscr{H} \cup \{\text{cusps}\}$, where $\mathscr{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

This modular curve is not the usual modular curve of the form $X_0(M)$ any longer, if $N_1 \neq 1$. $X_K(N)$ parameterizes (E, C, α) where E is an elliptic curve over $\mathbb{C}$, C is a cyclic subgroup of E of order N_0 and α is an H-orbit of an isomorphism $(\mathbb{Z}/N_1\mathbb{Z})^2 \simeq E[N_1]$, where

$$H = (\mathcal{O}_K/N_1\mathcal{O}_K)^\times \subset \mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z}).$$

The readers are referred to [9] theorem 7.1.3. Let h_0 be the fixed point of $\mathscr{H}$ under the action of $K^\times$. Note that since $\mathbb{Z} + \mathbb{Z}h_0^{-1}$ is an invertible ideal of $\mathcal{O}_c$, then the triple $P = \left(\mathbb{C}/\mathbb{Z} + \mathbb{Z}h_0, \langle \frac{1}{N_0} \rangle, H \begin{pmatrix} \frac{h_0}{N_1} \\ \frac{1}{N_1} \end{pmatrix} \right)$ is a Heegner point on $X_K(N)$ in the sense of Definition 2.2. By CM theory, $P \in X_K(N)(K^{\mathrm{ab}})$. The conductor of P is also defined to be c, the conductor of $\mathcal{O}_c$. For details, see Section 2.

Assume ϕ corresponds to an elliptic curve $E/\mathbb{Q}$, by modularity of elliptic curves, Jacquet-Langlands correspondence and [27, Theorem 3.8], there is a modular parametrization $f : X_K(N) \to E$, taking $[\infty]$ to identity in E. It is unique in the sense that given two parametrizations f_1, f_2, there exist integers n_1, n_2 such that $n_1 f_2 = n_2 f_2$ [3, Proposition 3.8]. Now we can formulate the following Gross-Zagier formula:

Theorem 1.1 ([3]). *Under the assumption* $(*)$

$$L'(1, E, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2 (\phi,\phi)_{\Gamma_0(N)}}{u^2 c \sqrt{|D_K|}} \frac{\widehat{h}_K(P_\chi(f))}{\deg f}, \tag{GZ}$$

where $(\ ,\ )_{\Gamma_0(N)}$ *is the Petersson inner product,* $\hat{h}_K$ *is the Néron-Tate height over* K, $\mu(N,D)$ *is the number of prime factors of* (N,D), $u=[\mathcal{O}_c^\times:\{\pm 1\}]$.

As an application of such a kind of parametrization, we will construct a family of quadratic twists of an elliptic curve with Mordell-Weil groups of rank one. The action of complex conjugation on the CM-points of the modular curve is a crucial point in the proof of the nontriviality of the Heegner point. For the usual modular curve $X_0(N)$, complex conjugation is essentially the Atkin-Lehner operator. However, it does not hold for the modular curve $X_K(N)$. We will find that the action of complex conjugation is given in terms of a combination of local Atkin-Lehner operators and the nontrivial normalizer of $K^\times$ in $\mathrm{GL}_2(\mathbb{Q})$. Denote this operator by w. Then $f+f^w$ is a constant map with its image a nontrivial 2-torsion point; see Lemma 3.8. This phenomenon and the norm compatible relation control the divisibility of Heegner cycles. Together with the Gross-Zagier formula, the divisibility of Heegner cycles implies the 2-part of the BSD conjecture for our family of quadratic twists.

For each square free nonzero integer $d\neq 1$, we write $E^{(d)}$ for the twist of an elliptic curve $E/\mathbb{Q}$ by the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. The results of [26], [2], [5], [14] show that there are infinitely many d such that $L(E^{(d)},s)$ is nonvanishing at $s=1$, and infinitely many d such that $L(E^{(d)},s)$ has a simple zero at $s=1$.

The work of [21], [22] for the elliptic curve $(X_0(32),[\infty]):y^2=x^3-x$ constructs explicitly families of d with $\mathrm{ord}_{s=1}L(E^{(d)},s)=1$. The work of [4] deals with the elliptic curve $E=(X_0(49),[\infty])$ which has CM by $\sqrt{-7}$, gets similar results to [21].

Here, we construct a family of quadratic twists of $E=(X_0(36),[\infty])$ such that the ranks of the Mordell-Weil groups for these twists are one. In this paper, we have made a new argument different from [4], [21] and [22], which is much shorter and simpler. The new argument relies on a norm compatible relation between Heegner points of different conductors. See Theorem 2.15.

Theorem 1.2. *Let* ℓ *be a prime such that* 3 *is split in* $\mathbb{Q}(\sqrt{-\ell})$ *and* 2 *is unramified in* $\mathbb{Q}(\sqrt{-\ell})$. *Let* $M=q_1\cdots q_r$ *be a positive square-free integer with prime factors* q_i *all inert in* $\mathbb{Q}(\sqrt{-3})$, $q_i\equiv 1\,(\mathrm{mod}\,4)$ *and* q_i *inert in* $\mathbb{Q}(\sqrt{-\ell})$. *Then*

(1) $\mathrm{ord}_{s=1}L(s,E^{(-\ell M)})=1=\mathrm{rank}E^{(-\ell M)}(\mathbb{Q})$;
(2) $\#Ш(E^{(-\ell M)}/\mathbb{Q})$ *is odd, and the p-part of the full BSD conjecture of* $E^{(-\ell M)}$ *holds for* $p\nmid 3\ell M$, *i.e.,*

$$\mathrm{ord}_p\left(\frac{L'(E^{(-\ell M)})}{\Omega(E^{(-\ell M)})\mathrm{Reg}(E^{(-\ell M)})}\right)=\mathrm{ord}_p\left(\frac{\#Ш(E^{(-\ell M)})}{\prod_{q<\infty}c_q(E^{(-\ell M)})(\#E^{(-\ell M)}(\mathbb{Q})_{\mathrm{tor}})^2}\right).$$

The nontriviality of Heegner cycles and Gross-Zagier formula also imply the rank part of BSD conjecture for $E^{(M)}$, namely,

$$\mathrm{ord}_{s=1}L(s,E^{(M)})=0=\mathrm{rank}E^{(M)}(\mathbb{Q}).$$

We are also interested in the full BSD conjecture for $E^{(M)}$. In fact, the part (2) of Theorem 1.2 depends on the similar assertion for $E^{(M)}$, which is the part (2) of Theorem 1.3.

A new feature of this paper is that we give a parallel proof of the BSD conjecture for $E^{(M)}$ as we have mentioned above, that is, using the Waldspurger formula and the norm property of Gross points. For the induction method used in [4], [23], there is an embedding problem of imaginary quadratic fields to quaternion algebras

which is related to the problem of representing integers by ternary quadratic forms (see also the argument before [4, Definition 5.5], [23, Section 2.1] and [13]). The use of the norm compatible property of Gross points avoids this embedding problem.

If, for the data (ϕ, K, χ), the root number $\epsilon(\phi, \chi)$ equals $+1$, by [3] we can choose an appropriate definite quaternion algebra B over $\mathbb{Q}$ containing K, an order R of B of discriminant N with $R \cap K = \mathcal{O}_K$ and a "unique" function $f : B^\times \backslash \widehat{B}^\times / \widehat{R}^\times \to \mathbb{C}$. Assume the conductor c of χ satisfies $(c, N) = 1$. Let $x_c \in K^\times \backslash \widehat{B}^\times / \widehat{R}^\times$ be a Gross point of conductor c, that is, x_c satisfies that $x_c \widehat{R} x_c^{-1} \cap \widehat{K} = \widehat{\mathcal{O}}_c$. Denote by

$$P_\chi(f) = \sum_{\sigma \in \mathrm{Gal}(H_c/K)} f(\sigma \cdot x_c)\chi(\sigma).$$

Then with similar notation as for Gross-Zagier formula, we have the Waldspurger formula (see Theorem 2.16)

$$L(1, E, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \frac{|P_\chi(f)|^2}{\langle f, f \rangle}.$$

Moreover, the Gross points of different conductors also form an "Euler system" (see Section 2). The following theorem can be viewed as the rank zero version of Theorem 1.2:

Theorem 1.3. *Let $M = q_1 \cdots q_r$ be a positive square-free integer with prime factors q_i all inert in $\mathbb{Q}(\sqrt{-3})$ and $q_i \equiv 1 \pmod 4$; then*

1. $\mathrm{ord}_{s=1} L(s, E^{(M)}) = 0 = \mathrm{rank} E^{(M)}(\mathbb{Q})$;
2. $\#Ш\left(E^{(M)}/\mathbb{Q}\right)$ *is odd, and the p-part of the full BSD conjecture of $E^{(-\ell M)}$ holds for $p \neq 3$.*

2. The modular curve and Heegner points

2.1. **The modular curve $X_K(N)$.** Let K be an imaginary quadratic field with discriminant D. Let $N = N_0 N_1^2$ be a positive integer such that $p | N_1$ if and only if p is inert in K. Let c be another positive integer coprime to N. Take an embedding $K \hookrightarrow M_2(\mathbb{Q})$ which is admissible in the sense that

$$K \cap M_2(\mathbb{Z}) = K \cap R_0(N_0) = \mathcal{O}_c.$$

Let R be the order of $M_2(\mathbb{Z})$ given by $R = \mathcal{O}_c + N_1 R_0(N_0)$. Then R has discriminant N with $R \cap K = \mathcal{O}_c$.

Let $\Gamma_K(N) = R^\times \cap \mathrm{SL}_2(\mathbb{Z})$ and $X_K(N)$ be the modular curve over $\mathbb{Q}$ with level $\Gamma_K(N)$. It's well known that $X(N_0 N_1)(\mathbb{C})$ parameterizes $(E, (\mathbb{Z}/N_0 N_1)^2 \simeq E[N_0 N_1]))$ where E is an elliptic curve over $\mathbb{C}$. By [9] chapter 3.5, it parameterizes $(E, (\mathbb{Z}/N_0)^2 \simeq E[N_0], (\mathbb{Z}/N_1)^2 \simeq E[N_1]))$. Then by [9] chapter 7, $X_K(N)$ parameterizes $(E, C, \alpha : (\mathbb{Z}/N_1)^2 \simeq E[N_1]))$, where C is a cyclic subgroup of $E[N_0]$ of order N_0, and α is an H-orbit of a basis of $E[N_1]$ where $H := (\mathcal{O}_K/N_1\mathcal{O}_K)^\times \subset \mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$. Precisely, the class of $z \in \mathscr{H}$ in $X_K(N)$ corresponds to the triple

$$\left(\mathbb{C}/\mathbb{Z} \cdot z + \mathbb{Z}, \left\langle \frac{1}{N_0} \right\rangle, H \begin{pmatrix} \frac{z}{N_1} \\ \frac{1}{N_1} \end{pmatrix}\right).$$

Recall that $h_0 = \mathscr{H}^{K^\times}$. For X a field, a quaternion algebra over $\mathbb{Q}$ (the situations involved in this paper), or an order in them, we denote $\widehat{X} = X \otimes_{\mathbb{Z}} \prod_{\ell<\infty} \mathbb{Z}_\ell$.

Lemma 2.1. *If m is a positive integer and $(m, cND_K) = 1$, then for any invertible fractional ideals $\mathfrak{a}, \mathcal{N}$ of $\mathcal{O}_{cm}$, satisfying $\mathcal{N}^{-1}\mathfrak{a}/\mathfrak{a} \simeq \mathbb{Z}/N_0\mathbb{Z}$, there exist a $\mathbb{Z}$-basis $\{u, v\}$ of $\mathfrak{a}$ and $g \in \mathrm{GL}_2^+(\mathbb{Q})$, such that $\mathcal{N}^{-1}\mathfrak{a} = \mathbb{Z}\frac{u}{N_0} + \mathbb{Z}v$, $\frac{v}{u} = g^{-1}h_0$, and $K \cap gRg^{-1} = \mathcal{O}_{cm}$.*

Proof. Consider the natural projection between curves over $\mathbb{Q}$: $X_K(N) \to X_0(N_0)$, which is the forgetful functor in the moduli aspect $(E, C, [\alpha]) \mapsto (E, C)$. $\mathfrak{a}, \mathcal{N}$ define a Heegner point $(\mathbb{C}/\mathfrak{a}, \mathcal{N}^{-1}\mathfrak{a}/\mathfrak{a})$ on $X_0(N_0)$. Then there exists a $\mathbb{Z}$-basis $\{u, v\}$ of $\mathfrak{a}$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$, such that $\mathcal{N}^{-1}\mathfrak{a} = \mathbb{Z}\langle\frac{u}{N_0}, v\rangle$, $\frac{v}{u} = g^{-1}h_0$, and $K \cap g\widehat{R_0(N_0)}g^{-1} = \mathcal{O}_{cm}$. If we choose another basis, g will differ by an element in $\Gamma_0(N_0)$ on the right and an element in $K^\times$ on the left. So we have to prove there exists $g' \in \Gamma_0(N_0)$, such that $K \cap gg'\widehat{R}g'^{-1}g^{-1} = \mathcal{O}_{cm}$.

Denote by $\mathcal{O}' = g^{-1}\mathcal{O}_{cm}g$, it suffices to prove that there exists $g' \in \Gamma_0(N_0)$, such that for any $\ell | N_1$, $\mathcal{O}'_\ell \subset g'R_\ell g'^{-1}$. In fact, if it holds, then

$$\mathcal{O}'_\ell \subset g^{-1}K_\ell g \cap g'R_\ell g'^{-1},$$

hence they are equal, since $\mathcal{O}'_\ell$ is the maximal compact subring of $g^{-1}K_\ell g$. This implies that $\mathcal{O}' = g^{-1}Kg \cap g'\widehat{R}g'^{-1}$. i.e., $K \cap gg'\widehat{R}g'^{-1}g^{-1} = \mathcal{O}_{cm}$.

Note that $\mathcal{O}_\ell \subset R_\ell$, by Lemma 2.7, there exists a $g_\ell \in \mathrm{SL}_2(\mathbb{Z}_\ell)$, such that $\mathcal{O}'_\ell = g_\ell \mathcal{O}_\ell g_\ell^{-1}$. By Lemma 2.9, there exists a $g' \in \Gamma_0(N_0)$, such that

$$g' \equiv g_\ell \,(\mathrm{mod}\, \ell^{\mathrm{ord}_\ell N_1}) \ \forall \ell | N_1.$$

Let $\beta : M_2(\mathbb{Z}_\ell) \to M_2(\mathbb{Z}_\ell/N_1\mathbb{Z}_\ell)$, be the natural projection. We see that $g'R_\ell g'^{-1} = \beta^{-1}(\beta(\mathcal{O}'_\ell))$. This induces $\mathcal{O}'_\ell \subset g'R_\ell g'^{-1}$. □

Definition 2.2. Let $\mathfrak{a}, \mathcal{N}$ and u, v, g be as in Lemma 2.1. A Heegner point on $X_K(N)$ of conductor cm is a triple

$$P = \left(\mathbb{C}/\mathfrak{a}, \mathcal{N}^{-1}\mathfrak{a}/\mathfrak{a}, H\begin{pmatrix} \frac{v}{N_1} \\ \frac{u}{N_1} \end{pmatrix}\right).$$

Remark 2.3. This point corresponds to the point $\frac{v}{u} \in \mathscr{H}$.

The order $\mathcal{O}_c$ is of the form $\mathbb{Z} + \mathbb{Z}\varpi_c$ where $\varpi_c = \frac{cD + c\sqrt{D}}{2}$. Denote by $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$ the image of ϖ_c under the fixed embedding $K \hookrightarrow M_2(\mathbb{Q})$. Since K is a field, $yz \neq 0$.

Lemma 2.4. *$K = \mathbb{Q} + \mathbb{Q}h_0$ and $\mathcal{O}_c = \mathbb{Z} + \mathbb{Z}yh_0^{-1}$.*

Proof. We have $x + w = Dc, xw - yz = \frac{c^2(D^2 - D)}{4}$. As h_0 is fixed by $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$,

$$\frac{xh_0 + y}{zh_0 + w} = h_0 \quad \text{and} \quad zh_0^2 + (w - x)h_0 - y = 0.$$

Hence

$$h_0 = \frac{(x-w)+c\sqrt{D}}{2z} \in K\backslash\mathbb{Q} \quad \text{and} \quad h_0^{-1} = \frac{2z}{(x-w)+c\sqrt{D}} = \frac{(x-w)-c\sqrt{D}}{2y},$$

so

$$yh_0^{-1} = -w + \frac{Dc + c\sqrt{D}}{2}.$$

□

Lemma 2.5. *Let* $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\cdot h_0^{-1}$ *and* $\mathcal{N}^{-1} = \mathbb{Z} + \mathbb{Z}\cdot N_0^{-1}h_0^{-1}$. *Then* $\mathrm{End}(\mathfrak{a}) := \{x \in K : x\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_c$, *and* $\mathrm{End}(\mathcal{N}^{-1}) = \mathcal{O}_c$.

Proof. Let $(a + bh_0^{-1})\mathfrak{a} \subset \mathfrak{a}$. It is equivalent to that

$$(a + bh_0^{-1}) \in \mathfrak{a} \quad \text{and} \quad (a + bh_0^{-1})h_0^{-1} \in \mathfrak{a}.$$

The first condition implies $a, b \in \mathbb{Z}$; then the second one is equivalent to $bh_0^{-2} \in \mathfrak{a}$. But

$$bh_0^{-2} = y^{-1}b((w-x)h_0^{-1} + z) \in \mathfrak{a}.$$

The condition $R \cap K = \mathcal{O}_c$ tells $(w - x, z, y) = 1$, so the above condition implies $b \in y\mathbb{Z}$, which tells us that $\mathrm{End}(\mathfrak{a}) = \mathcal{O}_c$. The assertion for $\mathcal{N}^{-1}$ is similar, noticing that $N_0|z$. □

Clearly, $\mathfrak{a}$ and $\mathcal{N}$ are invertible ideals of $\mathcal{O}_c$, and $\mathcal{N}^{-1}/\mathfrak{a} \simeq \mathbb{Z}/N_0\mathbb{Z}$. Summing up:

Proposition 2.6. *Let* $K \hookrightarrow M_2(\mathbb{Q})$ *be an admissible embedding and* $h_0 \in \mathcal{H}^{K^\times}$. *Denote by* $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\cdot h_0^{-1}$ *and* $\mathcal{N}^{-1} = \mathbb{Z} + \mathbb{Z}\cdot N_0^{-1}h_0^{-1}$; *then*

$$P = \left(\mathbb{C}/\mathfrak{a}, \mathcal{N}^{-1}/\mathfrak{a}, H\begin{pmatrix} \frac{y}{N_1} \\ \frac{yh_0^{-1}}{N_1} \end{pmatrix}\right)$$

is a Heegner point on $X_K(N)$ *of conductor* c.

Now we prove lemmas needed in Lemma 2.1.

Lemma 2.7. *For any two embeddings* $\varphi_i : \mathbb{Z}_{p^2} \to M_2(\mathbb{Z}_p), i = 1, 2$, *there exists* $g \in \mathrm{SL}_2(\mathbb{Z}_p)$, *such that* $\varphi_1 = g^{-1}\varphi_2 g$.

Remark 2.8. If we change $\mathbb{Z}_p$ to $\mathbb{Q}_p$, $\mathbb{Z}_{p^2}$ to $\mathbb{Q}_{p^2}$ and SL_2 to GL_2, this lemma is well-known as a consequence of Noether-Skolem theorem.

Proof. Consider $V = \mathbb{Z}_p \oplus \mathbb{Z}_p$, with the natural action of $M_2(\mathbb{Z}_p)$. Via φ_i, we view V as a $\mathbb{Z}_{p^2}$-module, denoted by $V_i, i = 1, 2$. Since $\mathbb{Z}_{p^2}$ is a discrete valuation ring and V_i are torsion free, both V_1, V_2 are free $\mathbb{Z}_{p^2}$-modules of rank one. So there exists an isomorphism $g_0 : V_1 \to V_2$ of $\mathbb{Z}_{p^2}$-modules, this isomorphism corresponds to an element of $\mathrm{GL}_2(\mathbb{Z}_p)$, also denoted by g_0. The fact g_0 is an isomorphism of $\mathbb{Z}_{p^2}$-modules means that

$$g_0\varphi_1(x) = \varphi_2(x)g_0 \ \forall x \in \mathbb{Z}_{p^2}.$$

Note that $\mathrm{N}_{\mathbb{Z}_{p^2}/\mathbb{Z}_p}\mathbb{Z}_{p^2}^\times = \mathbb{Z}_p^\times$, choose $t \in \mathbb{Z}_{p^2}^\times$, such that $\mathrm{N}_{\mathbb{Z}_{p^2}/\mathbb{Z}_p}t = (\det g_0)^{-1}$, i.e., $\det\varphi_1(t) = (\det g_0)^{-1}$. Therefore

$$g_0\varphi_1(t)\varphi_1(x) = g_0\varphi_1(x)\varphi_1(t) = \varphi_2(x)g_0\varphi_1(t).$$

So $g = g_0\varphi_1(t) \in \mathrm{SL}_2(\mathbb{Z}_p)$ is the desired element. □

Lemma 2.9. *Let M_1, M_2 be two coprime positive integers, and let $\varphi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/M_1\mathbb{Z})$ be the natural projection. Then $\varphi(\Gamma_0(M_2)) = \mathrm{SL}_2(\mathbb{Z}/M_1\mathbb{Z})$.*

Proof. By Chinese remainder theorem, we have

$$\mathrm{SL}_2(\mathbb{Z}/(M_1M_2\mathbb{Z})) \simeq \mathrm{SL}_2(\mathbb{Z}/M_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/M_2\mathbb{Z}).$$

Given any $g \in \mathrm{SL}_2(\mathbb{Z}/M_1\mathbb{Z})$, let $g' \in \mathrm{SL}_2(\mathbb{Z}/(M_1M_2\mathbb{Z}))$ correspond to $(g, 1) \in \mathrm{SL}_2(\mathbb{Z}/M_1\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/M_2\mathbb{Z})$ via the above isomorphism. It's well-known that for any integer M, $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/M\mathbb{Z})$ is surjective. So we choose a matrix G such that $G \equiv g' \pmod{M_1M_2}$. Then $G \in \Gamma(M_2) \subset \Gamma_0(M_2)$ and $\varphi(G) = g$. □

Example 2.1. Now we construct an admissible embedding $K \hookrightarrow M_2(\mathbb{Q})$ as following. Since $\ell | N_0$ implies that ℓ is split in K, there exists an integral ideal $\mathfrak{N}_0$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{N}_0 \simeq \mathbb{Z}/N_0$, which implies $\mathbb{Z} + \mathfrak{N}_0 = \mathcal{O}_K$. Then there exists $n \in \mathbb{Z}$ and $m \in \mathfrak{N}_0$ such that

$$\frac{D + \sqrt{D}}{2} = n + m.$$

Taking trace and norm, we get

$$D = 2n + (m + \bar{m}) \quad \text{and} \quad \frac{D^2 - D}{4} = n^2 + n(m + \bar{m}) + m\bar{m}.$$

Since $m\bar{m} \in \mathfrak{N}_0\overline{\mathfrak{N}_0} = N_0\mathcal{O}_K$ and it is an integer, we have $m\bar{m} = N_0b$ for some $b \in \mathbb{Z}$. Let $a = D - 2n$. We see that

$$D = a^2 - 4N_0b.$$

It's easy to check that $(a, b, N_0) = 1$. Given an integer c such that $(c, N) = 1$, we let the embedding $i_c : K \longrightarrow B$ be given by

$$\frac{D + \sqrt{D}}{2} \longmapsto \begin{pmatrix} \frac{D+a}{2} & -c^{-1} \\ N_0bc & \frac{D-a}{2} \end{pmatrix}, \text{ or } \frac{Dc + \sqrt{Dc^2}}{2} \longmapsto \begin{pmatrix} \frac{Dc+ac}{2} & -1 \\ N_0bc^2 & \frac{Dc-ac}{2} \end{pmatrix}.$$

We can see this embedding is normalized in the sense of [18, p. 104], and

$$h_0 = \frac{a + \sqrt{D}}{2N_0bc}.$$

We should mention that, for the normalized embedding, we have Shimura's reciprocity law, which interpretes the Galois action on Heegner points.

The modular curve $X_K(N)$ depends on the admissible embedding $K \hookrightarrow M_2(\mathbb{Q})$. However, we will prove that all those modular curves given by admissible embeddings are isomorphic over $\mathbb{Q}$. Let $i : K \hookrightarrow M_2(\mathbb{Q})$ be an admissible embedding. Let $H = i(\mathcal{O}_K/N_1\mathcal{O}_K) \subset \mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$, and let H_0 be the upper-triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/N_0\mathbb{Z})$; then $H = \prod_{p|N_1} H_p$, where $H_p \subset \mathrm{GL}_2(\mathbb{Z}/p^{\mathrm{ord}_p N_1}\mathbb{Z})$. Then

$$X_K(N) = X(N_0N_1)/(H \times H_0).$$

If i' is another admissible embedding, and for any $p|N_1$, H_p and H'_p are conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^{\mathrm{ord}_p N_1}\mathbb{Z})$, we obviously have

$$X(N_0N_1)/(H \times H_0) \simeq X(N_0N_1)/(H' \times H_0).$$

In fact, H_p is the image of the composition homomorphism of $\mathbb{Z}_{p^2}^\times \to \mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}_p/p^{\mathrm{ord}_p(N_1)}\mathbb{Z}_p)$. Lemma 2.7 implies that H_p and H_p' are conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^{\mathrm{ord}_p N_1}\mathbb{Z})$. Thus,

Proposition 2.10. *The modular curve $X_K(N)$ is unique up to an isomorphism over $\mathbb{Q}$.*

Cusps. Now we study the cusps on $X_K(N)$.

Lemma 2.11. *Let ζ_{N_1} be a primitive N_1-th root of unity. Then the cusp $[\infty]$ of $X_K(N)$ is defined over $\mathbb{Q}(\zeta_{N_1})$.*

Proof. In the adelic language, we have the following complex uniformization:

$$X_K(N)(\mathbb{C}) = \mathrm{GL}_2^+(\mathbb{Q})\backslash\mathcal{H} \times \mathrm{GL}_2(\widehat{\mathbb{Z}})/\widehat{R}^\times \cup \{\text{cusps}\},$$

where the cusps are

$$\mathrm{GL}_2^+(\mathbb{Q})\backslash\mathbb{P}^1(\mathbb{Q}) \times \mathrm{GL}_2(\widehat{\mathbb{Z}})/\widehat{R}^\times.$$

The cusps are all defined over $\mathbb{Q}^{\mathrm{ab}}$. By [16, p. 507], if we let $r : \widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ be the Artin map, then $r(x) \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ acts on the cusps by left multiplication the matrix $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$. Since $\widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times \simeq \widehat{\mathbb{Z}}^\times$, if $x \in \widehat{\mathbb{Z}}^\times$ is such that $r(x)\cdot[\infty, 1] = [\infty, 1]$, there exists $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$, such that $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in \widehat{R}^\times$, which implies

$$\gamma \in \mathbb{Z}_p^\times,\ \alpha x_p \in \mathbb{Z}_p^\times,\ \beta \in N_1\mathbb{Z}_p \text{ for all } p, \text{ and } \alpha x_p \equiv \gamma \,(\mathrm{mod}\, N_1) \text{ for all } p|N_1.$$

Hence $\alpha = \gamma = \pm 1$, and $x_p \equiv 1 \,(\mathrm{mod}\, N_1)$. So the definition field of $[\infty, 1]$ corresponds to

$$\widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times\mathbb{Z}^{\times(N_1)} \prod_{p|N_1}(1 + N_1\mathbb{Z}_p),$$

via class field theory, this is $\mathbb{Q}(\zeta_{N_1})$. □

In the following, we fix the embedding $i_c : K \hookrightarrow M_2(\mathbb{Q})$ given in Example 2.1.

Atkin-Lehner operator. For each $p \mid N_0$, let

$$w_p = \begin{pmatrix} 0 & 1 \\ p^{\mathrm{ord}_p N} & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

be the local Atkin-Lehner operator.

Although it will not be used later in this paper, to compare with equation (5.1) of [7], we give a description of w_pP for $p|N_0$ and $P = \left(\mathbb{C}/\mathfrak{a}, \mathcal{N}^{-1}\mathfrak{a}/\mathfrak{a}, H\begin{pmatrix} \frac{v}{N_1} \\ \frac{u}{N_1} \end{pmatrix}\right)$.

Write $N_0 = p^k m$ with $(p, m) = 1$. We can choose $a, b \in \mathbb{Z}$ such that $p^k a + mb = 1$. Let $g = \begin{pmatrix} p^k & 1 \\ -N_0 b & p^k a \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}) \cap M_2(\mathbb{Z})$, such that $g^{-1}w_p \in \widehat{R}^\times$, so

$$w_pP = [v/u, w_p] = [g^{-1}v/u, 1] = \left(\mathbb{C}/\mathbb{Z}\cdot g^{-1}v/u + \mathbb{Z}, \left\langle\frac{1}{N_0}\right\rangle, H\begin{pmatrix} \frac{g^{-1}v/u}{N_1} \\ \frac{1}{N_1} \end{pmatrix}\right).$$

Modifying it, we get

$$w_p P = \left(\mathbb{C}/\mathfrak{a}', \mathcal{N}'^{-1}\mathfrak{a}'/\mathfrak{a}', H\begin{pmatrix} \frac{av-u/p^k}{N_1} \\ \frac{mbv+u}{N_1}\end{pmatrix}\right)$$

where $\mathfrak{a}' = \mathbb{Z}\langle v, u/p^k\rangle$ and $\mathcal{N}'^{-1}\mathfrak{a}' = \mathbb{Z}\langle v/p^k, u/(p^k m)\rangle$. Considering the quotient map $\xi : X_K(N) \to X_0(N_0)$ induced by $\Gamma_K(N) \subset \Gamma_0(N_0)$, which is defined over $\mathbb{Q}$, the above argument says that $\xi \circ w_p = w_p \circ \xi$, where the action of w_p on $X_0(N_0)$ is defined by [7, p. 90].

Take $j = \begin{pmatrix} 1 & 0 \\ ac & -1\end{pmatrix}$, then $kj = j\overline{k}$ for all $k \in K$ where $^-$is the complex conjugation of K and coincides with the nontrivial element in $\mathrm{Gal}(K/\mathbb{Q})$.

Define

$$w = j^{(N_0)} \cdot \prod_{p|N_0} w_p \in \mathrm{GL}_2(\widehat{\mathbb{Q}}) \cap M_2(\widehat{\mathbb{Z}}).$$

Since w normalizes $\widehat{R}^\times$, it acts on $X_K(N)$. To study the action of w on $X_K(N)$, we can prove the following lemma:

Lemma 2.12. *There exists $t_0 \in \widehat{K}^\times$ and $u \in \widehat{R}^\times$ such that $w = t_0 j u$.*

Proof. For $p|N_0$, let $k = \mathrm{ord}_p N_0 \geq 1$, $K_p^\times = (\mathbb{Q}_p + \mathbb{Q}_p(\sqrt{D}))^\times$. Let $x, y \in \mathbb{Q}_p$; then

$$(x + y\sqrt{D}) j_p^{-1} w_p = \begin{pmatrix} -2p^k y & x + ay \\ -p^k(x+ay) & a(x+ay) - 2N_0 by\end{pmatrix}.$$

So we choose $\mathrm{ord}_p y = -k - \mathrm{ord}_p 2, x + ay \in \mathbb{Z}_p$ and such that $a(x+ay) \in \mathbb{Z}_p^\times$. Then let $t_{0,p} = x + y\sqrt{D}$.

For $p \nmid N_0$, let $t_{0,p} = 1$. Then such choice of t_0 works. □

Remark 2.13. By Shimura reciprocity law, if we use $[x] \mapsto \overline{[x]}$ to denote the complex conjugation on $X_K(N)(\mathbb{C})$, then

$$\overline{[h_0, g]} = [h_0, jg] \ \forall g \in \mathrm{GL}_2(\mathbb{A}_f).$$

Lemma 2.12 in fact tells us that the action of w on certain Heegner points is a combination of a Galois action and complex conjugation. For details, we can see the proof of Lemma 3.11.

Hecke correspondences. Let $\ell \nmid N$ be a prime. The Hecke correspondence T_ℓ on X_U is defined by

$$T_\ell\left(E, C, H\begin{pmatrix} x_1 \\ x_2\end{pmatrix}\right) = \sum_i \left(E/C_i, (C + C_i)/C_i, H\begin{pmatrix} x_1 \bmod C_i \\ x_2 \bmod C_i\end{pmatrix}\right),$$

where the sum is taken over all cyclic subgroups C_i of E of order ℓ, α_i is given by $(\mathbb{Z}/N_1\mathbb{Z})^2 \xrightarrow{\alpha} E[N_1] \simeq (E/C_i)[N_1]$. $E[N_1] \simeq (E/C_i)[N_1]$ is because $(\ell, N) = 1$. This is just by definition.

2.2. **Gross-Zagier formula.** Let E be an elliptic curve of conductor N, let K be an imaginary quadratic field of discriminant D and let χ be a ring class character over K of conductor c. Assume

$$E, K, \chi \text{ satisfy the condition } (*).$$

Then we can write $N = N_0 N_1^2$, where $p|N$ is inert in K if and only if $p|N_1$.

Embed K in $M_2(\mathbb{Q})$ by i_c. There is a modular parametrization $f : X_K(N) \to E$ mapping $[\infty]$ to the identity of E. If f_1, f_2 are two such morphisms, then there exist integers n_1, n_2 such that $n_1 f_1 = n_2 f_2$. Let h_0 be the point in $\mathcal{H}$ fixed by $K^\times$; then $\mathcal{O}_c = \mathbb{Z} + \mathbb{Z}h_0^{-1}$, $\mathcal{N} = \mathbb{Z} + \mathbb{Z}N_0^{-1}h_0^{-1}$ is an invertible ideal of $\mathcal{O}_c$ such that $\mathcal{N}/\mathcal{O}_c \cong \mathbb{Z}/N_0\mathbb{Z}$. Consider the following Heegner point on $X_K(N)$ of conductor c:

$$P = \left(\mathbb{C}/\mathcal{O}_c, \mathcal{N}/\mathcal{O}_c, H\begin{pmatrix}\frac{1}{N_1}\\ \frac{h_0^{-1}}{N_1}\end{pmatrix}\right) \in X_K(N)(H_c).$$

Form the cycle:

$$P_\chi(f) = \sum_{\sigma \in \mathrm{Gal}(H_c/K)} f(P^\sigma)\chi(\sigma) \in E(H_c) \otimes_{\mathbb{Z}} \mathbb{C}.$$

Theorem 2.14 (Explicit Gross-Zagier formula [3])**.** *We have the following equation:*

$$L'(1, E, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2(\phi,\phi)_{\Gamma_0(N)}}{u^2 c\sqrt{|D|}} \frac{\widehat{h}_K(P_\chi(f))}{\deg f}. \tag{GZ}$$

Here ϕ is the normalized newform associated to E, $\mu(N, D)$ is the number of prime factors of (N, D), $u = [\mathcal{O}_K^\times : \mathbb{Z}^\times]$, $\widehat{h}_K$ is the Néron-Tate height pairing over K and $(\phi, \phi)_{\Gamma_0(N)}$ is the Petersson inner product defined by

$$(\phi,\phi)_{\Gamma_0(N)} = \int_{\Gamma_0(N)\backslash\mathcal{H}} |\phi(x+iy)|^2 dxdy.$$

2.3. **Euler system.** Let S be a finite set of primes containing the prime factors of $6cND_K$,

$$\mathbb{N}_S = \{n \text{ is an integer} : \ell | n \Rightarrow \ell \notin S\}.$$

For any $\ell, m \in \mathbb{N}_S$ with ℓ a prime and $\ell \nmid m$, let $P_m = (\mathbb{C}/\mathfrak{a}_m, \mathcal{N}_m^{-1}\mathfrak{a}_m/\mathfrak{a}_m, \alpha_m)$ be a Heegner point of conductor cm. Let $P_{m\ell} = (\mathbb{C}/\mathfrak{a}_{m\ell}, \mathcal{N}_{m\ell}^{-1}\mathfrak{a}_{m\ell}/\mathfrak{a}_{m\ell}, \alpha_{m\ell})$, such that $\mathcal{N}_{m\ell} = \mathcal{N}_m \cap \mathcal{O}_{m\ell}$, $\mathfrak{a}_{m\ell} = \mathfrak{a} \cap \mathcal{O}_{m\ell}$, and $\alpha_{m\ell}$ is the composition

$$(\mathbb{Z}/N_1\mathbb{Z})^2 \xrightarrow{\alpha_m} N_1^{-1}\mathfrak{a}_m/\mathfrak{a}_m \xrightarrow{\sim} N_1^{-1}\mathfrak{a}_{m\ell}/\mathfrak{a}_{m\ell}.$$

Theorem 2.15. *We have that $[H_{m\ell} : H_m] = (\ell+1)/u_m$ if ℓ is inert in K and $(\ell-1)/u_m$ if ℓ is split and*

$$u_m \sum_{\sigma \in \mathrm{Gal}(H_{m\ell}/H_m)} P_{m\ell}^\sigma = \begin{cases} \mathrm{T}_\ell P_m, & \text{if } \ell \text{ is inert in } K, \\ (\mathrm{T}_\ell - \sum_{w|\ell} \mathrm{Frob}_w) P_m, & \text{if } \ell \text{ is split in } K, \end{cases}$$

where T_ℓ is the Hecke correspondence, Frob_w is the Frobenius at $w|\ell$ in $\mathrm{Gal}(H_m/K)$, and $u_m = 1$ if $m \neq 1$ and $u_1 = [\mathcal{O}_K^\times : \mathbb{Z}^\times]$.

This theorem is proved in general by [10, Proposition 4.8] or [20, Theorem 3.1.1].

2.4. **Waldspurger formula and Gross points.** Let $\phi = \sum_{n=1}^{\infty} a_n q^n$ be a newform of weight 2, level $\Gamma_0(N)$, normalized such that $a_1 = 1$. Let K be an imaginary quadratic field of discriminant D and χ a ring class character over K of conductor c. Let $L(s, \phi, \chi)$ be the Rankin-Selberg convolution of ϕ and χ.

Assume that $(c, N) = 1$. Denote by $\mathbb{S}$ the set of primes $p|N$ satisfying one of the following conditions:

- p is inert in K with $\mathrm{ord}_p(N)$ odd;
- $p|D$, $\mathrm{ord}_p(N) = 1$ and $\chi([\mathfrak{p}]) = a_p$ where $\mathfrak{p}$ is the prime of $\mathcal{O}_K$ above p and $[\mathfrak{p}]$ is its class in $\mathrm{Pic}(\mathcal{O}_c)$;
- $p|D$, $\mathrm{ord}_p(N) \geq 2$ and the local root number of $L(s, \phi, \chi)$ at p equals $-\eta_p(-1)$ where η_p is the quadratic character for $K_p/\mathbb{Q}_p$.

Assume $\mathbb{S}$ has odd cardinality; then the sign of $L(s, \phi, \chi)$ is $+1$. Let B be the definite quaternion algebra defined over $\mathbb{Q}$ ramified exactly at primes in $\mathbb{S} \cup \{\infty\}$. Fix an embedding from K into B. Let R be an order in B with discriminant N and such that $R \cap K = \mathcal{O}_c$. Denote by $\hat{R} = R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ and $U = \hat{R}^\times$ which is an open compact subgroup of $\hat{B}^\times$. Consider the Shimura set $X_U = B^\times \backslash \hat{B}^\times / U$ which is a finite set. A point in X_U represented by $x \in \hat{B}^\times$ is denoted by $[x]$. Note that for $p|(D, N)$, $K_p^\times$ normalizes U and then $K_p^\times$ acts on X_U by right multiplication. Let

$$\mathbb{C}[X_U]^0 = \left\{ f \in \mathbb{C}[X_U] \,\middle|\, \sum_{x \in X_U} f(x) = 0 \right\}.$$

For each $p \nmid N$, there are Hecke correspondences T_p and S_p. In this case, B_p is split while U_p is maximal. Then the quotient $B_p^\times / U_p$ can be identified with $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$. Then for any $[x] \in X_U$,

$$S_p[x] := [x^{(p)} s_p], \quad T_p[x] := \sum_{h_p} [x^{(p)} h_p],$$

where if x_p corresponds to a lattice Λ, then s_p is the lattice $p\Lambda$ and the set $\{h_p\}$ is the set of sublattices Λ' of Λ with $[\Lambda : \Lambda'] = p$. There is then a line $V(\phi, \chi)$ of $\mathbb{C}[X_U]^0$ characterized as follows:

- for any $p \nmid N$, T_p acts on $V(\phi, \chi)$ by a_p and S_p acts trivially;
- for any $p|(D, N)$ with $\mathrm{ord}_p(N) \geq 2$, $K_p^\times$ acts on $V(\phi, \chi)$ by χ_p.

Let f be a nonzero vector in $V(\phi, \chi)$ and consider the period

$$P_\chi(f) = \sum_{\sigma \in \mathrm{Gal}(H_c/K)} f(\sigma)\chi(\sigma),$$

where the embedding of K into B induces a map

$$\mathrm{Gal}(H_c/K) = K^\times \backslash \hat{K}^\times / \widehat{\mathcal{O}}_c^\times \longrightarrow X_U.$$

Theorem 2.16 (Explicit Waldspurger formula [3])**.** *We have the following equation:*

$$L(1, \phi, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(N)}}{u^2 c \sqrt{|D|}} \frac{|P_\chi(f)|^2}{\langle f, f \rangle},$$

where the pairing is given by

$$\langle f, f\rangle = \sum_{[x]\in X_U} |f(x)|^2 w([x])^{-1}$$

and $w([x])$ *is the order of the finite group* $(B^\times \cap xUx^{-1})/\{\pm 1\}$.

There is an analogue to Heegner points, the so-called Gross points. Let S and $\mathbb{N}_S$ be the same as in Section 2.3.

Definition 2.17. Let $m \in \mathbb{N}_S$. A point $x_m \in K^\times\backslash\hat{B}^\times/U$ is called a **Gross point** of conductor cm, if $x_m U x_m^{-1} \cap \hat{K}^\times = \widehat{\mathcal{O}}_{cm}^\times$.

Each element in $K^\times\backslash\widehat{K}^\times/\widehat{\mathcal{O}}_{cm}^\times$ acts on x_m by left multiplication. This induces an action of $\mathrm{Gal}(H_{cm}/K)$ on x_m, also called the Galois action.

For each prime $\ell \in \mathbb{N}_S$, fix an isomorphism $\beta_\ell : B_\ell \xrightarrow{\sim} M_2(\mathbb{Q}_\ell)$, such that $\beta_\ell(U_\ell) = \mathrm{GL}_2(\mathbb{Z}_\ell)$, and, under this isomorphism, we have

- $\beta_\ell(K_\ell) = \left\{\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix} : a, b \in \mathbb{Q}_\ell\right\}$, if ℓ is split in K;
- $\beta_\ell(K_\ell) = \left\{\begin{pmatrix} a & b\delta \\ b & a\end{pmatrix} : a, b \in \mathbb{Q}_\ell\right\}$, where $\delta \in \mathbb{Z}_p^\times\backslash\mathbb{Z}_p^{\times 2}$, if ℓ is inert in K.

For $m \in \mathbb{N}_S$, define $x_m \in \widehat{B}^\times$ by

$$(x_m)_\ell = \begin{cases} \beta_\ell^{-1}\begin{pmatrix} \ell^{\mathrm{ord}_\ell m} & 0 \\ 0 & 1\end{pmatrix} & \ell | m, \\ 1 & \ell \nmid m. \end{cases}$$

Then the image of x_m in $K^\times\backslash\widehat{B}^\times/U$, still denoted by x_m, is a Gross point of conductor cm.

Theorem 2.18. *For any* $\ell, m \in \mathbb{N}_S$ *with* ℓ *a prime and* $\ell \nmid m$, *we have that*

$$u_m \sum_{\sigma\in\mathrm{Gal}(H_{cm\ell}/H_{cm})} [\sigma.x_{m\ell}] = \begin{cases} T_\ell[x_m], & \text{if } \ell \text{ is inert in } K, \\ (T_\ell - \sum_{w|\ell}\mathrm{Frob}_w)[x_m], & \text{if } \ell \text{ is split in } K, \end{cases}$$

where the equality holds as divisors on X_U, *with* Frob_w *and* u_m *the same as Theorem* 2.15.

The proof is the same as the norm relation of Heegner points on Shimura curves. One can refer to [10, Proposition 4.8] or [20, Theorem 3.1.1].

3. Quadratic twists of $X_0(36)$

The modular curve $X_0(36)$ has genus one and its cusp $[\infty]$ is rational over $\mathbb{Q}$ so that $E = (X_0(36), [\infty])$ is an elliptic curve defined over $\mathbb{Q}$. The elliptic curve E has CM by $\mathbb{Q}(\sqrt{-3})$ and has minimal Weierstrass equation

$$y^2 = x^3 + 1.$$

Note that its Tamagawa numbers are $c_2 = 3, c_3 = 2$ and $E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ is generated by the cusp $[0] = (2, 3)$. We use T to denote the nontrivial 2-torsion point in the following. Denote by $L^{\mathrm{alg}}(E, s)$ the algebraic part of $L(E, s)$. Then $L^{\mathrm{alg}}(E, 1) = 1/6$.

For a nonzero integer m, let $E^{(m)} : y^2 = x^3 + m^3$ be the quadratic twist of E by the field $\mathbb{Q}(\sqrt{m})$. Then $E^{(m)}$ and $E^{(-3m)}$ are 3-isogenous to each other.

Lemma 3.1. *Let $D \in \mathbb{Z}$ be a fundamental discriminant of a quadratic field. Then the sign for the functional equation of $E^{(D)}$, denoted by $\epsilon(E^{(D)})$, is*

$$(-1)^{\#\{p|D, p=2,3,\infty\}},$$

where $\infty|D$ means that $D < 0$.

Proof. For each D, denote by $K = \mathbb{Q}(\sqrt{D})$; then

$$L(s, E_K) = L(s, E)L(s, E^{(D)}),$$

where $L(s, E_K)$ is the base change L-function and it suffices to determine the sign of $L(s, E_K)$. Note that the local components of the cuspidal automorphic representation for E at places 2 and 3 are supercuspidal with conductor 2; then by [19, Proposition 3.5], the local root number for the base change L-function at places 2 (resp. 3) is negative if and only if $2|D$ (resp. $3|D$). Meanwhile, the local root number at ∞ is positive if and only if D is positive and for any place not dividing 6∞ it is positive. Summing up, the result holds. □

3.1. **The Waldspurger formula.** Let B be the definite quaternion algebra over $\mathbb{Q}$ ramified at $3, \infty$; then we know that

$$B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k, \quad i^2 = -1, j^2 = -3, k = ij = -ji.$$

Let $\mathcal{O}_B = \mathbb{Z}[1, i, (i + j)/2, (1 + k)/2]$ be a maximal order of B. The unit group $\mathcal{O}_B^\times$ of $\mathcal{O}_B$ is equal to

$$\{\pm 1, \pm i, \pm(i + j)/2, \pm(i - j)/2, \pm(1 + k)/2, \pm(1 - k)/2\}.$$

Let $K = \mathbb{Q}(\sqrt{-3})$ and $\eta : \widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times \to \{\pm 1\}$ be the quadratic character associated to K. Embed $K \hookrightarrow B$ by sending $\sqrt{-3}$ to k, this induces an embedding $\widehat{K}^\times \hookrightarrow \widehat{B}^\times$.

Let $\pi = \otimes_v \pi_v$ be the automorphic representation of $B_{\mathbb{A}}^\times$ corresponding to E via the modularity of E and the Jacquet-Langlands correspondence. Let $\mathcal{R} = \prod_p \mathcal{R}_p$ be an order of $\widehat{B}^\times$ defined as follows. If $p = 2$, then $\mathcal{R}_2 = \mathcal{O}_{K,2} + 2\mathcal{O}_{B,2}$. If $p = 3$, then $\mathcal{R}_3 = \mathcal{O}_{K,3} + \lambda\mathcal{O}_{B,3}$ where $\lambda \in B^\times$ is a uniformizer of B_3; for example, we may choose $\lambda = k$, which is also a uniformizer of K_3. For $p \nmid 6$, $\mathcal{R}_p = \mathcal{O}_{B,p}$. Denote by $U = \mathcal{R}^\times$. Then U is an open compact subgroup of $\widehat{B}^\times$.

The local components of π have the following properties:

- π_∞ is trivial;
- π_p is unramified if $p \neq 2, 3, \infty$, i.e., $\pi^{\mathcal{O}_{B,p}^\times}$ is one dimensional;
- $\pi_2^{\mathcal{O}_{K,2}^\times}$ is one dimensional and $\pi_3^{\mathcal{O}_{K,3}^\times}$ is two dimensional.

The first two properties are standard, while the last property comes from [3, proposition 3.8]. Then π^U is a representation of $B_3^\times$ with dimension 2. As $K_3^\times$-modules, $\pi^U = \mathbb{C}\chi_+ \oplus \mathbb{C}\chi_-$ where χ_+ is the trivial character of $K_3^\times$ and χ_- is the nontrivial quadratic unramified character on $K_3^\times$.

This representation π^U is naturally realized as a subspace of the space of the infinitely differentiable complex-valued functions $C^\infty(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times)$. The space π^U is contained in the space $C^\infty(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U)$ and is perpendicular to the spectrum consisting of characters (the residue spectrum). In fact, we have the following more

detailed proposition, which are easy calculations on automorphic representations, based on the discussion above:

Proposition 3.2. (1) *π^U has an orthonormal basis f_+, f_- under the Petersson inner product defined by*

$$\| f \|^2 = \int_{B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times} |f(g)|^2 dg$$

with the Tamagawa measure $\mathrm{Vol}(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times) = 2$.

(2) *Moreover, f_+ (resp. f_-) is the function on $B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U$, supported on those $g \in \widehat{B}^\times$ with $\chi_0(g) = +1$ (resp. $= -1$), valued in $0, \pm 1$ with total mass zero, where χ_0 is the composition of the following morphisms:*

$$B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U \xrightarrow{\det} \widehat{\mathbb{Q}}^\times \xrightarrow{\eta} \pm 1.$$

(3) *For any $t \in K_3^\times$, $\pi(t) f_+ = \chi_+(t) f_+$ and $\pi(t) f_- = \chi_-(t) f_-$.*

The values of $f_\pm$ on Gross points essentially induce Theorem 1.3, via explicit Waldspurger formula, as we will see later.

Since the class number of B with respect to $\mathcal{O}_B$ is 1 by [24, p. 152], one has

$$\widehat{B}^\times = B^\times \widehat{\mathcal{O}}_B^\times = B^\times B_3^\times \widehat{\mathcal{O}}_B^{\times(3)}.$$

Therefore,

$$B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U = B^\times \backslash B^\times B_3^\times \widehat{\mathcal{O}}_B^{\times(3)} / U_2 U_3 \widehat{\mathcal{O}}_B^{\times(6)} = H \backslash B_3^\times \mathcal{O}_{B,2}^\times / U_2 U_3,$$

where $H = B^\times \cap B_3^\times \widehat{\mathcal{O}}_B^{\times(3)} = \mathcal{O}_B^\times \lambda^{\mathbb{Z}} \subset B_3^\times \mathcal{O}_{B,2}^\times$ and the last inclusion is given by the diagonal embedding.

Lemma 3.3. *The double coset $H \backslash \mathcal{O}_{B,2}^\times / U_2$ is trivial and $H \cap U_2 \backslash B_3^\times / U_3 = \mathcal{O}_{B,3}^\times / U_3$.*

Proof. The proof is elementary. First, we prove that $H \backslash \mathcal{O}_{B,2}^\times / U_2$ is trivial. Recall that $U_2 = \mathcal{O}_{K,2}^\times (1 + 2M_2(\mathbb{Z}_2))$. As $\mathrm{GL}_2(\mathbb{Z}_2)/(1 + 2M_2(\mathbb{Z}_2)) = \mathrm{GL}_2(\mathbb{F}_2)$, for any $g \in \mathrm{GL}_2(\mathbb{F}_2)$, one may find $h \in H$ and $u \in \mathcal{O}_{K,2}^\times$ such that $g \equiv hu \,(\mathrm{mod}\, 2\mathbb{Z}_2)$. For the second claim, note that

$$H \cap U_2 = \langle k, -1, \frac{1+k}{2} \rangle.$$

For any $x \in B_3^\times$, $x^{-1}(1+\lambda)x = 1 + x^{-1}\lambda x \in U_3$ where λ is any uniformizer of $B_3^\times$. In particular, the action of $H \cap U_2$ on $B_3^\times / U_3$ is equal to the action of the group generated by some uniformizer. Hence $H \cap U_2 \backslash B_3^\times / U_3 = H \cap U_2 \backslash (B_3^\times / U_3) = \mathcal{O}_{B,3}^\times / U_3$. □

If we denote $\mathbb{Z}_9$ the integer ring for the unramified quadratic extension field of $\mathbb{Q}_3$, then

$$\mathcal{O}_{B,3}^\times = \mathbb{Z}_9^\times (1 + \lambda \mathbb{Z}_9); U_3 = \mathcal{O}_{K,3}^\times (1 + \lambda \mathcal{O}_{B,3}) = \mu_2 (1 + 3\mathbb{Z}_9)(1 + \lambda \mathbb{Z}_9),$$

where $\mu_2 = \{\pm 1\}$. Hence

$$\begin{aligned} H \backslash B_3^\times \mathcal{O}_{B,2}^\times / U_2 U_3 &\xleftarrow{\sim} H \cap U_2 \backslash B_3^\times / U_3 \\ &\xleftarrow{\sim} \mathcal{O}_{B,3}^\times / U_3 \\ &\xleftarrow{\sim} \mathbb{Z}_9^\times / \mu_2 (1 + 3\mathbb{Z}_9) \cong \mathbb{Z}/4\mathbb{Z}, \end{aligned}$$

and we can identify $C^\infty(B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U)$ with $\mathbb{C}[\mathbb{Z}/4\mathbb{Z}]$.

The image of $B^\times\backslash\hat{B}^\times/U$ under the norm map is $\mathbb{Q}_+^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nr}U$. If $p\neq 3$, $\mathrm{Nr}U_p=\mathbb{Z}_p^\times$ while if $\mathrm{Nr}U_3=1+3\mathbb{Z}_3$. Therefore, by the approximation theorem,

$$\mathbb{Q}_+^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nr}U=\mathbb{Z}_3^\times/\mathrm{Nr}U_3=\mathbb{Z}_3^\times/1+3\mathbb{Z}_3.$$

In paticular, the cardinality of $\mathbb{Q}_+^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nr}U$ is 2. Forms in $C^\infty(B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U)$ of the form $\mu\circ\mathrm{Nr}$ for some Hecke character μ corresponds to characters on $\mathbb{C}[\mathbb{Z}/4\mathbb{Z}]$ of order dividing 2. Summing up, we obtain

Lemma 3.4. *There is a natural bijection*

$$\mathbb{Z}_9^\times/\mu_2(1+3\mathbb{Z}_9)\xrightarrow{\sim}B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U$$

which is induced by the embedding $\mathbb{Z}_9^\times\to B_3^\times\to\widehat{B}^\times$, and the left hand side of the above bijection is isomorphic to the cyclic group of order 4. Via this bijection, the space π^U is spanned by characters on the cyclic group with order not dividing 2.

Since $\mathcal{O}_{K,3}^\times\subset U_3$, f is $\chi_\pm$-eigen if and only if $\pi_3(\varpi_3)f=\pm f$, if and only if $f(\zeta^a\varpi_3)=\pm f(\zeta^a)$ for $a=0,\cdots,3$ where ζ is a primitive 8-th root of unity in $\mathbb{Z}_9^\times$. Moreover, we may assume $\zeta\equiv 1+\sqrt{-1}\,(\mathrm{mod}\,1+3\mathbb{Z}_9)$.

To compute $f(\zeta^a\varpi_3)$, since $k\in H\cap U_2$ and $f\in\pi^U$, we have

$$f(\zeta^a\varpi_3)=f(k^{-1}\zeta^a\varpi_3)=f(k_3^{-1}\zeta^a\varpi_3),$$

where k_3 denotes the 3-component of k.

Take $\varpi_3=\sqrt{-3}\in K_3^\times$. Then

$$f(k_3^{-1}\zeta^a\varpi_3)=f(k_3^{-1}\zeta^a k_3)=f(\zeta^{3a}),\quad a\in\mathbb{Z}/4\mathbb{Z},$$

because the conjugate action of k_3 on $\mathbb{Z}_9$ is the Galois conjugation. Thus

$$\pi(\varpi_3)f(\zeta)=f(\zeta^3),\quad \pi(\varpi_3)f(\zeta^a)=f(\zeta^a)\quad\text{if } 2a=0.$$

Thus, one may take f_+ and f_- by

$$\begin{array}{llll} f_+(1)=1, & f_+(\zeta^2)=-1, & f_+(\zeta)=f_+(\zeta^3)=0 & \text{and}\\ f_-(\zeta)=1, & f_-(\zeta^3)=-1, & f_-(1)=f_-(\zeta^2)=0. & \end{array}$$

Finally, we show that χ_0 is the nontrivial element in the residue spectrum of $C^\infty(B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U)$ and $\chi_0(\zeta^a)=(-1)^a$ for $a=0,\cdots,3$. Thus, up to ±1, f_+ (resp. f_-) is the function on $B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U$, supported on those $g\in\widehat{B}^\times$ with $\chi_0(g)=+1$ (resp. $=-1$), valued in $0,\pm1$ with total mass zero. It is clear that f_+ and f_- is an orthonormal basis of π^U. We have completed the proof of Proposition 3.2.

Now let $M=q_1\dots q_r$ with $q_i\equiv 5\,(\mathrm{mod}\,12)$. For any $q|M$, we take an isomorphism $\iota_q: B_q\xrightarrow{\sim}M_2(\mathbb{Q}_q)$ given by $i\mapsto\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ and $k\mapsto\begin{pmatrix}0&3\\1&0\end{pmatrix}$. In particular,$\iota_q(\mathcal{O}_{B,q})=M_2(\mathbb{Z}_q)$. Denote by $x_q\in B_q^\times$ an element such that $\iota_q(x_q)=\begin{pmatrix}q&\\&1\end{pmatrix}$. Then $x_q\mathcal{O}_{B,q}x_q^{-1}\cap K_q=\mathcal{O}_{M,q}$. Take $x_M=\prod_i x_{q_i}\in\widehat{B}^\times$. Denote by

$$f_M=\begin{cases}f_+(\cdot x_M) & \text{if } r \text{ is even;}\\ f_-(\cdot x_M) & \text{if } r \text{ is odd.}\end{cases}$$

Let χ_M be the quadratic Hecke character of K associated to $K(\sqrt{M})/K$; then $\chi_M(\varpi_3) = (-1)^r$. Then f_M is in the line $V(\pi, \chi_M)$ defined in Section 2.4. In particular, it satisfies that

(1) $\forall p \nmid 6M, T_p f_M = a_p f_M$;
(2) f_M is integer-valued with minimal norm;
(3) $\pi(\varpi_3) f_M = \chi_M(\varpi_3) f_M$.

Let H_M be the ring class field of K of conductor M, i.e., the abelian extension of K with Galois group $\mathrm{Gal}(H_M/K) \simeq \mathrm{Pic}(\mathcal{O}_M) = \widehat{K}^\times / K^\times \widehat{\mathcal{O}}_M^\times$. The embedding $K \hookrightarrow B$ induces a map

$$K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_M^\times \longrightarrow B^\times \backslash \widehat{B}^\times / U.$$

Consider

$$P_{\chi_M}(f_M) = \sum_{t \in \mathrm{Pic}(\mathcal{O}_M)} f_M(t) \chi_M(t).$$

Denote by

$$L^{\mathrm{alg}}(s, E) = L(s, E)/\Omega(E),$$

where for any elliptic curve A over $\mathbb{Q}$, $\Omega(A)$ is the real period for the Neron differential of A; and for simplicity, we let $\Omega = \Omega(E)$; then the imaginary period of E is $\Omega^- = \Omega/\sqrt{-3}$.

Proposition 3.5. *Up to* ± 1, $L^{\mathrm{alg}}(1, E^{(M)}) = 2^{-1} P_{\chi_M}(f_M)$.

Proof. By Theorem 2.16,

$$L(1, E, \chi_M) = 2^{-1} \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(36)}}{\sqrt{3} M} \frac{|P_{\chi_M}(f_M)|^2}{\langle f_M, f_M \rangle}.$$

Here,

$$\langle f_M, f_M \rangle = \frac{||f_M||^2}{2} \mathrm{Vol}(X_U)$$

and $\mathrm{Vol}(X_U)$ is the mass of U. By [3, Lemma 2.2],

$$\mathrm{Vol}(X_U) = 2(4\pi^2)^{-1} \mathrm{Vol}(U)^{-1},$$

where $\mathrm{Vol}(U)$ is with respect to Tamagawa measures so that for any finite $p \neq 3$, $\mathrm{Vol}(\mathrm{GL}_2(\mathbb{Z}_p)) = L(2, 1_p)^{-1}$, $\mathrm{Vol}(\mathcal{O}_{B,3}^\times) = 2^{-1} L(2, 1_3)^{-1}$. Therefore $\mathrm{Vol}(X_U) = 4/3$, and $\langle f_M, f_M \rangle = 2/3$. On the other hand,

$$8\pi^2 (\phi, \phi)_{\Gamma_0(36)} = 8\pi^2 \int_{\Gamma_0(36) \backslash \mathcal{H}} |\phi(x + iy)|^2 dx dy = i \Omega \Omega^-.$$

As $E^{(M)}$ and $E^{(-3M)}$ are isogenous over $\mathbb{Q}$, $L(s, E, \chi_M) = L(s, E^{(M)}) L(s, E^{(-3M)})$ $= L(s, E^{(M)})^2$. Denote by $\Omega^{(M)}$ the real period for $E^{(M)}$; then $\Omega^{(M)} = \Omega/\sqrt{M}$. Thus, $L^{\mathrm{alg}}(1, E^{(M)})^2 = (L(1, E^{(M)})/\Omega^{(M)})^2 = M L(1, E, \chi_M)/\Omega^2$ and

$$L^{\mathrm{alg}}(1, E^{(M)})^2 = 2^{-2} |P_{\chi_M}(f_M)|^2.$$

□

3.2. **Rank zero twists.** Keep the notation from the last section. Denote by $\mathscr{A} = \mathrm{Gal}(H_M/K)$; then $2\mathscr{A} = \mathrm{Gal}(H_M/H_M^0)$, where $H_M^0 = K(\sqrt{q} : q \mid M)$. Let $\widehat{\mathscr{A}}$ (resp. $\widehat{\mathscr{A}/2\mathscr{A}}$) be a group of characters on $\mathscr{A}$ (resp. on $\mathscr{A}$ which factors through $2\mathscr{A}$). Then

$$\sum_{\chi \in \widehat{\mathscr{A}/2\mathscr{A}}} P_\chi(f_M) = 2^r y_0, \text{ where } y_0 := \sum_{\sigma \in 2\mathscr{A}} f_M(\sigma).$$

Note that each $\chi \in \widehat{\mathscr{A}/2\mathscr{A}}$ corresponds to an integer $d|M$, in the sense that χ corresponds to the extension $K(\sqrt{d})/K$.

Proposition 3.6. *If $\chi \in \widehat{\mathscr{A}/2\mathscr{A}}$ corresponds to an integer $d \neq M$, then $P_\chi(f_M) = 0$.*

Proof. Choose a prime $q \in \mathbb{N}_S$ such that $qd|M$. Then

$$\begin{aligned} P_\chi(f_M) &= \sum_{\sigma \in \mathscr{A}} f_M(\sigma)\chi(\sigma) \\ &= \sum_{\sigma \in \mathrm{Gal}(H_{M/q}/K)} \sum_{\tau \in \mathrm{Gal}(H_M/H_{M/q})} f_M(\sigma\tau)\chi(\sigma\tau) \\ &= \sum_{\sigma \in \mathrm{Gal}(H_{M/q}/K)} \chi(\sigma) \sum_{\tau \in \mathrm{Gal}(H_M/H_{M/q})} f(\sigma\tau x_M). \end{aligned}$$

By Theorem 2.18, we have

$$u_{M/q} \sum_{\tau \in \mathrm{Gal}(H_M/H_{M/q})} f(\sigma\tau x_M) = a_q f(\sigma x_{M/q}) = 0.$$

So the proposition holds. □

By Proposition 3.6, we have the equality

$$P_{\chi_M}(f_M) = 2^r y_0.$$

Lemma 3.7. *The values of $f_M|_{\widehat{B}^{\times 2}}$ are odd. In particular, y_0 is odd and*

$$v_2(P_{\chi_M}(f_M)) = r.$$

Proof. By the definition of f_M, $f_M|_{\widehat{B}^{\times 2}}$ is odd if and only if for any $g \in \widehat{B}^{\times 2}$, $\chi_0(gx_M) = (-1)^r$. Since χ_0 is quadratic, $\chi_0(g) = 1$. Then $\chi_0(gx_M) = \chi_0(x_M) = \prod_{i=1}^r \chi_0(x_{q_i}) = (-1)^r$ as q_i is inert in K. Hence

$$y_0 \equiv [H_M : H_M^0] \equiv \frac{1}{3} \prod_{q|M} \frac{q+1}{2} \equiv 1 \,(\mathrm{mod}\, 2).$$

□

The Proof of Theorem 1.3. By Proposition 3.5, $v_2(L^{\mathrm{alg}}(1, E^{(M)})) = r - 1$. The 2-part of BSD is equivalent to

$$v_2\left(L^{\mathrm{alg}}\left(1, E^{(M)}\right)\right) = \sum_{p|6M} v_2\left(c_p\left(E^{(M)}\right)\right) - 2v_2\left(\#E^{(M)}_{\mathrm{tor}}\right) + v_2\left(\#Ш\left(E^{(M)}/\mathbb{Q}\right)\right).$$

The Tamagawa numbers of $E^{(M)}$ are: $c_2(E^{(M)}) = 3$ (resp. $= 1$) if $M \equiv 1 \,(\mathrm{mod}\, 8)$ (resp. otherwise), $c_3(E^{(M)}) = 2$ and $c_q(E^{(M)}) = 2$ for $q|M$. On the other hand, $E^{(M)}(\mathbb{Q}) = E^{(M)}(\mathbb{Q})_{\mathrm{tor}} = \mathbb{Z}/2\mathbb{Z}$. Finally, using classical 2-descent, $Ш(E^{(M)}/\mathbb{Q})[2] = 0$. Combining the results above, it is clear that the 2-part of BSD conjecture holds.

By [15, Theorem 11.1], the p-part of the BSD-conjecture for $E^{(M)}$ holds for $p \nmid 6$, therefore the first part of Theorem 1.3 holds. □

3.3. **The Gross-Zagier formula.** Let $K = \mathbb{Q}(\sqrt{-\ell})$ with $\ell \equiv 11 \pmod{12}$. Let $N = 36$. Write $N = N_0 N_1^2$ as before. There are two cases:

(1) if $\ell \equiv -1 \pmod{24}$, then the Heegner hypothesis holds and $N = N_0 = 36$;
(2) if $\ell \equiv 11 \pmod{24}$, then $N_0 = 9$.

Embed K into $M_2(\mathbb{Q})$ as i_c with $c = 1$ in Example 2.1. Precisely, take an odd integer a with $4 \cdot N_0 | (\ell + a^2)$ and embed K into $M_2(\mathbb{Q})$ by

$$\sqrt{-\ell} \mapsto \begin{pmatrix} a & 2 \\ -\frac{\ell + a^2}{2} & -a \end{pmatrix}.$$

Then $M_2(\mathbb{Z}) \cap K = R_0(N_0) \cap K = \mathcal{O}_K$. Under such embedding, take $R = \mathcal{O}_K + N_1 R_0(N_0)$ and consider the modular curve $X_K(N)$. For the first case, $X_K(N) = X_0(36)$. For the second case, the modular curve $X_K(N)$ has genus one and by Lemma 2.11, the cusp $[\infty]$ is defined over $\mathbb{Q}$. In fact, by [6, Example 11.7.c], $A := (X_K(N), [\infty])$ is the elliptic curve

$$y^2 = x^3 - 27 \quad (36\mathrm{C})$$

which is 3-isogenous to E. We have $A(\mathbb{Q}) = A(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. For the first case (resp. the second case), take f to be the identity morphism on E (resp. on A). Denote by

$$j = \begin{pmatrix} 1 & 0 \\ -a & -1 \end{pmatrix} \in K^-.$$

Lemma 3.8. *Take $w \in \mathrm{GL}_2(\widehat{\mathbb{Q}})$ the Atkin-Lehner operator defined in Section 2.1. More precisely, for the Heegner hypothesis case, $w = j^{(36)} w_2 w_3$ while for the second case, $w = j^{(3)} w_3$. Then w normalizes $\widehat{R}^\times$ and $w = t_0 j u$ for some $t_0 \in \widehat{K}^\times$ and $u \in \widehat{R}^\times$. Moreover, $f + f^w$ is a constant map and its image is not in $2E(\mathbb{Q})$ for the Heegner hypothesis case or not in $2A(\mathbb{Q}) = \{O\}$ for the other case.*

Proof. By Lemma 2.12, it suffices to prove the "Moreover" part.

For the first case, denote by $\mathrm{Hom}_{[\infty]}(X_0(N), E)$ the space of $\mathbb{Q}$-morphisms from $X_0(N)$ to E taking $[\infty]$ to O and $\mathrm{Hom}^0_{[\infty]}(X_0(N), E) = \mathrm{Hom}_{[\infty]}(X_0(N), E) \otimes_{\mathbb{Z}} \mathbb{Q}$. By Atkin-Lehner theory, $f^w = -f$ in $\mathrm{Hom}^0_{[\infty]}(X_0(N), E)$. So $f^w + f$ is a constant map. However, $f([\infty]) = O$, $f^w([\infty]) = f([0]) = [0]$, while $[0]$ is the generator of $E(\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$. Thus, the image of $f + f^w$ is not in $2E(\mathbb{Q})$.

For the second case, view $f \in \mathrm{Hom}^0_{[\infty]}(X_K(N), A)$. Then $f^{w_3} = \epsilon(A/\mathbb{Q}_3) f = f$. As f and f^{j_2} are both $K_2^\times$-invariant and such elements in $\mathrm{Hom}^0_{[\infty]}(X_K(N), A)$ form a $\mathbb{Q}$-vector space of dimension 1, there is a sign $\epsilon \in \{\pm 1\}$ such that $f^{j_2} = \epsilon_2 f$. By [11, Theorem 4], the sign $\epsilon_2 = +1$ if and only if $\epsilon(A/\mathbb{Q}_2) = \epsilon(A^{(-\ell)}/\mathbb{Q}_2) = 1$. Since $\epsilon(A/\mathbb{Q}_2) = -1$, we obtain $f^{j_2} = -f$. Thus $f^w = -f$ and, as a morphism from $X_K(N)$ to A, $f + f^w = T$ for some torsion point $T \in A(\mathbb{Q})$. To see $T \neq O$, it suffices to show $[\infty] \neq [\infty]^w$. This is equivalent to saying that $w \notin P(\mathbb{Q})\widehat{R}^\times$ with P the upper-triangular matrices in GL_2. This holds since $w_3 \notin P(\mathbb{Q}_3) R_3^\times$. In fact, $P(\mathbb{Q}_3) w_3 \subset \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} : bc \in \mathbb{Q}_3^\times \right\}$, while $R_3^\times = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_3) : 9 | c \right\}$. □

Write $\mathrm{Isom}_{\mathbb{Q}}(A)$ for the group of algebraic isomorphisms of A over $\mathbb{Q}$ and $\mathrm{Aut}_{\mathbb{Q}}(A)$ the subrgroup of algebraic isomorphisms over $\mathbb{Q}$ which fix O. Then $\mathrm{Aut}_{\mathbb{Q}}(A) = \mathbb{Z}/2\mathbb{Z}$ is generated by multiplication -1 and $\mathrm{Isom}_{\mathbb{Q}}(A) = \langle t_T \rangle \times \mathrm{Aut}_{\mathbb{Q}}(A)$ where $t_T : P \mapsto P + T$ the translation on A by T.

Lemma 3.9. *For any $P \in A$, $P^{w_3} = t_T(P)$ and $P^{j^{(3)}} = -P$.*

Proof. In the above proof, we have seen that $w_3 \notin PU_3$. Thus $[\infty]^{w_3} \neq [\infty]$. Hence for any point P, $P^{w_3} = t_T(P)$. On the other hand, $P^w = t_T(-P)$. Therefore, $P^{j^{(3)}} = (P^w)^{w_3^{-1}} = -P$. □

Let $M = \prod_i q_i$ where q_i are distinct positive integers $\equiv 5 \pmod{12}$. Denoted by χ_M the quadratic character of K is associated to the extension $K(\sqrt{M})/K$. Let $P_M \in X_K(N)(H_M)$ be the Heegner point defined in Subsection 2.3. Consider

$$P_{\chi_M}(f) = \sum_{\sigma \in \mathrm{Gal}(H_M/K)} f(P_M)^{\sigma} \chi_M(\sigma) \in E(K).$$

Proposition 3.10. *Up to ± 1,*

$$L^{\mathrm{alg}}(1, E^{(M)}) \frac{L^{'}(1, E^{(-\ell M)})}{\Omega(E^{(-\ell M)})} = \widehat{h}_K(P_{\chi_M}(f)).$$

Proof. By Theorem 2.14,

$$L'(1, E, \chi_M) = \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(36)}}{\sqrt{\ell} M} \cdot \widehat{h}_K(P_{\chi_M}(f)).$$

Since $L(s, E, \chi_M) = L(s, E^{(M)}) L(s, E^{(-\ell M)})$, and we have proved that $L(s, E^{(M)})$ is nonvanishing at $s = 1$,

$$L'(1, E, \chi_M) = L(1, E^{(M)}) L'(1, E^{(-\ell M)}).$$

As in in the proof of Proposition 3.5

$$8\pi^2 (\phi, \phi)_{\Gamma_0(36)} = 8\pi^2 \int_{\Gamma_0(36) \backslash \mathcal{H}} |\phi(x + iy)|^2 dx dy = i \Omega \Omega^{-}.$$

By [25], we know $\Omega(E^{(M)}) = \Omega / \sqrt{M}$ and up to sign $\Omega(E^{(-\ell M)}) = \Omega^{-} / \sqrt{-\ell M}$, so up to sign

$$\Omega(E^{(M)}) \Omega(E^{(-\ell M)}) = \frac{\Omega}{\sqrt{M}} \frac{\Omega^{-}}{\sqrt{-\ell M}} = -\frac{8\pi^2 (\phi, \phi)_{\Gamma_0(36)}}{M \sqrt{\ell}};$$

thus up to sign:

$$L^{\mathrm{alg}}(1, E^{(M)}) \frac{L^{'}(1, E^{(-\ell M)})}{\Omega(E^{(-\ell M)})} = \widehat{h}_K(P_{\chi_M}(f)).$$

□

3.4. **Rank one twists.** Let ℓ be a prime with $\ell \equiv 11 \pmod{12}$. Denote by $K = \mathbb{Q}(\sqrt{-\ell})$. We only prove Theorem 1.2 in the case $\ell \equiv 11 \pmod{24}$, that is, 2 is inert in K and 3 is split in K, while its proof for the other case is similar.

Let $M = q_1 \cdots q_r$ where q_i are distinct primes such that $q_i \equiv 5 \pmod{12}$ and inert in K. Denote by $\mathscr{A} = \mathrm{Gal}(H_M/K)$. Then $2\mathscr{A} = \mathrm{Gal}(H_M/H_M^0)$, where $H_M^0 = K(\sqrt{q} : q \mid M)$. Let $\widehat{\mathscr{A}}$ (resp. $\widehat{\mathscr{A}/2\mathscr{A}}$) be the group of characters on $\mathscr{A}$ (resp. on $\mathscr{A}$ which factors through $\mathrm{Gal}(H_M^0/K)$).

Let A be the elliptic curve $y^2 = x^3 - 27$. Observe that $A(H_M^0)[2^\infty] = A(\mathbb{Q})[2^\infty] = A(\mathbb{Q})[2]$. In fact, suppose $Q \in A(H_M^0)[2^\infty]$ but $Q \notin A(\mathbb{Q})[2^\infty]$. Then the extension $\mathbb{Q}(Q)/\mathbb{Q}$ is unramified outside 2 and 3. However, as $\mathbb{Q}(Q) \subset H_M^0$, $\mathbb{Q}(Q)/\mathbb{Q}$ must be ramified at ℓ or q_i for some i. It's a contradiction. Let T be the nontrivial element in $A(\mathbb{Q})[2]$, and let $C = \#A(H_M^0)_{\mathrm{tor}}/2$ be the cardinality of the odd part of $A(H_M^0)_{\mathrm{tor}}$. Denote by

$$y_M = P_{\chi_M}(f) = \sum_{\sigma \in \mathscr{A}} f(P_M)^\sigma \chi_M(\sigma) \in A(H_M^0).$$

Similar to Proposition 3.6, we have

$$y_M = 2^r y_0, \text{ where } y_0 := \sum_{\sigma \in 2\mathscr{A}} f(P_M)^\sigma,$$

as an equality of divisors in $A(H_M^0)$. The key point is the following lemma:

Lemma 3.11.

$$\overline{y}_0 + y_0 = T.$$

Proof. By Lemma 2.12, one can write $w = t_0 j u$ with $t_0 \in \widehat{K}^\times$, $j = K^-$ and $u \in \widehat{R}^\times$. Take $x_M \in \widehat{B}^\times$ as before such that $P_M = [h_0, x_M] \in X_K(N)(H_M)$ with $h_0 \in \mathscr{H}^{K^\times}$. Thus, for any $\sigma_t \in 2\mathscr{A}$ with $t \in \widehat{K}^\times$

$$f^w(P_M)^{\sigma_t} = f([h_0, t x_M t_0 j]).$$

Note that $x_M \in \mathrm{GL}_2(\mathbb{Q}^{(N)})$ while $t_0 \in K_{(N)}^\times \subset \mathrm{GL}_2(\mathbb{Q}_{(N)})$. Hence $x_M t_0 = t_0 x_M$ and

$$f^w(P_M)^{\sigma_t} = f([h_0, x_M j])^{\sigma_{t t_0}}.$$

Finally, we need to show that $x_M j \in j x_M U$. This reduces to show that for any $q|M$, the q-part of $x_M^{-1} j^{-1} x_M j$ belongs to $R_q^\times = \mathrm{GL}_2(\mathbb{Z}_q)$. It is easy to check this holds. Thus

$$f^w(P_M)^{\sigma_t} = f([h_0, j x_M])^{\sigma_{t t_0}} = \overline{f([h_0, x_M])}^{\sigma_{t t_0}}.$$

On the other hand, note that in the proof of Lemma 2.12, $t_{0,p} = 1$ for any $p \nmid N_0 = 9$. Denote by $a_0 = N_{K/\mathbb{Q}}(t_0) \in \widehat{\mathbb{Q}}^\times$. Taking determinant for the equation $w = j t_0 u$, we get $a_{0,p} = 1$ if $p \neq 3$ and $a_{0,3} \in 9\mathbb{Z}_3^\times$. Thus for any prime $q|M$

$$\sigma_{t_0}(\sqrt{q}) = \sigma_{a_0}(\sqrt{q}) = \sqrt{q},$$

where $\sigma_{a_0} \in \mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$ via the Artin map over $\mathbb{Q}$. Hence, $\sigma_{t_0} \in 2\mathcal{A}$.

Summing up, since $[H_M : H_M^0] = [H : K] \prod_{q|M} \dfrac{q+1}{2}$ is odd, we get

$$\overline{y}_0 + y_0 = \sum_{\sigma \in 2\mathscr{A}} (f + f^w)(P_M)^\sigma = [H_M : H_M^0] T = T.$$

□

Theorem 3.12. *$y_M \in A(K(\sqrt{M}))^-$ and the 2-index of y_M is $r-1$ in $A(K(\sqrt{M}))$.*

Proof. Consider the maps

$$\begin{array}{ccccccc} & & & & A(K(\sqrt{M}))/2^r A(K(\sqrt{M})) & & \\ & & & & \downarrow{\scriptstyle \delta} & & \\ 0 & \longrightarrow & H^1(H_M^0/K(\sqrt{M}), A[2^r](H_M^0)) & \longrightarrow & H^1(K(\sqrt{M}), A[2^r]) & \longrightarrow & H^1(H_M^0, A[2^r]) \end{array}$$

where δ is the Kummer map, which is injective, and the horizontal line is the inflation-restriction exact sequence. Since $y_M = 2^r y_0$ with $y_0 \in A(H_M^0)$, the image of $\delta(y_M)$ is 0 in $H^1(H_M^0, A[2^r])$, hence we see that $\delta(y_M)$ lies in the image of $H^1(H_M^0/K(\sqrt{M}), A[2^r](H_M^0))$, which is killed by 2. It follows that $2y_M \in 2^r A(K(\sqrt{M}))$; then

$$y_M = 2^{r-1}z + t, z = 2y_0 + s$$

for some $z \in A(K(\sqrt{M}))$ and $s, t \in A(\mathbb{Q})[2]$.

Let $\sigma \in \mathrm{Gal}(K(\sqrt{M})/K)$ be the nontrivial element. Then by definition, we have $y_M + y_M^\sigma = 0$, so $y_0 + y_0^\sigma \in A(H_M^0)[2^r] = A(\mathbb{Q})[2]$, so $z + z^\sigma = 0$. On the other hand

$$z + \overline{z} = 2(y_0 + \overline{y}_0) = 0,$$

which implies $z \in A(\mathbb{Q}(\sqrt{-\ell M}))^- = A^{(-\ell M)}(\mathbb{Q})$. Therefore

$$y_M \in 2^{r-1}A(\mathbb{Q}(\sqrt{-\ell M}))^- + A(\mathbb{Q})[2].$$

We will show that the 2-index of y_M is exactly $r-1$. Suppose that $y_M = 2^r z + t$ for some $z \in A(\mathbb{Q}(\sqrt{-\ell M}))^-$ and $t \in A(\mathbb{Q}(\sqrt{-\ell M}))_{\mathrm{tor}}$. Then $2^r(z - y_0) + t = 0$, which implies $C(z - y_0) \in A(\mathbb{Q})[2]$. Hence $C(z - y_0) + C(\overline{z} - \overline{y}_0) = 0$. But we have $z + \overline{z} = 0$, so $C(y_0 + \overline{y}_0) = 0$. But this contradicts the fact that $\overline{y}_0 + y_0 = T \neq 0$. □

The Proof of Theorem 1.2. Observe that A and E are 3-isogenuous, so to prove Theorem 1.2, we only need to prove that it holds for A.

By Proposition 3.10, up to ± 1,

$$L^{\mathrm{alg}}(1, A^{(M)}) \frac{L'(1, A^{(-\ell M)})}{\Omega(A^{(-\ell M)})} = \widehat{h}_K(y_M).$$

Denote by $R(-\ell M) = \widehat{h}(P_{-\ell M})$ where $P_{-\ell M}$ is the generator of $A^{(-\ell M)}(\mathbb{Q})/A^{(-\ell M)}(\mathbb{Q})_{\mathrm{tor}}$. In particular, by Theorem 3.12

$$\widehat{h}_K(y_M) = 2^{2(r-1)} R(-\ell M).$$

Thus, if we denote by

$$L'^{\mathrm{alg}}(s, A^{(-\ell M)}) = \frac{L'(s, A^{(-\ell M)})}{R(-\ell M)\Omega(A^{(-\ell M)})},$$

then by the result of the rank zero case, we have

$$v_2(L'^{\mathrm{alg}}(1, A^{(-\ell M)})) = r.$$

The Tamagawa numbers of $A^{(-\ell M)}$ are: $c_2(A^{(-\ell M)}) = 1$ or 3, $c_3(A^{(-\ell M)}) = 2$ and $c_q(A^{(-\ell M)}) = 2$ for $q | \ell M$. On the other hand, $A^{(-\ell M)}(\mathbb{Q}) = A^{(-\ell M)}(\mathbb{Q})_{\mathrm{tor}} = \mathbb{Z}/2\mathbb{Z}$. Finally, using classical 2-descent, $Ш(A^{(-\ell M)}/\mathbb{Q})[2] = 0$. Combining the results above, it is clear that the 2-part of BSD conjecture for $A^{(-\ell M)}$ holds.

Since $A^{(-\ell M)}$ has CM, the p-adic height pairing on $A^{(-\ell M)}(\overline{\mathbb{Q}})$ is nondegenerate. Then by [12, Corollary 1.9], p-part of the BSD conjecture for $A^{(-\ell M)}$ holds for $p \nmid 6\ell M$. So the second part of Theorem 1.2 holds for A, and hence for E. □

Acknowledgment

The authors greatly thank Professor Ye Tian for suggesting this problem and his persistent encouragement.

References

[1] Massimo Bertolini and Henri Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*, Invent. Math. **131** (1998), no. 3, 453–491, DOI 10.1007/s002220050211. MR1614543

[2] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618, DOI 10.1007/BF01233440. MR1074487

[3] Li Cai, Jie Shu, and Ye Tian, *Explicit Gross-Zagier and Waldspurger formulae*, Algebra Number Theory **8** (2014), no. 10, 2523–2572, DOI 10.2140/ant.2014.8.2523. MR3298547

[4] John Coates, Yongxiong Li, Ye Tian, and Shuai Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. (3) **110** (2015), no. 2, 357–394, DOI 10.1112/plms/pdu059. MR3335282

[5] Solomon Friedberg and Jeffrey Hoffstein, *Nonvanishing theorems for automorphic L-functions on* GL(2), Ann. of Math. (2) **142** (1995), no. 2, 385–423, DOI 10.2307/2118638. MR1343325

[6] Benedict H. Gross, *Local orders, root numbers, and modular curves*, Amer. J. Math. **110** (1988), no. 6, 1153–1182, DOI 10.2307/2374689. MR970123

[7] Benedict H. Gross, *Heegner points on* $X_0(N)$, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105. MR803364

[8] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, DOI 10.1007/BF01388809. MR833192

[9] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569

[10] Jan Nekovář, *The Euler system method for CM points on Shimura curves*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 471–547, DOI 10.1017/CBO9780511721267.014. MR2392363

[11] Dipendra Prasad, *Some applications of seesaw duality to branching laws*, Math. Ann. **304** (1996), no. 1, 1–20, DOI 10.1007/BF01446282. MR1367880

[12] Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques* (French), Invent. Math. **89** (1987), no. 3, 455–510, DOI 10.1007/BF01388982. MR903381

[13] H. Qin, *Representation of integers by positive ternary quadratic forms*, preprint, 2015.

[14] M. Ram Murty and V. Kumar Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475, DOI 10.2307/2944316. MR1109350

[15] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68, DOI 10.1007/BF01239508. MR1079839

[16] A. J. Scholl, *On modular units*, Math. Ann. **285** (1989), no. 3, 503–510, DOI 10.1007/BF01455070. MR1019715

[17] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. MR1757192

[18] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. MR1291394

[19] Jerrold B. Tunnell, *Local* ϵ*-factors and characters of* GL(2), Amer. J. Math. **105** (1983), no. 6, 1277–1307, DOI 10.2307/2374441. MR721997

[20] Ye Tian, *Euler systems of CM points on Shimura curves*, ProQuest LLC, Ann Arbor, MI, 2003. Thesis (Ph.D.)–Columbia University. MR2704579

[21] Ye Tian, *Congruent numbers and Heegner points*, Camb. J. Math. **2** (2014), no. 1, 117–161, DOI 10.4310/CJM.2014.v2.n1.a4. MR3272014

[22] Ye Tian, *Congruent numbers with many prime factors*, Proc. Natl. Acad. Sci. USA **109** (2012), no. 52, 21256–21258, DOI 10.1073/pnas.1216991109. MR3023667

[23] Y. Tian, X. Yuan, and S. Zhang, *Genus Periods, Genus Points and Congruent Number Problem*, preprint, 2015.

[24] Marie-France Vignéras, *Arithmétique des algèbres de quaternions* (French), Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980. MR580949

[25] Vivek Pal, *Periods of quadratic twists of elliptic curves*, Proc. Amer. Math. Soc. **140** (2012), no. 5, 1513–1525, DOI 10.1090/S0002-9939-2011-11014-1. With an appendix by Amod Agashe. MR2869136

[26] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier* (French), J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484. MR646366

[27] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang, *The Gross-Zagier formula on Shimura curves*, Annals of Mathematics Studies, vol. 184, Princeton University Press, Princeton, NJ, 2013. MR3237437

Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, People's Republic of China

Email address: lcai@math.tsinghua.edu.cn

Academy of Mathematics and Systems Science, Morningside center of Mathematics, Chinese Academy of Sciences, Beijing 100190, People's Republic of China

Email address: yihuachenamss@163.com

Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, People's Republic of China

Email address: yliu@math.tsinghua.edu.cn