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 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

2. The Modular Curve and Heegner points

3. Quadratic Twists of $X_0(36)$

3.1. The Waldspurger Formula

3.2. Rank Zero Twists

3.3. The Gross-Zagier Formula

3.4. Rank One Twists

References

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 $\chi$ a (primitive) ring class character over $K$ of conductor $c$, i.e. a character of $\text{Pic}(\mathcal{O}_c)$, 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 $\phi$ and $\chi$. Assume the Heegner condition:

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

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 $\text{Pic}(\mathcal{O}_c)$ by class field theory. Such points are called Heegner points over $K$ of conductor $c$ and only depends on the class of $\mathfrak{a}$ in $\text{Pic}(\mathcal{O}_c)$.

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

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

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

Let the data $(\phi, K, \chi)$ be as above, and generalize the Heegner condition to the following one ($\star$):

Li Cai was supported by the Special Financial Grant from the China Postdoctoral Science Foundation 2014T70067.
(i) \((c, N) = 1\).
(ii) if prime \(p|N\) is inert in \(K\), then \(\text{ord}_p N\) is even; if \(p|N\) is ramified in \(K\), then \(\text{ord}_p N = 1\) and \(\chi(p) \neq a_p\), where \(p\) is the unique prime ideal of \(\mathcal{O}_K\) above \(p\) and \([p]\) is its class in \(\text{Pic} (\mathcal{O}_K)\).

By this assumption, 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 \(K \cap M_2(\mathbb{Q}) = K \cap R_0(N_0) = \mathcal{O}_c\), where

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

Then \(R = \mathcal{O}_c + N_1 R_0(N_0)\) is an order of \(M_2(\mathbb{Z})\). Define

\[ \Gamma_K (N) = R^\times \cap \text{SL}_2(\mathbb{Z}) = \left\{ A \in \text{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N_0} \right\}. \]

The modular curve now we have to consider is \(X_K(N) = \Gamma_K(N) \backslash \mathcal{H} \cup \{\text{cusps}\}\).

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

\[ H = (\mathcal{O}_K/\mathcal{N}_1 \mathcal{O}_K)^\times \subset \text{GL}_2(\mathbb{Z}/N_1 \mathbb{Z}). \]

The readers are referred to [9]. Let \(h_0\) be the fixed point of \(\mathcal{H}\) under the action of \(K^\times\). Note that \(\mathbb{Z} + \mathbb{Z} h_0^{-1}\) is an invertible ideal of \(\mathcal{O}_c\), then the triple \(P = \left( \mathbb{C}/\mathbb{Z} + \mathbb{Z} h_0, (\alpha, 1), H \left( \begin{pmatrix} a & \beta \\ \gamma & \delta \end{pmatrix} \right) \right)\) is a Heegner point on \(X_K(N)\). By CM theory, \(P \in X_K(N)(K^{ab})\). The conductor of \(P\) is also defined to be \(c\), the conductor of \(\mathcal{O}_c\). For details, see Section 2.

Assume \(\phi\) corresponds to an elliptic curve \(E/\mathbb{Q}\), then 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 \((*)\)

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

(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 \((N, D)\), \(u = [\mathcal{O}_c^\times : \{\pm 1\}]\).

In another way, following the idea of Kolyvagin, these Heegner points form an “Euler system”. There is a norm compatible relation between Heegner points of different conductors. See Theorem 2.13.

As an application of such kind of parametrization, we will construct a family of quadratic twists of an elliptic curve with Mordell-Weil groups being rank one. The action of complex conjugation on the CM-points of modular curve is a crucial point in the proof of the nontriviality of the Heegner point. For usual modular curve \(X_0(N)\), the complex conjugation is essentially the Atkin-Lehner operator. However, it does not keep for the modular curve \(X_K(N)\). We find the correct one, namely, the combination of local Atkin-Lehner operators? and the nontrivial normalizer of \(K^\times\) in \(\text{GL}_2(\mathbb{Q})\). 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 deduces the 2-part of the BSD conjecture for our family of quadratic twists.

For each square free non-zero 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] shows 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 \(\text{ord}_d L(E^{(d)}, s) = 1\). The work of [3] deals with the elliptic curve \(E = (X_0(49), \{\infty\})\) which has CM by \(\sqrt{-7}\), gets the similar results to [21].

Here, we construct a family of quadratic twists of \(E = (X_0(36), \{\infty\})\) such that the ranks of Mordell-Weil groups for this twists are one.
Theorem 1.2. Let $\ell$ 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 $\mathbb{Q}(\sqrt{-3})$, $q_i \equiv 1 \pmod{4}$ and $q_i$ inert in $\mathbb{Q}(\sqrt{-\ell})$. Then

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

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

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

However, the proof of the 2-part of the BSD conjecture for $E^{(M)}$ needs that for $E^{(1)}$.

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

If the data $(\phi, K, \chi)$ satisfies that the root number $\epsilon(\phi, \chi) = +1$, 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 $f : B^{\times} \backslash B^{\times}/R^{\times} \to \mathbb{C}$. Assume the conductor $c$ of $\chi$ satisfies $(c, N) = 1$. Let $x_c \in K^{\times} \backslash B^{\times}/R^{\times}$ be a Gross point of conductor $c$, that is $x_c R x_c^{-1} \cap K = \mathcal{O}_c$. Denote by

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

Then with similar notations as for Gross-Zagier formula, we have the Waldspurger formula (See Theorem 2.14)

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

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

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

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 $N = N_0 N_1$ 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

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

Denote by $R = \mathcal{O}_c + N_1 R_0(\mathbb{N})$ an order of $M_2(\mathbb{Q})$. Then $R$ has discriminant $N$ with $R \cap K = \mathcal{O}_c$.

Let $\Gamma_K(N) = \Gamma \cap \text{SL}_2(\mathbb{Z})$ 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 $E, (Z/(N_0 N_1)^2 \cong E[N_0 N_1])$ where $E$ is an elliptic curve over $\mathbb{C}$. By [9], it parameterizes $E, (Z/N_0)^2 \cong E[N_0], (Z/N_1)^2 \cong E[N_1])$. Then $X_K(N)$ parameterizes $(E, C, \alpha : (Z/N_1)^2 \cong E[N_1])$, where $C$ is a cyclic subgroup of $E[N_0]$ of order $N_0$, and $\alpha$ is an $H$-orbit of a basis of $E[N_1]$ where $H := (\mathcal{O}_K/N_1 \mathcal{O}_K)^\times \subset \text{GL}_2(Z/N_1 \mathbb{Z})$. Precisely, the class of $z \in \mathcal{H}$ in $X_K(N)$ corresponds to the triple

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

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

3
Proof. Consider the curve morphism $X_K(N) \to X_0(N_0)$ over $\mathbb{Q}$, which is the forgetful functor in the moduli aspect $(E,C,[\alpha]) \mapsto (E,C)$. $\mathcal{a}, \mathcal{N}$ defines a Heegner point $(\mathbb{C}/\mathcal{a}, \mathcal{N}^{-1} \mathcal{a}/\mathcal{a})$ on $X_0(N_0)$. Then exists a $\mathbb{Z}$-basis $\{u, v\}$ of $\mathcal{a}$ and $g = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{GL}_2(\mathbb{Q})$. $\mathcal{N}^{-1} \mathcal{a} = \mathbb{Z} \left( \begin{array}{c} u \\ N_0 \end{array} \right)$, $\mathcal{v} = g^{-1} h_0$, and $K \cap gR_0(N_0)g^{-1} = \mathcal{O}_c$. Different choice of basis $(u, v)$ make $g$ differ an element in $\Gamma_0(N_0) = R_0(N_0)^\times$ and a scalar. So we have to prove there exists $g' \in \Gamma_0(N_0)$, such that $K \cap gg' R_0(N_0)g'^{-1} = \mathcal{O}_c$.

In fact, we choose $g' \in \Gamma_0(N_0)$, such that $gg' \in \prod_{\ell \mid N_1} K_\ell^\times(1 + N_1 M_2(\mathbb{Z}_\ell))$, embedding $gg'$ into $\bigoplus_{\ell \mid N_1} \text{GL}_2(\mathbb{Q}_\ell)$. Note that if $g^{-1} = \left( \begin{array}{cc} a' & b' \\ c' & d' \end{array} \right)$, and multiply a scalar if necessary, we may assume $g^{-1} \in M_2(\mathbb{Z})$, then $\mathbb{Z}(a'h_0 + b') + \mathbb{Z}(c'h_0 + d)$ and $\mathcal{a}$ belong to a same class in $\text{Pic}(\mathcal{O}_c)$, hence

$$ \det g^{-1} = |\mathcal{O}_c : \mathcal{a}| := \frac{|\mathcal{O}_c : \mathcal{O}_c \cap \mathcal{a}|}{|\mathcal{a} : \mathcal{O}_c \cap \mathcal{a}|}. $$

Therefore there exists an integer $N'_1$ whose prime factors are prime factors of $N_1$, s.t. $\ell \mid \det(N'_1 g^{-1})$, $\forall \ell \mid N_1$. So $N'_1 g^{-1} \in \text{GL}_2(\mathbb{Z}_\ell)$, $\forall \ell \mid N_1$. By strong approximation, $\Gamma_0(N_0) \prod_{\ell \mid N_1} \text{O}_{K,\ell}^\times(1 + N_1 M_2(\mathbb{Z}_\ell)) = \prod_{\ell \mid N_1} \text{GL}_2(\mathbb{Z}_\ell)$, then there exists $g' \in \Gamma_0(N_0), X \in \prod_{\ell \mid N_1} \text{O}_{K,\ell}^\times(1 + N_1 M_2(\mathbb{Z}_\ell))$, such that $g' X = N'_1 g^{-1}$, thus $gg' = N'_1 X \in \prod_{\ell \mid N_1} K_\ell^\times(1 + N_1 M_2(\mathbb{Z}_\ell))$. The proof is completed. 

\begin{definition}
Let $\mathcal{a}, \mathcal{N}$ and $u, v, g$ be as in the above lemma. A Heegner point on $X_K(N)$ of conductor $cm$ is a triple

$$ P = \left( \mathbb{C}/\mathcal{a}, \mathcal{N}^{-1} \mathcal{a}/\mathcal{a}, H \left( \frac{u}{\mathcal{N}_1}, \frac{v}{\mathcal{N}_1} \right) \right). $$

\end{definition}

\begin{remark}
This point corresponds to the point $\frac{v}{u} \in \mathcal{H}$. Let $h_0$ be the point $\mathcal{H}^{K^\times}$. The order $\mathcal{O}_c = \mathbb{Z} + \mathbb{Z} \mathcal{a}$, where $\mathcal{a} = \frac{e^{2(D^2-D)}}{2}$. Denote by $\left( \begin{array}{cc} x & y \\ z & w \end{array} \right) \in \text{GL}_2(\mathbb{Q})$ the image of $\mathcal{a}$ under the fixed embedding $K \hookrightarrow M_2(\mathbb{Q})$. Since $K$ is a field, $z \neq 0$.

\begin{lemma}
$K = \mathbb{Q} + Qh_0$ and $\mathcal{O}_c = \mathbb{Z} + \mathbb{Z} h_0^{-1}$.
\end{lemma}

\begin{proof}
We have $x + w = Dc, xw - yz = \frac{e^2(D^2-D)}{4}$. As $h_0$ is fixed by $\left( \begin{array}{cc} x & y \\ z & w \end{array} \right)$,

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

Hence

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

so

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

\end{proof}

\begin{lemma}
Let $\mathcal{a} = \mathbb{Z} + \mathbb{Z} \cdot h_0^{-1}$ and $\mathcal{N}^{-1} = \mathbb{Z} + \mathbb{Z} \cdot N_0^{-1} h_0^{-1}$. Then $\text{End}(\mathcal{a}) = \{ x \in K : x \mathcal{a} \subset \mathcal{a} \} = \mathcal{O}_c$, and $\text{End}(\mathcal{N}^{-1}) = \mathcal{O}_c$.
\end{lemma}

\begin{proof}
Let $(a + bh_0^{-1}) \mathcal{a} \subset \mathcal{a}$. Then it is equivalent to

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

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

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

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 is exactly $\text{End}(\mathcal{a}) = \mathcal{O}_c$. The assertion for $\mathcal{N}^{-1}$ is the same, noticing that $N_0 z$.

\end{proof}

Clearly, $\mathcal{a}$ and $\mathcal{N}$ are invertible ideals of $\mathcal{O}_c$, and $\mathcal{N}^{-1}/\mathcal{a} \simeq \mathbb{Z}/N_0 \mathbb{Z}$. 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 $a = \mathbb{Z} + \mathbb{Z} \cdot h_0^{-1}$ and $N^{-1} = \mathbb{Z} + \mathbb{Z} \cdot N_0^{-1} h_0^{-1}$, then

$$P = \left( \mathbb{C}/a, N^{-1}/a, H \left( \frac{N_1}{N_1^2} \right) \right)$$

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

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

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

Take trace and norm, we get

$$D = 2n + (m + \overline{m})$$

and

$$\frac{D^2 - D}{4} = n^2 + n(m + \overline{m}) + mm\overline{m}.$$

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

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

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

$$\frac{D+\sqrt{D}}{2} \xrightarrow{(\frac{D+a}{N_0bc} \quad -e^{-1}} \quad \frac{Dc+\sqrt{Dc^2}}{2} \xrightarrow{(\frac{Dc+ac}{N_0bc^2} \quad -1}} \frac{D-a}{2}.$$

We can see this embedding is normal in the sense of [18], and $h_0 = \frac{a + \sqrt{D}}{2N_0bc}$.

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, $H = i(\mathcal{O}_K/N_1 \mathcal{O}_K) \subset \text{GL}_2(\mathbb{Z}/N_1 \mathbb{Z})$, and $H_0$ be the upper-triangular matrices in $\text{GL}_2(\mathbb{Z}/N_0 \mathbb{Z})$, then $H = \prod_{p|N_1} H_p$, where $H_p \subset \text{GL}_2(\mathbb{Z}/p^{\text{ord}_pN_1} \mathbb{Z})$. 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 $\text{GL}_2(\mathbb{Z}/p^{\text{ord}_pN_1} \mathbb{Z})$, then we obviously have

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

In fact, $H_p$ is the image of following kind of morphism: $\mathbb{Z}_p^{\times} \rightarrow \text{GL}_2(\mathbb{Z}_p) \rightarrow \text{GL}_2(\mathbb{Z}_p/p^{\text{ord}_pN_1} \mathbb{Z})$, then the following lemma implies that $H_p$ and $H'_p$ are conjugate in $\text{GL}_2(\mathbb{Z}/p^{\text{ord}_pN_1} \mathbb{Z})$.

Lemma 2.7. For any two embeddings $\varphi_i : \mathbb{Z}_p^{\times} \rightarrow M_2(\mathbb{Z}_p), i = 1, 2$, there exists $g \in \text{GL}_2(\mathbb{Z}_p)$, such that $\varphi_1 = g^{-1}\varphi_2g$.

Remark 2.8. If we change $\mathbb{Z}_p$ to $\mathbb{Q}_p$, and $\mathbb{Z}_p^{\times}$ to $\mathbb{Q}_p^{\times}$, this lemma is well-known.

Proof. Consider $V = \mathbb{Z}_p \oplus \mathbb{Z}_p$, with a natural action of $M_2(\mathbb{Z}_p)$. Via $\varphi$, we view $V$ as an $\mathbb{Z}_p$-module, denoted by $V_i, i = 1, 2$. Since $\mathbb{Z}_p$ is a discrete valuation ring and $V_i$ are torsion free, so $V_1, V_2$ are both free $\mathbb{Z}_p$-module of rank 1, so there exists an isomorphism $g : V_1 \rightarrow V_2$ of $\mathbb{Z}_p$-module, this isomorphism corresponds to an element of $\text{GL}_2(\mathbb{Z}_p)$, also denoted by $g$. $g$ is an isomorphism of $\mathbb{Z}_p$-modules means that

$$g\varphi_1(x) = \varphi_2(x)g, \forall x \in \mathbb{Z}_p^{\times}.$$

Lemma 2.9. Let $\zeta_{N_1}$ be a primitive $N_1$-th root of unity. Then the cusp $\infty$ of $X_K(N)$ is defined over $\mathbb{Q}(\zeta_{N_1})$. 

\[\Box\]
Proof. In the adelic language, we have the following complex uniformization

\[ X_K(N)(\mathbb{C}) = \text{GL}_2(\mathbb{Q})_+ \backslash \mathbb{H} \times \text{GL}_2(\mathbb{Z}) / \hat{R}^\times \cup \{\text{cusps}\} \]

where \( \hat{R} = R \otimes \mathbb{Z} \hat{\mathbb{Z}} \) and the cusps are

\[ \text{GL}_2(\mathbb{Q})_+ \backslash \mathbb{P}^1(\mathbb{Q}) \times \text{GL}_2(\mathbb{Z}) / \hat{R}^\times. \]

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

\[ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} x \\ 0 \end{pmatrix} \in \hat{R}^\times, \]

which implies

\[ \gamma \in \mathbb{Z}_p^\times, \quad \alpha x \in \mathbb{Z}_p^\times, \quad \beta, \gamma \in N_1 \mathbb{Z}_p \text{ for all } p, \text{ and } \alpha x \equiv \gamma \pmod{N_1} \text{ for all } p \mid N_1. \]

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

\[ \mathbb{Q}^\times / Q^\times \mathbb{Z}^\times(N_1) \prod_{p \mid N_1} (1 + N_1 \mathbb{Z}_p), \]

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

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

**Atkin-Lehner operator.** Take \( j = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix} \), then \( kj = jk \) for all \( k \in K \) where \( k \) is the Galois conjugation of \( k \). For each \( p \mid N_0 \), let

\[ w_p = \begin{pmatrix} 0 \\ \text{ord}_p N \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{Q}_p) \]

be the local Atkin-Lehner operator. Define

\[ w = j^{(N_0)} \cdot \prod_{p \mid N_0} w_p \in \text{GL}_2(\mathbb{Q}) \cap M_2(\mathbb{Z}). \]

Since \( w \) normalizes \( \hat{R}^\times \), it acts on \( X_K(N) \).

For each \( p \mid N_0 \), write \( N_0 = p^{k} \cdot m \) with \((p, m) = 1 \). Similar to the proof of lemma (2.1), we can choose \( u, v \in \mathbb{Z} \) such that \( p^k u + mv = 1 \), let \( g = \begin{pmatrix} p^k \\ -N_0 v \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^k u \end{pmatrix} \in \text{GL}_2^+(\mathbb{Q}) \cap M_2(\mathbb{Z}) \), such that \( g^{-1} w_p \in U \), so

\[ w_p P = [h_0, w_p] = [g^{-1} h_0, 1] = \left( \mathbb{C}/\mathbb{Z} \cdot g^{-1} h_0 + \mathbb{Z}, \left( \frac{1}{N_0}, \mathbb{H} \left( \frac{g^{-1} h_0}{N_0} \right) \right) \right). \]

Modify it, we get

\[ w_p P = \left( \mathbb{C}/\mathbb{Z} h_0^{-1} + \mathbb{Z} \cdot p^k, \left( v + \frac{h_0^{-1}}{m} \right), \mathbb{H} \left( \frac{\frac{1}{N_0}}{N_0} \right) \right). \]

However, \( a = \mathbb{Z} h_0^{-1} + \mathbb{Z} \cdot p^k = \mathbb{Z}^\times \)

is an invertible ideal of \( \mathcal{O} \) dividing \( N \). Suppose \( N = \mathfrak{a} m \), let \( N' = \mathfrak{a} \mathfrak{m} \), then \( N'^{-1} \mathfrak{a}/\mathfrak{a} = \left( v + \frac{h_0^{-1}}{m} \right). \)

In another words, consider 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 \( \mathbb{Q} \), then 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 [6, pp.90].

To study the action of \( w \) on \( X_K(N) \), we can prove the following lemma:

**Lemma 2.10.** There exists \( t_0 \in \hat{K}^\times \) and \( u \in \hat{R}^\times \) such that \( w = t_0 j u \).

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

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

So we choose \( \text{ord}_p y = -k - \text{ord}_p x + ay \in \mathbb{Z}_p \) 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. \( \square \)
Remark 2.11. By Shimura reciprocity law, if we use \([x] \mapsto [\overline{x}]\) to denote the complex conjugation on \(X_K(N)(\mathbb{C})\), then
\[\overline{[h_0,g]} = [h_0,\overline{g}], \forall g \in \text{GL}_2(\mathbb{A}_f).\]

Lemma 2.10 in fact tells that the action of \(w\) is the composition of a Galois action and the complex conjugation.

**Hecke correspondence.** Let \(\ell \nmid N\) be a prime, the Hecke correspondence on \(X_U\) is defined by
\[T_\ell \left( E, C, H \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) \right) = \sum_i \left( E/C_i, (C + C_i)/C_i, H \left( \frac{x_1 \mod C_i}{x_2 \mod C_i} \right) \right)\]
where the sum is taken over all cyclic subgroups \(C_i\) of \(E\) of order \(\ell\), \(\alpha_i\) is given by \((\mathbb{Z}/N_i\mathbb{Z})^2 \xrightarrow{\alpha} E[N_i] \simeq (E/C_i)[N_i].\) \(E[N_i] \simeq (E/C_i)[N_i]\) is because \((\ell, N) = 1\). This is just by definition.

2.2. **Gross-Zagier Formula.** Let \(E\) be an elliptic curve of conductor \(N\), \(K\) be an imaginary quadratic field of discriminant \(D\) and \(\chi\) be a ring class character over \(K\) of conductor \(c\). Assume \(E, K, \chi\) satisfy the condition \((*)\)

Then we can write \(N = N_0 N_1^2\), where \(p\mid N\) is inert in \(K\) if and only if \(p\mid N_1\).

Embed \(K\) in \(M_2(\mathbb{Q})\) by \(i\). There is a modular parametrization \(f : X_K(N) \to E\) mapping \([\bar{x}]\) 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 \(H\) fixed by \(K^\times\), then \(\mathcal{O}_c = \mathbb{Z} + \mathbb{Z} h_0^{-1}, N = \mathbb{Z} + \mathbb{Z} h_0^{-1}\) is an invertible ideal of \(\mathcal{O}_c\) such that \(N/\mathcal{O}_c \simeq \mathbb{Z}/N_0 \mathbb{Z}\).

Consider the following Heegner point on \(X_K(N)(\mathcal{O}_c)\) of conductor \(c\)
\[P = \left( \mathbb{C}/\mathcal{O}_c, N/\mathcal{O}_c, H \left( \frac{x_1}{h_0^{-1}} \right) \right) \in X_K(N)(\mathcal{O}_c).\]

Form the cycle:
\[P_\chi(f) = \sum_{\sigma \in \text{Gal}(H_c/K)} f(P_{\sigma})\chi(\sigma) \in E(H_c) \otimes \mathbb{C}.\]

**Theorem 2.12 (Explicit Gross-Zagier formula [3]).** We have the following equation
\[L'(1, E, \chi) = 2^{-\mu(N,D)} \frac{8\pi^2 \phi(\phi) H_K(P_\chi(f))}{w^2 c \sqrt{|D|}} \deg f (GZ)\]
here \(\phi\) is the normalized newform associated to \(E\), \(\mu(N,D)\) is the number of prime factors of \((N,D), u = [\mathcal{O}_K^*: \mathbb{Z}^*], H_K\) is the Neron-Tate height pairing over \(K\) and the Petersson inner product
\[(\phi, \phi)_{T_\chi(N)} = \int_{T_\chi(N) \backslash H} \phi(x + iy)^2 dx dy.\]

2.3. **Euler System.** Let \(S\) be a finite set of primes containing the prime factors of \(6cND_K\), \(N_S\) denote the set of integers any of whose prime divisors is not in \(S\). For any \(\ell, m \in N_S\) with \(\ell\) a prime and \(\ell \nmid m\), let \(P_m = (\mathbb{C}/a_m, N_1^{-1}a_m/\alpha_m, \alpha_m)\) be a Heegner point of conductor \(cm\). Let \(P_{m\ell} = (\mathbb{C}/a_{m\ell}, N_2^{-1}a_{m\ell}/\alpha_{m\ell}, \alpha_{m\ell})\), such that \(N_{m\ell} = N_m \cap \mathcal{O}_{m\ell}, a_{m\ell} = a \cap \mathcal{O}_{m\ell}, \alpha_{m\ell}\) is the composition \(\mathbb{Z}/N_1\mathbb{Z} \xrightarrow{\alpha_m} N_1^{-1}a_m/\alpha_m \xrightarrow{\sim} N_1^{-1}a_{m\ell}/\alpha_{m\ell}\).

**Theorem 2.13.** Then we have that \([H_{m\ell} : H_m] = (\ell + 1)/u_m\) if \(\ell\) is inert in \(K\) and \((\ell - 1)/u_m\) if \(\ell\) is split and
\[u_m \sum_{\sigma \in \text{Gal}(H_{m\ell}/H_m)} P_{m\ell}^\sigma = \begin{cases} T_\ell P_m, & \text{if } \ell \text{ is inert in } K, \\ \left(T_\ell - \sum w_{m\ell} \text{Frob}_w\right) P_m, & \text{if } \ell \text{ is split in } K, \end{cases}\]
where \(T_\ell\) is the Hecke correspondence, \(\text{Frob}_w\) is the Frobenius at \(w|\ell\) in \(\text{Gal}(H_m/K)\), and \(u_m = 1\) if \(m \neq 1\) and \(u_1 = [\mathcal{O}_K^*: \mathbb{Z}^*]\).

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 $\chi$ a ring class character over $K$ of conductor $c$. Let $L(s, \phi, \chi)$ be the Rankin-Selberg convolution of $\phi$ and $\chi$.

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

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

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 $\mathbb{Q} \setminus \{\infty\}$. Fix an embedding from $K$ in $B$. Let $R$ be an order in $B$ with discriminant $N$ and $R \cap K = \mathcal{O}_c$. 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 $p | (D, N)$, $K^\times_p$ normalizes $U$ and then $K^\times_p$ acts on $X_U$ by right multiplication. Let

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

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 $B^\times_p / U_p$ can be identified with $\mathbb{Z}_p$-lattices in $\mathbb{Q}^2_p$. 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 $\Lambda$, then $S_p$ is the lattice $p\Lambda$ and the set $\{h_p\}$ is the set of sublattices $\Lambda'$ of $\Lambda$ with $[\Lambda : \Lambda'] = p$. There is then a line $V(\phi, \chi)$ of $\mathbb{C}[X_U]^0$ characterized as following

- for any $p | N$, $T_p$ acts on $V(\phi, \chi)$ by $a_p$ and $S_p$ acts trivially;
- for any $p | (D, N)$ with ord$_p(N) \geq 2$, $K^\times_p$ acts on $V(\phi, \chi)$ by $\chi_p$.

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

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

where the embedding of $K$ to $B$ induces a map

$$\text{Gal}(H_c / K) = K^\times \backslash \hat{K}^\times / \hat{\mathcal{O}}^\times_c \rightarrow X_U.$$  

Theorem 2.14 (Explicit Waldspurger formula [3]). We have the following equation

$$L(1, \phi, \chi) = 2^{-\nu(N, D)} \frac{\delta^2(\phi, \chi) \Gamma_1(N)}{a^2 c^{\sqrt{D}} |D|} \left\langle f, f \right\rangle$$

(Wald)

where the pairing

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

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 $S$ be a set of finite places of $\mathbb{Q}$ containing all places dividing $6cND$. Let $\mathbb{N}_S$ denote the set of integers whose prime divisors are not in $S$.

Definition 2.15. 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 $x_m U x_m^{-1} \cap K^\times = \hat{\mathcal{O}}^\times_{cm}$.

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

For each prime $\ell \in \mathbb{N}_S$, fix an isomorphism $\beta_{\ell} : B_{\ell} \cong M_2(\mathbb{Q}_\ell)$, such that $\beta_{\ell}(U_{\ell}) = \text{GL}_2(\mathbb{Z}_\ell)$, 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 $\ell$ 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 $\delta \in \mathbb{Z}_p^\times \backslash \mathbb{Z}_p^2$, if $\ell$ is inert in $K$.  

8
For \( m \in \mathbb{N}_S \), define \( x_m \in \hat{B}^\times \) by

\[
(x_m)_\ell = \begin{cases} \beta_\ell^{-1} \begin{pmatrix} \text{ord}_m \ 0 \\ 0 \\ 1 \end{pmatrix} & \text{if } \ell \nmid m \\
1 & \text{if } \ell \mid m
\end{cases}
\]

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

**Theorem 2.16.** For any \( \ell, m \in \mathbb{N}_S \) with \( \ell \) a prime and \( \ell \nmid m \), we have that

\[
\sum_{\sigma \in \text{Gal}(H_{cm}/H_{cm})} [\sigma, x_m] = \begin{cases} 0 & \text{if } \ell \text{ is inert in } K, \\
(T_\ell - \sum_{w|\ell} \text{Frob}_w)[x_m] & \text{if } \ell \text{ is split in } K,
\end{cases}
\]

where the equality holds as divisors on \( X_U \), with \( \text{Frob}_w \) and \( u_m \) the same as Theorem 2.13.

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 non-trivial 2-torsion point in the following. Denote by \( L^{\text{alg}}(E, s) \) the algebraic part of \( L(E, s) \). Then \( L^{\text{alg}}(E, 1) = 1/6 \).

For a non-zero integer \( m \), let \( E^{(m)} : y^2 = x^3 + m^3 \) the quadratic twist of \( E \) by the field \( \mathbb{Q}(\sqrt{m}) \). Then \( E^{(m)} \) and \( E^{(m\cdot 3^m)} \) 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

\[
(-1)^{\# \{p \mid D, p=2,3,\infty\}}
\]

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 \( \infty \) is positive if and only if \( D \) is positive and for any place not dividing 6\( \infty \) 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 \( \mathcal{O}_B = \mathbb{Z}[1, i, (i + j)/2, (1 + k)/2] \) of \( B \). The unit group \( \mathcal{O}_B^\times \) of \( \mathcal{O}_B \) equals 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 \( \eta : \hat{\mathbb{Q}}^\times /\mathbb{Q}^\times \to \{\pm 1\} \) is the quadratic character associated to \( K \). Embed \( K \hookrightarrow B \) by sending \( \sqrt{-3} \) to \( k \), which induces an embedding \( \hat{\mathbb{Q}}^\times \hookrightarrow \hat{B}^\times \).

Let \( \pi = \otimes_v \pi_v \) be the automorphic representation of \( B_v^\times \) 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 \( \hat{B}^\times \) defined as following. If \( p = 2 \), then \( \mathcal{R}_2 = \mathcal{O}_{K,2} + 2\mathcal{O}_B \). 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 \( \hat{B}^\times \).

The local components of \( \pi \) have the following properties:

- \( \pi_\infty \) is trivial;
• $\pi_p$ is unramified if $p \neq 2, 3, \infty$, i.e. $\pi^{O_{B,p}}$ is one dimensional;
• $\pi^{O_{K,2}}$ is one dimensional and $\pi^{O_{K,3}}$ is two dimensional.

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

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

**Proposition 3.2.**

1. $\pi^U$ has an orthonormal basis $f_+$, $f_-$ under the Petersson inner product defined by

   \[ \| f \|^2 = \int_{B^x \backslash \tilde{B}^x / \hat{Q}^x} |f(g)|^2 dg \]

   with the Tamagawa measure $\text{Vol}(B^x \backslash \tilde{B}^x / \hat{Q}^x) = 2$.

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

3. For any $t \in K^x_3$, $\pi(t)f_+ = \chi_+(t)f_+$ and $\pi(t)f_- = \chi_-(t)f_-$.

Since the class number of $B$ with respect to $O_B$ is 1 by [24, pp. 152], one has

\[ \hat{B}^x = B^x \hat{O}_B^x = B^x B_3^x \hat{O}_B^x. \]

Therefore,

\[ B^x \backslash \tilde{B}^x / \hat{Q}^x U = B^x \backslash B^x B_3^x \hat{O}_B^{(3)} / U_2 U_3 \hat{O}_B^{(6)} = H^x \backslash B_3^x O_{B,3}^x / U_2 U_3, \]

where $H = B^x \cap B_3^x \hat{O}_B^{(3)} = O_{B,1}^x \subset B_3^x O_{B,2}^x$ and the last inclusion is given by the diagonal embedding.

**Lemma 3.3.** The double coset $H \backslash O_{B,2}^x / U_2$ is trivial and $H \cap U_2 \backslash B_3^x / U_3 = O_{B,2}^x / U_3$.

**Proof.** The proof is elementary. Firstly, we prove that $H \backslash O_{B,2}^x / U_2$ is trivial. Recall that $U_2 = O_{K,2}^x(1 + 2M_2(Z_2))$. As $GL_2(Z_2)/(1 + 2M_2(Z_2)) = GL_2(F_2)$, the claim follows from that for any $g \in GL_2(F_2)$, one may find $h \in H$ and $u \in O_{B,2}^x$ such that $g \equiv hu (\text{mod } 2Z_2)$. For the second claim, note that

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

For any $x \in B_3^x$, $x^{-1}(1 + \lambda)x = 1 + x^{-1} \lambda x \in U_3$ where $\lambda$ is any uniformizer of $B_3^x$. In particular, the action of $H \cap U_2$ on $B_3^x / U_3$ is equal to the action of the group generated by some uniformizer. Hence $H \cap U_2 \backslash B_3^x / U_3 = O_{B,2}^x / U_3$.

If we denote $Z_0$ the integer ring for the unramified quadratic extension field of $Q_3$, then

\[ O_{B,2}^x = Z_0^x(1 + \lambda Z_0); U_3 = O_{K,3}^x(1 + \lambda O_{B,3}) = \mu_2(1 + 3Z_0)(1 + \lambda Z_0) \]

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

\[ H' \backslash B_3^x O_{B,2}^x / U_2 U_3 \stackrel{\sim}{\leftarrow} H \cap U_2 \backslash B_3^x / U_3 \]

\[ \stackrel{\sim}{\leftarrow} O_{B,3}^x / U_3 \]

\[ \stackrel{\sim}{=\rightarrow} Z_0^x / \mu_2(1 + 3Z_0) \cong Z/4Z, \]

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

The image of $B^x \backslash \tilde{B}^x / \hat{Q}^x$ under the norm map is $Q_3^x \backslash \hat{Q}^x / \text{N}rU$. If $p \neq 3$, $\text{N}rU_p = Z_0^x$ while if $\text{N}rU_3 = 1 + 3Z_3$. Therefore, by the approximation theorem,

\[ Q_3^x \backslash \hat{Q}^x / \text{N}rU = Z_0^x / \text{N}rU_3 = Z_0^x / 1 + 3Z_3. \]

In particular, the cardinality of $Q_3^x \backslash \hat{Q}^x / \text{N}rU$ is 2. Forms in $C^\infty(B^x \backslash \tilde{B}^x / \hat{Q}^x U)$ of the form $\mu \circ \text{N}r$ for some Hecke character $\mu$ correspond to characters on $C[Z/4Z]$ of order dividing 2. Sum up, we obtain
**Lemma 3.4.** There is a natural bijection

\[ \mathbb{Z}_q^* / \mu_2(1 + 3\mathbb{Z}_q) \xrightarrow{\sim} B^\times \backslash \hat{B}^\times / \hat{\mathbb{Q}}^\times U \]

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

Since \( \mathcal{O}_K^\times \subset U_3 \), \( f \) is \( \chi \)-eigen and only if \( \pi_3(\varpi_3)f = \pm f \), if and only if \( f(\zeta^a \varpi_3) = \pm f(\zeta^a) \) for \( a = 0, \ldots, 3 \) where \( \zeta \) is a primitive 8th root of unity in \( \mathbb{Z}_q^* \). Moreover, we may assume \( \zeta \equiv 1 + i \pmod{1 + 3\mathbb{Z}_q} \).

To compute \( f(\zeta^a \varpi_3) \), since \( k \in H \cap U_3 \) 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 \( k_3 \) denote 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 \( \varpi_3 = 3 \) 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

\[ f_+(1) = 1, \quad f_+(\zeta^2) = -1, \quad f_+(\zeta^4) = f_+(\zeta^6) = 0 \text{ and } f_-(1) = 1, \quad f_-(\zeta^2) = -1, \quad f_-(\zeta^4) = f_-(\zeta^6) = 0. \]

Finally, \( \chi_0 \) is the non-trivial element in the residue spectrum of \( C^\infty(B^\times \backslash \hat{B}^\times / \hat{\mathbb{Q}}^\times U) \) and \( \chi_0(\zeta^a) = (-1)^a \) for \( a = 0, \ldots, 3 \). Thus, up to \( \pm 1 \), \( f_+ \) (resp. \( f_- \)) is the function on \( B^\times \backslash \hat{B}^\times / \hat{\mathbb{Q}}^\times U \), supported on those \( g \in \hat{B}^\times \) with \( \chi_0(g) = +1 \) (resp. \( = -1 \)), valued in \( 0, \pm 1 \) with total mass zero. It is clear that \( f_+ \) and \( f_- \) is an orthonormal basis of \( \pi^U \). We have completed the proof of Proposition 3.2.

Now let \( M = q_1 \cdots q_r \) with \( q_i \equiv 5 \pmod{12} \). For any \( q \mid M \), taking an isomorphism \( \iota_q : B_q \iso M_2(\mathbb{Q}_q) \)

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 \( x_q \in B_q^\times \) with \( \iota_q(x_q) = \begin{pmatrix} q \\ 1 \end{pmatrix} \). Then \( x_q \mathcal{O}_{B,q} x_q^{-1} \cap K_q = \mathcal{O}_{M,q} \). Take \( x_M = \prod_i x_{q_i} \in B^\times \). Denote by

\[ f_M = \begin{cases} f_+(x_M), & \text{if } r \text{ is even} \\ f_-(x_M), & \text{if } r \text{ is odd}. \end{cases} \]

Let \( \chi_M \) be the quadratic Hecke character of \( K \) associated to \( K(\sqrt{M})/K \), then \( \chi_M(\varpi_3) = (-1)^r \). Then \( f_M = \pi^U \). In particular, it satisfies that

1. \( \forall p \nmid 6M, T_p f_M = a_p f_M; \)
2. \( f_M \) is integrable-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 \( \text{Gal}(H_M/K) \simeq \text{Pic}(\mathcal{O}_M) = \hat{K}^\times / K^\times \hat{\mathcal{O}}_M^\times \). The embedding \( K \hookrightarrow B \) induces a map

\[ K^\times \backslash \hat{K}^\times / \hat{\mathcal{O}}_M^\times \to B^\times \backslash \hat{B}^\times / U. \]

Consider

\[ P_{K_M}(f_M) = \sum_{t \in \text{Pic}(\mathcal{O}_M)} f_M(t) \chi_M(t). \]

Denote by

\[ L^{alg}(s, E) = L(s, E)/\Omega(E) \]

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 \( \pm 1 \), \( L^{alg}(1, E^{(M)}) = 2^{-1} P_{K_M}(f_M) \).
Proof. By Theorem 2.14,
\[ L(1, E, \chi_M) = 2^{-3} \frac{8\pi^2 \langle \phi, \phi \rangle_{\Gamma_0(36)} |P_{\chi_M}(f_M)|^2}{\sqrt{3}M} \langle f_M, f_M \rangle. \]
Here,
\[ \langle f_M, f_M \rangle = \frac{|f_M|^2}{2} \text{Vol}(X_U) \]
and Vol($X_U$) is the mass of $U$. By [3, Lemma 2.2],
\[ \text{Vol}(X_U) = 2(4\pi^2)^{-1} \text{Vol}(U)^{-1} \]
where Vol($U$) is with respect to Tamagawa measures so that for any finite $p \neq 3$, Vol($\text{GL}_2(\mathbb{Z}_p)$) = $L(2,1_p)^{-1}$ and Vol($O_{B,3}^\times$) = $2^{-1}L(2,1_3)^{-1}$. By [3, Lemma 3.5], Vol($X_U$) = 4/3. Thus, deg$_U f_M$ = 2/3. On the other hand,
\[ 8\pi^2 \langle \phi, \phi \rangle_{\Gamma_0(36)} = 8\pi^2 \int_{\Gamma_0(36) \backslash \mathbb{H}} |\phi(x + iy)|^2 dx dy = i\Omega^{-1}. \]
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, $L^{alg}(1, E(M))^2 = (L(1, E(M))/\Omega(M))^2 = M\mathcal{L}(1, E, \chi_M)/\Omega^2$ and
\[ L^{alg}(1, E(M))^2 = 2^{-2}|P_{\chi_M}(f_M)|^2. \]
\[ \square \]

3.2. Rank Zero Twists. Keep the notations from the last section. Denote by $\mathcal{A} = \text{Gal}(H_M/K)$, then $2\mathcal{A} = \text{Gal}(H_M/H^0_M)$, where $H^0_M = K(\sqrt{q} : q \mid M)$. Let $\mathcal{A}$ (resp. $\mathcal{A}/2\mathcal{A}$) be groups of characters on $\mathcal{A}$ (resp. on $\mathcal{A}$ and factors through $\text{Gal}(H^0_M/K)$). Then
\[ \sum_{\chi \in \mathcal{A}/2\mathcal{A}} P_{\chi}(f_M) = 2^r y_0, \quad y_0 := \sum_{\sigma \in 2\mathcal{A}} f_M(\sigma) \]
Note that each $\chi \in \mathcal{A}/2\mathcal{A}$ corresponds to an integer $d|M$, in the sense that $\chi$ corresponds to the extension $K(\sqrt{d})/K$.

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

Proof. Choose primes $q \in \mathbb{N}_S$ such that $qd|M$. Then
\[ P_{\chi}(f_M) = \sum_{\sigma \in \mathcal{A}} f_M(\sigma)\chi(\sigma) = \sum_{\sigma \in \text{Gal}(H_{M/q}/K)} f_M(\sigma) \sum_{\tau \in \text{Gal}(H_M/H_{M/q})} \chi(\sigma\tau) = \sum_{\sigma \in \text{Gal}(H_{M/q}/K)} \chi(\sigma) \sum_{\tau \in \text{Gal}(H_M/H_{M/q})} f(\sigma x_M) \]
By Theorem 2.16, we have
\[ u_{M/q} \sum_{\tau \in \text{Gal}(H_M/H_{M/q})} f(\sigma x_M) = a_q f(\sigma x_{M/q}) = 0. \]
So the proposition holds. \[ \square \]

By Proposition 3.6, we have the equality
\[ P_{\chi_M}(f_M) = 2^r y_0 \]

Lemma 3.7. The values of $f_M|_{B_{x^2}}$ are odd. In particular, $y_0$ is odd and
\[ v_2(P_{\chi_M}(f_M)) = r. \]

Proof. By the definition of $f_M$, $f_M|_{B_{x^2}}$ is odd if and only if for any $g \in B_{x^2}$, $\chi_0(gx_M) = (-1)^r$. Since $\chi_0$ is quadratic, $\chi_0(g) = 1$. Then $\chi_0(gx_M) = \chi_0(x_M) = \prod_{i=1}^{q+1} \chi_0(q_i) = (-1)^r$ as $q_i$ is inert in $K$. Hence
\[ y_0 \equiv [H_M : H^0_M] \equiv \frac{1}{3} \prod_{q|M} q + \frac{1}{2} \equiv 1 (\text{mod } 2). \]
\[ \square \]
The Proof of Theorem 1.3. By Proposition 3.5, \(v_2(L_{alg}^1(1, E^{(M)})) = r - 1\). The 2-part of BSD is equivalent to

\[
v_2 \left( L_{alg}^1(1, E^{(M)}) \right) = \sum_{p \nmid 6M} v_2 \left( c_p \left( E^{(M)} \right) \right) - 2v_2 \left( \# E^{(M)}_{tor} \right) + v_2 \left( \# \text{III}(E^{(M)}/\mathbb{Q}) \right).
\]

The Tamagawa numbers of \(E^{(M)}\) are: \(c_2(E^{(M)}) = 3\) (resp. \(= 1\)) if \(M \equiv 1 \pmod{8}\) (resp. otherwise), \(c_3(E^{(M)}) = 2\) and \(c_4(E^{(M)}) = 2\) for \(q \mid M\). On the other hand, \(E^{(M)}(\mathbb{Q}) = E^{(M)}(\mathbb{Q})_{tor} = \mathbb{Z}/2\mathbb{Z}\). Finally, using classical 2-descent, \(\text{III}(E^{(M)}/\mathbb{Q})[2] = 0\). Combine 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 \(p \nmid 6\), hence and the first part of Theorem 1.3 holds.

\[\square\]

3.3. The Gross-Zagier Formula. Let \(K = \mathbb{Q}(\sqrt{-\ell})\) with \(\ell \equiv 11 \pmod{12}\). Let \(N = 36\). Write \(N = N_0 N_2^2\) 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 \(i_\epsilon\) with \(\epsilon = 1\) 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

\[
\sqrt{-\ell} \mapsto \begin{pmatrix} a & 2 \\ \ell a^2 & -a \end{pmatrix}.
\]

Then \(M_2(\mathbb{Z}) \cap K = R_0(N_0) \cap K = O_K\). Under such embedding, take \(R = O_K + N_1 R_0(N_0)\) and consider the modular curve \(X_K(N)\). For the Heegner hypothesis case, \(X_K(N) = X_0(36)\). For another case, the modular curve \(X_K(N)\) has genus one and by Lemma 2.9, 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

\[
y^2 = x^3 - 27 \quad (36C)
\]

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

\[
\epsilon = \begin{pmatrix} 1 & 0 \\ -a & -1 \end{pmatrix} \in K^-.
\]

Lemma 3.8. Take \(w \in \text{GL}_2(\mathbb{Q})\) the Atkin-Lehner operator defined in Section 2.1. Precisely, for the Heegner hypothesis case, \(w = j(3\ell)w_2w_3\) while for another case, \(w = j(3\ell)w_3\). Then \(w\) normalize \(R^*\) and \(w = toju\) for some \(t_0 \in R^*\) and \(u \in R^*\). 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 \(2A(\mathbb{Q}) = \{0\}\) for the other case.

Proof. By Lemma 2.10, it suffices to prove the “Moreover” part.

For the Heegner hypothesis case, denote by \(\text{Hom}_{\mathbb{Q}}(X_0(N), E)\) the space of \(\mathbb{Q}\)-morphisms from \(X_0(N)\) to \(E\) taking \([\infty]\) to \(O\) and \(\text{Hom}_{\mathbb{Q}}(X_0(N), E) = \text{Hom}_{\mathbb{Q}}(X_0(N), E) \otimes \mathbb{Z}\mathbb{Q}\). By Atkin-Lehner theory, \(f^w = -f \in \text{Hom}_{\mathbb{Q}}(X_0(N), E)\). So \(f^w + f\) is a constant map. However, \(f([\infty]) = 0\), \(f^w([\infty]) = f([0]) = [0]\), 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 another case, view \(f \in \text{Hom}_{\mathbb{Q}}(X_K(N), A)\). Then \(f^w = \epsilon(A/Q_3)f = f\). As \(f\) and \(f^3\) are both \(K^X\)-invariant and such vectors in \(\text{Hom}_{\mathbb{Q}}(X_K(N), A)\) is of dimension 1. There is a sign \(\epsilon \in \{\pm 1\}\) such that \(f^{32} = \epsilon f\). By [11, Theorem 4], the sign \(\epsilon_2 = +1\) if and only if \(\epsilon(A/Q_3) = \epsilon(A^{-1}/Q_3) = 1\). Since \(\epsilon(A/Q_3) = -1\), we obtain \(f^{32} = -f\). Thus \(f^w + f = -f\) 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 equivalent to say \(w \notin P(\mathbb{Q})R^X\) with \(P\) the upper-triangular matrices in \(\text{GL}_2\). This holds since \(w_3 \notin P(\mathbb{Q})R^X\).

Write \(\text{Isom}_Q(A)\) for the group of algebraic isomorphisms of \(A\) over \(Q\) and \(\text{Aut}_Q(A)\) the subgroup of algebraic isomorphisms over \(Q\) which fix \(O\). Then \(\text{Aut}_Q(A) = \mathbb{Z}/2\mathbb{Z}\) is generated by multiplication \(-1\) and \(\text{Isom}_Q(A) = (t_T) \times \text{Aut}_Q(A)\) where \(t_T : P \mapsto P + T\) for any \(P \in A\).

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, \(P^{j(3)} = P^w w_3^{-1} = -P\). \(\square\)
Let $M = \prod q_i$ where $q_i$ are distinct positive integers $\equiv 5 \pmod{12}$. Denoted by $\chi_M$ the quadratic character of $K$ associated to the extension $K(\sqrt{M})/K$. Let $P_M \in \mathcal{X}_K(N)(H_M)$ be the Heegner point defined in 2.3. Consider

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

**Proposition 3.10.** Up to $\pm 1$,

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

**Proof.** By Theorem 2.12,

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

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 the proof of 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:

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

□

3.4. **Rank One Twists.** Let $\ell$ 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 $q_i \equiv 5 \pmod{12}$ and inert in $K$. Denote by $\mathcal{A} = \text{Gal}(H_M/K)$. Then $2\mathcal{A} = \text{Gal}(H_M/H^0_M)$, where $H^0_M = K(\sqrt{q} : q \mid M)$. Let $\mathcal{A}^\ast$ (resp. $\mathcal{A}^\ast/2\mathcal{A}^\ast$) be the group of characters on $\mathcal{A}$ (resp. on $\mathcal{A}^\ast$ and factors through $\text{Gal}(H^0_M/K)$).

Let $A$ be the elliptic curve $y^2 = x^3 - 27$. Observe that $A(H^0_M)[2\infty] = A(\mathbb{Q})[2\infty] = A(\mathbb{Q})[2]$. In fact, suppose $Q \in A(H^0_M)[2\infty]$ but $Q \notin A(\mathbb{Q})[2\infty]$. Then the extension $\mathbb{Q}(Q)/\mathbb{Q}$ is unramified outside 2 and 3. However, as $Q(\mathbb{Q}) \subset H^0_M$, $Q(\mathbb{Q})/\mathbb{Q}$ must be ramified at $\ell$ or $q_i$ for some $i$. A contradiction. Let $T$ be the nontrivial element in $A(\mathbb{Q})[2]$, and $C = \#A(H^0_M)_{\text{tor}}$ be the cardinality of odd part of $A(H^0_M)_{\text{tor}}$.

Denote by

$$y_M = P_{\chi_M}(f) = \sum_{\sigma \in \mathcal{A}} f(P_M)^\sigma \chi_M(\sigma) \in A(H^0_M).$$

Then the same as Proposition 3.6, we have

$$y_M = 2^r y_0, \quad y_0 := \sum_{\sigma \in \mathcal{A}/2} f(P_M)^\sigma,$$

as equality of points in $A(H^0_M)$. The key point is the following lemma:

**Lemma 3.11.**

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

**Proof.** By Lemma 2.10, one can write $w = t_0 j u$ with $t_0 \in \hat{K}^\times$, $j = \hat{K}^-$ and $u \in \hat{R}^\times$. Take $x_M \in \hat{B}^\times$ such that $P_M = [z, x_M] \in \mathcal{X}_K(N)(H_M)$ with $z \in \mathcal{H}^0_K$. Thus, for any $\sigma \in 2\mathcal{A}$ with $t \in \hat{K}^\times$

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

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

$$f^w(P_M)^{\sigma_t} = f([h_0, x_M j])^{\sigma t_0}.$$
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 $R_q^* = \text{GL}_2(\mathbb{Z}_q)$. It is easy to check this holds. Thus

$$f^w(P_M)^{\sigma_0} = f([h_0, j x_M])^{\sigma_0} = f([h_0, x_M])^{\sigma_0}.$$  

On the other hand, note that in the proof of Lemma 2.10, $t_0, p = 1$ for any $p \not| N_0 = 9$. Denote by $a_0 = N_{K'/Q}(t_0) \in \hat{Q}^\times$. Take determinant for the equation $w = j t_0$. Then $a_0, p = 1$ if $p \neq 3$ and $a_0, p = 2$ if $p = 3$. Thus for any prime $q | M$

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

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

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

$$\eta_0 + \eta = \sum_{\sigma \in 2A} (f + f^w) (P_M)^{\sigma} = [H_M : H^0_M] T = T.$$  

\[ \square \]

**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

$$A(K(\sqrt{M}))/2^r A(K(\sqrt{M}))$$

$$\begin{array}{c}
0 \to H^1(H^0_M/K(\sqrt{M}), A[2]^r(H^0_M)) \to H^1(K(\sqrt{M}), A[2]^r) \to H^1(H^0_M, A[2]^r)
\end{array}$$

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

$$y_M = 2^r z + t, z = 2 \eta + s$$

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

Let $\sigma \in \text{Gal}(K(\sqrt{M})/K)$ be the nontrivial element. Then by definition, we have $y_M + y_M^\sigma = 0$, so

$$y_0 + y_0^\sigma \in A(H^0_M)[2] = A(Q)[2],$$

thus $z + z^\sigma = 0$. On the other hand

$$z + \overline{z} = 2(\eta + \overline{\eta}) = 0,$$

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

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

We will show that the 2-index of $y_M$ is exactly $r - 1$. Suppose that $y_M = 2^r z + t$ for some $z \in A(Q(\sqrt{-LM}))$ and $t \in A(Q(\sqrt{-LM}))$ tor. Then $2^r (z - \eta) + t = 0$, which implies $C(z - \eta) \in A(Q)[2]$. Operating by complex conjugation and plus together, $C(z - \eta) + C(\overline{z} - \overline{\eta}) = 0$. But we have $z + \overline{z} = 0$, so $C(z + \overline{z}) = 0$. But it contradicts to the fact that $\overline{\eta} + \overline{\eta} = T \neq 0$. \[ \square \]

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

By Proposition 3.10, up to $\pm 1$,

$$L_{\text{alg}}(1, A(M)) \frac{L'(1, A(-LM))}{\Omega(A(-LM))} = \tilde{h}_K(y_M).$$

Denote by $R(-LM) = \tilde{h}(P_{LM})$ where $P_{LM}$ is the generator of $A(-LM)(Q)/A(-LM)(Q)$ tor. In particular, by Theorem 3.12

$$\tilde{h}_K(y_M) = 2^{2r-1} R(-LM)$$

Thus, if denote by

$$L_{\text{alg}}(s, A(-LM)) = \frac{L'(s, A(-LM))}{R(-LM) \Omega(A(-LM))}$$

then by the result of rank zero case, we have

$$v_2(L_{\text{alg}}(1, A(-LM))) = r.$$
The Tamagawa numbers of $A^{(−LM)}$ are: $c_2(A^{(−LM)}) = 1$ or 3, $c_3(A^{(−LM)}) = 2$ and $c_q(A^{(−LM)}) = 2$ for $q∤\ell M$. On the other hand, $A^{(−LM)}(\mathbb{Q}) = A^{(−LM)}(\mathbb{Q})_{\text{tor}} = \mathbb{Z}/2\mathbb{Z}$. Finally, using classical 2-descent, $III(A^{(−LM)}/\mathbb{Q})[2] = 0$. Combine the results above, it is clear that the 2-part of BSD conjecture for $A^{(−LM)}$ holds.

Since $A^{(−LM)}$ has CM, so the $p$-adic height paring is nontrivial. Then by [12, Corollary 1.9], $p$-part of the BSD conjecture for $A^{(−LM)}$ holds for $p ∤ 6\ell M$. So the second part of Theorem 1.2 holds for $A$, and hence for $E$.

References

[1] M.Bertolini and H.Darmon, Heegner points, L-functions and Cerednik-Drinfeld uniformization. Invent. Math. 131 (1998), no. 3 453-491.
[2] D.Bump, S.Friedberg and J.Hoffstein, Non-vanishing theorems for L-functions for modular forms and their derivatives, Invent. Math. 102 (1990), 543-618.
[3] L.Cai, J.Shu and Y.Tian, Explicit Gross-Zagier formula and Waldspurger formula, Algebra Number Theory 8 (2014), no. 10, 2523C2572.
[4] J. Coates, Y. Li, Y. Tian, and S. Zhai, Modular units, Algebra Number Theory 8 (2014), no. 10, 2523C2572.
[5] Solomon Friedberg and Jeffrey Hoffstein, Nonvanishing theorems for automorphic L-functions on GL(2), Ann. of Math. 142 (1995), 385-423
[6] B.Gross Local Orders, Root Numbers, and Modular Curves, Amer. J.Mathp, Vol 110, No. 6 (Dec. 1988), pp. 1153-1182.
[7] B.Gross Heegner points on $X_0(N)$, Modular forms (Durham, 1983), 87-105, Ellis Horwood Ser. Math. Appl.:Statist. Oper. Res., Horwood, Chichester, 1984.
[8] B. Gross and D. Zagier, Heegner points an derivatives of L-series, Invent. Math. 84 (1986), no. 2, 225-320.
[9] N.Katz and B.Mazur Arithmetic moduli of elliptic curves Princeton Univ. Press, Princeton, NJ, 1985;
[10] J.Nekovář, The Euler system method for CM points on Shimura curves, L-functions and Galois representations, 471C547, London Math. Soc. Lecture Note Ser., 320, Cambridge University Press, Cambridge, 2007.
[11] D.Prasad, Some applications of seesaw duality to branching laws. Math. Ann. 304 (1996), no. 1, 1C20.
[12] Perrin-Riou, Points de Heegner et dérivées de fonctions L p-adiques, Invent. Math. 89 (1987), no.3 455-510.
[13] H. Qin, Representation of integers by positive ternary quadratic forms, Cambridge Journal of Mathematics, 2 (2014), 117-161.
[14] K. Rubin, The main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. Math. 103 (1991), no. 1, 25-68.
[15] Anthony J. Scholl, On modular units. Math. Ann. 285 (1990), no. 3, 503C510.
[16] J-P.Serre, Lectures on the Mordell-Weil theorem. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. With a foreword by Brown and Serre. Third edition. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1989. x+218 pp. ISBN: 3-528-22732-2 11G05 (11D41 11G30 14G25)
[17] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton, NJ, 1971.
[18] J. Tunnell, Local epsilon factors and characters of GL(2), Amer. J. Math 105 (1983), 1277-1307.
[19] Y. Tian Euler systems of CM points on Shimura curves, Ph.D Thesis, Columbia University, 2003.
[20] Y. Tian, Congruent Numbers and Heegner Points, Cambridge Journal of Mathematics, 2 (2014), 117-161.
[21] Y. Tian, Congruent numbers with many prime factors, Proc. Natl. Acad. Sci. USA 109 (2012), 21256-21258.
[22] Y. Tian, X. Yuan, S. Zhang, Genus Periods, Genus Points and Congruent Number Problem, preprint, 2015.
[23] Vigneras, Arithmétique des algèbres de quaternions, Lect. Notes in Math., 800. Springer, Berlin, 1980. vii+169 pp.
[24] V. Pal, Periods of quadratic twists of elliptic curves, Proceedings AMS 140 (2012), 1513-1525.
[25] J-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier J. Math. Pures Appl. 60 (1981), 375-484.
[26] Xinyi Yuan, Shouwu Zhang and Wei Zhang, The Gross-Zagier Formula on Shimura Curves, Princeton University Press, Annals of Mathematics Studies, (2013).