TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 10, 15 November 2019, Pages 6905–6925
https://doi.org/10.1090/tran/7760
Article electronically published on January 16, 2019

AN EXPLICIT GROSS–ZAGIER FORMULA RELATED TO THE SYLVESTER CONJECTURE

YUEKE HU, JIE SHU, AND HONGBO YIN

ABSTRACT. Let $p \equiv 4, 7 \bmod 9$ be a rational prime number such that 3 mod p is not a cube. In this paper, we prove the 3-part of $|Ш(E_p)| \cdot |Ш(E_{3p^2})|$ is as predicted by the Birch and Swinnerton-Dyer conjecture, where $E_p : x^3+y^3 = p$ and $E_{3p^2} : x^3 + y^3 = 3p^2$ are the elliptic curves related to the Sylvester conjecture and cube sum problems.

1. INTRODUCTION

In this paper, we are concerned about the explicit Gross–Zagier formula and the full Birch and Swinnerton-Dyer (BSD) conjecture for the elliptic curves which are related to the Sylvester conjecture. The motivation comes from the cube sum problem. A nonzero rational number is called a cube sum if it is of the form a^3+b^3 with $a, b \in \mathbb{Q}^\times$. For any $n \in \mathbb{Q}^\times$, let E_n be the elliptic curve over $\mathbb{Q}$ defined by the projective equation $x^3 + y^3 = nz^3$ with the distinguished point $(1 : -1 : 0)$. If n is not a cube or twice a cube of nonzero rationals, then n is a cube sum if and only if $E_n(\mathbb{Q})$ has a point of infinite order. A famous conjecture concerning the cube sums, attributed to Sylvester, is the following.

Conjecture 1.1 (Sylvester [Syl79] and Selmer [Sel51])**.** *Any prime number* $p \equiv 4, 7, 8 \bmod 9$ *is a cube sum.*

For a good summary of this conjecture, please refer to [DV09, DV18]. For an odd prime $p \geq 5$, a 3-descent [Sat86, DV09] gives

$$\operatorname{rank}_{\mathbb{Z}} E_p(\mathbb{Q}) \leq \begin{cases} 0, & p \equiv 2, 5 \bmod 9, \\ 1, & p \equiv 4, 7, 8 \bmod 9, \\ 2, & p \equiv 1 \bmod 9. \end{cases}$$

Let $\epsilon(E_p)$ be the sign in the functional equation of the Hasse–Weil L-function $L(s, E_p)$. From [Liv95], we know that

$$\epsilon(E_p) = \begin{cases} -1, & p \equiv 4, 7, 8 \bmod 9, \\ +1, & \text{otherwise.} \end{cases}$$

Then the BSD conjecture implies the Sylvester conjecture. In 1994, Elkies announced a proof of Conjecture 1.1 for all primes $p \equiv 4, 7 \bmod 9$, but without any

Received by the editors October 25, 2018.
2010 *Mathematics Subject Classification.* Primary 11G05.
The first author was supported by SNF-169247.
The second author was supported by NSFC-11701092.
The third author was partially supported by NSFC-11701548 and The Fundamental Research Funds of Shandong University.

detailed publication. However, Dasgupta and Voight [DV18] proved the following weaker theorem using a method substantially different than that of Elkies.

Theorem 1.2. *Let $p \equiv 4, 7 \bmod 9$ be a rational prime number such that $3 \bmod p$ is not a cubic residue. Then p and p^2 are cube sums.*

Dasgupta and Voight proved the above theorem by establishing the nontriviality of certain related Heegner points. By the work of Gross and Zagier [GZ86] and Kolyvagin [Kol90], the nontriviality of Heegner points implies that the rank part of the BSD conjecture for E_p is true.

If $\ell \nmid 6p$ is a prime, then E_p has good reduction at ℓ. Then Perrin-Riou [PR87] and Kobayashi [Kob13] proved that the ℓ-part full BSD conjecture holds for E_p. Since E_p has potential good ordinary reduction at p, the p-part full BSD conjecture of E_p is also true by the work of Li, Liu, and Tian [LLT16]. To summarize, the following theorem is known.

Theorem 1.3. *Let $p \equiv 4, 7 \bmod 9$ be a rational prime number such that $3 \bmod p$ is not a cubic residue. Then*

1. $\mathrm{ord}_{s=1} L(s, E_p) = \mathrm{rank}_{\mathbb{Z}} E_p(\mathbb{Q}) = 1$*; and*
2. *the Tate–Shafarevich group $Ш(E_p)$ is finite, and for any prime $\ell \nmid 6$, the ℓ-part of $|Ш(E_p)|$ is as predicted by the BSD conjecture for E_p.*

But for the primes $\ell = 2, 3$, there are no results known for the ℓ-part full BSD conjecture of E_p. In this paper, we adopt a similar method as in [CST17] to approach the 3-part full BSD conjecture of E_p and E_{3p^2} by comparing to an explicit Gross–Zagier formula.

Let $Ш(E_p)$ denote the Shafarevich–Tate group of E_p, let $E_p(\mathbb{Q})_{\mathrm{tor}}$ denote the torsion subgroup of $E_p(\mathbb{Q})$, let Ω_p denote the minimal real period of E_p, let $\widehat{h}(\cdot)$ denote the Néron–Tate height of E_p over $\mathbb{Q}$, and let c_ℓ denote the Tamagawa number of E_p at a prime ℓ. From [DV18], we know that $E_p(\mathbb{Q})$ (resp., $E_{3p^2}(\mathbb{Q})$) has rank 1 (resp., 0). Let P be a generator of the free part of $E_p(\mathbb{Q})$. Then the BSD conjecture predicts that

$$|Ш(E_p)| = \frac{L'(1, E_p)}{\Omega_p \cdot \widehat{h}_{\mathbb{Q}}(P)} \cdot \frac{|E_p(\mathbb{Q})_{\mathrm{tor}}|^2}{\prod_\ell c_\ell(E_p)},$$

where ℓ runs through all prime numbers. Similarly, for $E_{3p^2}(\mathbb{Q})$, the BSD conjecture predicts that

$$\left|Ш(E_{3p^2})\right| = \frac{L(1, E_{3p^2})}{\Omega_{3p^2}} \cdot \frac{|E_{3p^2}(\mathbb{Q})_{\mathrm{tor}}|^2}{\prod_\ell c_\ell(E_{3p^2})}.$$

Combining these two formulae, we shall expect that

$$|Ш(E_p)| \cdot |Ш(E_{3p^2})| = \frac{L'(1, E_p)}{\Omega_p \cdot \widehat{h}_{\mathbb{Q}}(P)} \cdot \frac{L(1, E_{3p^2})}{\Omega_{3p^2}} \cdot \frac{|E_p(\mathbb{Q})_{\mathrm{tor}}|^2}{\prod_\ell c_\ell(E_p)} \cdot \frac{|E_{3p^2}(\mathbb{Q})_{\mathrm{tor}}|^2}{\prod_\ell c_\ell(E_{3p^2})}. \tag{1.1}$$

Our main result is the following.

Theorem 1.4. *Let $p \equiv 4, 7 \bmod 9$ be a rational prime number such that $3 \bmod p$ is not a cubic residue. Then both sides of (1.1) are nonzero rational numbers and the exponents of 3 in both sides of (1.1) are equal, as expected.*

In the following, we sketch the proof of Theorem 1.4. Let $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the Poincaré upper half plane, and $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ by fractional linear

transformations. Let $\Gamma_0(3^5) \subset \mathrm{SL}_2(\mathbb{Z})$ be the congruence subgroup of level 3^5 which consists of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{with } c \equiv 0 \bmod 3^5.$$

Then $Y_0(3^5) = \Gamma_0(3^5)\backslash\mathcal{H}$ is an affine smooth curve over $\mathbb{Q}$, and let $X_0(3^5)$ be its projective closure.

Fix $K = \mathbb{Q}(\sqrt{-3}) \subset \mathbb{C}$, with $\mathcal{O}_K = \mathbb{Z}[\omega]$ being its ring of integers, where $\omega = \frac{-1+\sqrt{-3}}{2}$. We carefully embed K into $\mathrm{M}_2(\mathbb{Q})$ as follows. Once such an embedding is given, the group $K^\times$ of invertible elements acts on $\mathcal{H}$ through fractional linear transformations, and there is a unique point in $\mathcal{H}$ which is invariant under the action of $K^\times$. There are exactly two embeddings $\rho : K \hookrightarrow \mathrm{M}_2(\mathbb{Q})$ with fixed point $\tau = (2p\omega - 9)/(9p\omega - 36) \in \mathcal{H}$, and we choose the normalized one, i.e., we have

$$\rho(t)\begin{pmatrix} \tau \\ 1 \end{pmatrix} = t\begin{pmatrix} \tau \\ 1 \end{pmatrix} \qquad \text{for any } t \in K.$$

For any $n \in \mathbb{Q}^\times$, the elliptic curve E_n has the Weierstrass equation

$$y^2 = x^3 - 432n^2$$

and has complex multiplication by $\mathcal{O}_K$ over K. We fix the complex multiplication $[\,] : \mathcal{O}_K \simeq \mathrm{End}_{\overline{\mathbb{Q}}}(E_n)$ by $[\omega](x, y) = (\omega x, y)$. The image of $\tau \in \mathcal{H}$ defines a complex multiplication (CM) point on $X_0(3^5)$. Let $f : X_0(3^5) \to E_9$ be the the natural modular parametrization. The Heegner point $f(\tau)$ is defined over the ring class field H_{9p} over K of conductor $9p$.

Let $p \equiv 4, 7 \bmod 9$ be a prime. Let $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathcal{O}_K^\times$ be the character given by $\chi(\sigma) = (\sqrt[3]{3p})^{\sigma-1}$. Define the Heegner cycle

$$P_\chi(f) = \sum_{\sigma \in \mathrm{Gal}(H_{9p}/K)} f(\tau)^\sigma \otimes \chi(\sigma) \in E_9(H_{9p}) \otimes_{\mathbb{Q}} K.$$

The base change L-function $L(s, E_9, \chi)$ has sign -1 and has a decomposition

$$L(s, E_9, \chi) = L(s, E_p) \cdot L(s, E_{3p^2}).$$

By the work [DV18], we know that $L(s, E_p)$ has a 0 of order 1 at $s = 1$ and $L(1, E_{3p^2}) \neq 0$. The morphism f is a test vector for the pair (E_9, χ), i.e., there is a nontrivial relation between the central value of the derivative of the L-function $L(s, E_9, \chi)$ and the height of the Heegner cycle $P_\chi(f)$. More precisely, we have the following result (see Theorem 4.3).

Theorem 1.5. *For primes $p \equiv 4, 7 \bmod 9$, we have the following explicit height formula of Heegner cycles:*

$$\frac{L'(1, E_p)L(1, E_{3p^2})}{\Omega_p \Omega_{3p^2}} = 2^\alpha \cdot \left\langle P_\chi(f), P_{\chi^{-1}}(f) \right\rangle_{K,K},$$

where $\alpha = 0$ if $p \equiv 4 \bmod 9$ and $\alpha = -1$ if $p \equiv 7 \bmod 9$, and where $\langle \cdot, \cdot \rangle_{K,K}$ denotes the K-linear Néron–Tate height pairing of E_9 over K.

For the definition of $\langle \cdot, \cdot \rangle_{K,K}$, see, for example, [CST14, page 2531]. We remark that we do not need the hypothesis that 3 is not a cube modulo p in the above theorem.

The proof of this theorem requires an ingredient on the local Waldspurger's period integral at 3-adic place, that is,

$$\frac{\beta_3^0(f_3', f_3')}{\beta_3^0(f_3, f_3)} = 2^{\alpha+2}. \tag{1.2}$$

Here f_3 is a local newform, f_3' is an eigenvector for the character χ, and β_3^0 is the normalized local Waldspurger period integral, as in (4.2). The computation and proof for this formula will, however, be skipped for conciseness and simplicity in this paper and are intended for a separate publication, as they are treated in more general situations and have independent interest. Interested readers can see the complete preprint version [HSY17] of this paper for details.

Comparing this explicit Gross–Zagier fomula with the product formula (1.1) of full BSD conjectures for E_p and E_{3p^2}, Theorem 1.4 follows from the $\sqrt{-3}$-nondivisibility of Heegner points.

This paper is organized as follows. In Section 2, we give the construction of the Heegner points and study the Galois actions on the Heegner points via modular actions. In Section 3, we briefly recall the nontriviality of the Heegner points from [DV18] and study the 3-nondivisibility of the Heegner points. In Section 4, we establish the explicit Gross–Zagier formula for the Heegner points (Theorem 1.5). In Section 5, we prove Theorem 1.4 by comparing the explicit Gross–Zagier formula and the full BSD conjecture.

2. Modular actions on Heegner points

2.1. **The modular curves and modular actions.** Let X be an algebraic curve defined over $\mathbb{Q}$, and let F be a field extension of $\mathbb{Q}$. Denote by $\mathrm{Aut}_F(X)$ the group of algebraic automorphisms of X which are defined over F. Let

$$\mathcal{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$$

be the Poincaré upper half plane. The group $\mathrm{GL}_2(\mathbb{Q})^+$ acts on $\mathcal{H}$ by linear fractional transformations.

Let $U_0(3^5)$ be the open compact subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $c \equiv 0 \bmod 3^5$, and let $\Gamma_0(3^5) = \mathrm{GL}_2(\mathbb{Q})^+ \cap U_0(3^5)$. Let $X_0(3^5)$ be the modular curve over $\mathbb{Q}$ of level $\Gamma_0(3^5)$ whose underlying Riemann surface is

$$\begin{aligned} X_0(3^5)(\mathbb{C}) &= \mathrm{GL}_2(\mathbb{Q})^+ \backslash \left(\mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q})\right) \times \mathrm{GL}_2(\mathbb{A}_f)/U_0(3^5) \\ &\simeq \left(\Gamma_0(3^5)\backslash\mathcal{H}\right) \sqcup \left(\Gamma_0(3^5)\backslash\mathbb{P}^1(\mathbb{Q})\right), \end{aligned}$$

where $\mathbb{A}_f$ denote the finite adèle of $\mathbb{Q}$. Define N to be the normalizer of $\Gamma_0(3^5)$ in $\mathrm{GL}_2^+(\mathbb{Q})$. It follows from [KM88, Theorem 1] that the linear fractional transformation action of N on $X_0(3^5)$ induces an isomorphism

$$N/\mathbb{Q}^\times\Gamma_0(3^5) \simeq \mathrm{Aut}_{\overline{\mathbb{Q}}}(X_0(3^5)).$$

Moreover, all of the algebraic automorphisms in $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_0(3^5))$ are defined over K. We identify $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_0(3^5))$ with $N/\mathbb{Q}^\times\Gamma_0(3^5)$ by this isomorphism. By [AL70, Theorem 8], [Ogg80], the quotient group $N/\mathbb{Q}^\times\Gamma_0(3^5) \simeq S_3 \rtimes \mathbb{Z}/3\mathbb{Z}$, where S_3 denotes the symmetric group with three letters which is generated by the Atkin–Lehner operator $W = \left(\begin{smallmatrix} 0 & 1 \\ -3^5 & 0 \end{smallmatrix}\right)$ and the matrix $A = \left(\begin{smallmatrix} 28 & 1/3 \\ 3^4 & 1 \end{smallmatrix}\right)$, and the subgroup $\mathbb{Z}/3\mathbb{Z}$ is generated by the matrix $B = \left(\begin{smallmatrix} 1 & 0 \\ 3^4 & 1 \end{smallmatrix}\right)$.

Put

$$U = \langle U_0(3^5), W, A\rangle \subset \mathrm{GL}_2(\mathbb{A}_f).$$

Then $\mathbb{Q}^\times\backslash\mathbb{Q}^\times U$ is an open compact subgroup of $\mathbb{Q}^\times\backslash\mathrm{GL}_2(\mathbb{A}_f)$. Put

$$\Gamma = \mathrm{GL}_2(\mathbb{Q})^+ \cap U = \langle \Gamma_0(3^5), W, A\rangle,$$

and let X_Γ be the modular curve over $\mathbb{Q}$ of level Γ whose underlying Riemann surface is

$$X_\Gamma(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})^+\backslash\left(\mathcal{H}\sqcup\mathbb{P}^1(\mathbb{Q})\right)\times\mathrm{GL}_2(\mathbb{A}_f)/U \simeq (\Gamma\backslash\mathcal{H})\sqcup(\Gamma\backslash\mathbb{P}^1(\mathbb{Q})).$$

Then X_Γ is a smooth projective curve over $\mathbb{Q}$ of genus 1, and X_Γ has three cusps

$$\Gamma\backslash\mathbb{P}^1(\mathbb{Q}) = \{[\infty], [1/9], [2/9]\}.$$

The cusp $[\infty]$ is rational over $\mathbb{Q}$, and the cusps $[1/9]$ and $[2/9]$ are both defined over K. We identify X_Γ with an elliptic curve over $\mathbb{Q}$ with $[\infty]$ as its zero element. Let N_Γ be the normalizer of Γ in $\mathrm{GL}_2(\mathbb{Q})^+$. Then we have a natural embedding

$$\Phi : N_\Gamma/\mathbb{Q}^\times\Gamma \hookrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}}(X_\Gamma) \simeq \mathcal{O}_K^\times \ltimes X_\Gamma(\overline{\mathbb{Q}}),$$

where $\mathcal{O}_K^\times$ embeds into $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_\Gamma)$ by CMs and $X_\Gamma(\overline{\mathbb{Q}})$ embeds into $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_\Gamma)$ by translations. The matrices

$$B = \begin{pmatrix} 1 & 0 \\ 3^4 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 1/9 \\ -3^3 & -2 \end{pmatrix}$$

lie in N_Γ, and hence induce automorphisms of X_Γ.

The elliptic curves E_n are all endowed with CM by K, and we fix the CM $[\cdot] : \mathcal{O}_K \simeq \mathrm{End}_K(E_n)$ by $[-\omega](x, y) = (\omega x, -y)$. We will always take the simple Weierstrass equation $y^2 = x^3 - 2^4\cdot 3$ for the elliptic curve E_9, unless stated otherwise.

Proposition 2.1.

1. *The elliptic curve $(X_\Gamma, [\infty])$ is isomorphic to E_9 over $\mathbb{Q}$.*
2. *We have an embedding*

$$\Phi : N_\Gamma/\mathbb{Q}^\times\Gamma \hookrightarrow \mathcal{O}_K^\times \ltimes (\Gamma\backslash\mathbb{P}^1(\mathbb{Q})) \subset \mathrm{Aut}_{\overline{\mathbb{Q}}}(X_\Gamma).$$

Moreover, for any point $P \in X_\Gamma$, we have

$$\Phi(B)(P) = [\omega^2]P, \quad \Phi(C)(P) = [\omega^2]P + [1/9].$$

In particular, the automorphisms $\Phi(B)$ and $\Phi(C)$ are defined over K.

Note that there exists a unique isomorphism $X_\Gamma \to E_9$ over $\mathbb{Q}$ such that the cusp $[1/9]$ has coordinates $(0, 4\sqrt{-3})$. We use this isomorphism to identify X_Γ with E_9.

Proof. It is known from [DV18] that E_9 is the natural quotient of $X_0(3^5)$ by the finite group S_3. Since the automorphism group of the elliptic curve E_9 is isomorphic to $\mathcal{O}_K^\times$, we have

$$\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_\Gamma) \simeq \mathcal{O}_K^\times \ltimes X_\Gamma(\overline{\mathbb{Q}}).$$

Then for any $M \in N_\Gamma$ and $P \in X_\Gamma$, $\Phi(M)(P) = [\alpha]P + S$ for some $\alpha \in \mathcal{O}_K^\times, S \in X_\Gamma(\overline{\mathbb{Q}})$. Taking $P = [\infty]$, we see $S = \Phi(M)([\infty]) \in \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$. The formulae for $\Phi(B)$ and $\Phi(C)$ are taken from [DV18], which can also be verified numerically using SageMath. □

Let $V \subset U_0(3^5)$ be the subgroup consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a \equiv d \bmod 3$, and put $U_0 = \langle V, W, A\rangle$. Let X_Γ^0 be the modular curve over $\mathbb{Q}$ whose underlying Riemann surface is

$$X_\Gamma^0(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})^+ \backslash \left(\mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q})\right) \times \mathrm{GL}_2(\mathbb{A}_f)/U_0.$$

By class field theory, $\mathbb{Q}_+^\times \widehat{\mathbb{Z}}^\times / \mathbb{Q}_+^\times \det(U_0) \simeq \mathrm{Gal}(K/\mathbb{Q})$. Noting that $\mathrm{GL}_2(\mathbb{Q})^+ \cap U_0 = \Gamma$, we see that the modular curve X_Γ^0 is isomorphic to $X_\Gamma \times_{\mathbb{Q}} K$ as a curve over $\mathbb{Q}$ (see [Shi94, Chapter 6]). Usually, we denote by $[z, g]_{U_0}$ the point on X_Γ^0 which is represented by the pair (z, g), where $z \in \mathcal{H}$ and $g \in \mathrm{GL}_2(\mathbb{A}_f)$. The curve X_Γ^0 is not geometrically connected and has two connected components over $\mathbb{C}$. Put

$$U/U_0 = \langle \epsilon \rangle, \qquad \epsilon = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The nontrivial Galois action of $\mathrm{Gal}(K/\mathbb{Q})$ on X_Γ^0 is given by the right translation of ϵ on X_Γ^0. We have

$$\mathrm{Aut}_{\mathbb{Q}}(X_\Gamma^0) = \mathrm{Aut}_K(X_\Gamma) \rtimes \mathrm{Gal}(K/\mathbb{Q}) \simeq (X_\Gamma(K) \rtimes \mathcal{O}_K^\times) \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

Let $N_{\mathrm{GL}_2(\mathbb{A}_f)}(U_0)$ be the normalizer of U_0 in $\mathrm{GL}_2(\mathbb{A}_f)$. Then there is a natural homomorphism

$$N_{\mathrm{GL}_2(\mathbb{A}_f)}(U_0)/U_0 \longrightarrow \mathrm{Aut}_{\mathbb{Q}}(X_\Gamma^0)$$

induced by right translation on X_Γ^0: for $P = [z, g]_{U_0} \in X_\Gamma^0$ and $x \in N_{\mathrm{GL}_2(\mathbb{A}_f)}(U_0)$,

$$P \mapsto P^x = [z, gx]_{U_0}.$$

An element $g \in N_{\mathrm{GL}_2(\mathbb{A}_f)}(U_0)$ maps one component of X_Γ^0 onto the other if and only if it has image -1 under the composition of the following morphisms:

$$\mathrm{GL}_2(\mathbb{A}_f) = \mathrm{GL}_2(\mathbb{Q})^+ \mathrm{GL}_2(\widehat{\mathbb{Z}}) \xrightarrow{\det} \mathbb{Q}_+^\times \widehat{\mathbb{Z}}^\times \longrightarrow \mathbb{Z}_3^\times/(1 + 3\mathbb{Z}_3),$$

where $\widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ and the last morphism is trivial on $\mathbb{Q}_+^\times$, and, on $\widehat{\mathbb{Z}}^\times$, it is the projection from $\widehat{\mathbb{Z}}^\times$ to its 3-adic factor composed with $\bmod 3$.

2.2. **The modular actions on Heegner points.** Let $p \equiv 4, 7 \bmod 9$ be a rational prime number. Let $\rho : K \to \mathrm{M}_2(\mathbb{Q})$ be the normalized embedding with fixed point $\tau = (2p\omega - 9)/(9p\omega - 36) \in \mathcal{H}$; i.e., we have

$$\rho(t) \begin{pmatrix} \tau \\ 1 \end{pmatrix} = t \begin{pmatrix} \tau \\ 1 \end{pmatrix} \qquad \text{for any } t \in K.$$

Here it is matrix multiplication on the left-hand side and scalar multiplication on the right-hand side. Note that

$$\tau = M\omega, \qquad M = \begin{pmatrix} 2 & -1 \\ 9 & -4 \end{pmatrix} \begin{pmatrix} \frac{p}{9} & 0 \\ 0 & 1 \end{pmatrix}.$$

Then the embedding $\rho : K \to \mathrm{M}_2(\mathbb{Q})$ is explicitly given by

$$\rho(\omega) = M \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} M^{-1} = \begin{pmatrix} 2p + 8 + 36/p & -4p/9 - 2 - 9/p \\ 9p + 36 + 144/p & -2p - 9 - 36/p \end{pmatrix}.$$

Let $R_0(3^5)$ be the standard Eichler order of discriminant 3^5 in $\mathrm{M}_2(\mathbb{Q})$. For any integer $c \geq 1$, let $\mathcal{O}_c$ be the order of K of conductor c, and let H_c be the ring class

field of conductor c. Then $K \cap R_0(3^5) = \mathcal{O}_{9p}$. Let $\mathcal{O}_{K,3}$ be the completion of $\mathcal{O}_K$ at the unique place above 3. We have

$$\mathcal{O}_{K,3}^\times/\mathbb{Z}_3^\times(1+9\mathcal{O}_{K,3}) = \langle\omega_3\rangle \times \langle 1+3\omega_3\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

where ω_3 is the image of ω into $\mathcal{O}_{K,3}^\times$. Considered as elements in $\mathrm{GL}_2(\mathbb{A}_f)$ with other components 1, it is straightforward to verify that ω_3 and $1+3\omega_3$ normalize U_0, and hence we have an embedding

$$\mathcal{O}_{K,3}^\times/\mathbb{Z}_3^\times(1+9\mathcal{O}_{K,3}) \hookrightarrow \mathrm{Aut}_{\mathbb{Q}}(X_\Gamma^0).$$

If $p \equiv 7 \bmod 9$, it is straightforward to verify that the element

$$w = M\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}M^{-1} = \begin{pmatrix}-2p-17 & 4p/9+4\\ -9p-72 & 2p+17\end{pmatrix}$$

is a nontrivial normalizer of $K^\times$ in $\mathrm{GL}_2(\mathbb{Q})$ and $w\epsilon$ normalizes U_0, and hence $w\epsilon$ also induces an automorphism of X_Γ^0.

Theorem 2.2.

1. *For any point $P \in X_\Gamma^0$, we have*

$$P^{1+3\omega_3} = [\omega^2]P,$$

and

$$P^{\omega_3} = \begin{cases}[\omega^2]P + (0, 4\sqrt{-3}), & p \equiv 4 \bmod 9,\\ [\omega]P + (0, 4\sqrt{-3}), & p \equiv 7 \bmod 9.\end{cases}$$

2. *Suppose that $p \equiv 7 \bmod 9$. For any point $P \in X_\Gamma^0$, we have*

$$P^{w\epsilon} = [\omega^{\frac{p-7}{9}}]P - (0, 4\sqrt{-3}).$$

Proof. Since ω_3, $1+3\omega_3$, and $w\epsilon$ all have determinant $\equiv 1 \bmod 3$, when identified as elements in $\mathrm{Aut}_{\mathbb{Q}}(X_\Gamma^0)$, they actually lie in the subgroup $\mathrm{Aut}_K(X_\Gamma)$. Let $P = [z,1]_{U_0}$ for $z \in \mathcal{H}$ be a point on X_Γ^0. We have

$$B(1+3\omega_3)A^2 = \left(\begin{pmatrix}60p+837/p+214 & 2p/3+9/p+7/3\\ 5130p+71145/p+18252 & 57p+765/p+199\end{pmatrix}_3, BA^2\right) \in V,$$

where the subscript "3" denotes the 3-adic component of the adelic matrices. Then

$$P^{1+3\omega_3} = [z, 1+3\omega_3]_{U_0} = [B(z), B(1+3\omega_3)]_{U_0} = [B(z),1]_{U_0} = \Phi(B)P = [\omega^2]P.$$

If $p \equiv 4 \bmod 9$, then

$$C\omega_3A^2 = \left(\begin{pmatrix}867p+11635/p+2685 & 31p/3+416/3p+32\\ -20808p-281925/p-64440 & -248p-3360/p-768\end{pmatrix}_3, CA^2\right) \in V,$$

and hence

$$P^{\omega_3} = \Phi(C)(P) = [\omega^2]P + (0, 4\sqrt{-3}).$$

If $p \equiv 7 \bmod 9$, then

$$BC\omega_3A^2 = \left(\begin{pmatrix}867p+11635/p+2685 & 31p/3+416/3p+32\\ 49419p+660510/p+153045 & 589p+7872/p+1824\end{pmatrix}_3, BCA^2\right) \in V,$$

and hence

$$P^{\omega_3} = \Phi(BC)(P) = [\omega]P + (0, 4\sqrt{-3}).$$

Suppose that $p \equiv 7 \bmod 9$. It can verified that

$$\begin{cases} BC^2 w\epsilon A^2 \in V, & \dfrac{p-7}{9} \equiv 0 \bmod 3, \\ C^2 w\epsilon A^2 \in V, & \dfrac{p-7}{9} \equiv 1 \bmod 3, \\ B^2C^2 w\epsilon A^2 \in V, & \dfrac{p-7}{9} \equiv 2 \bmod 3. \end{cases}$$

Hence, the second assertion follows. □

Let $\sigma : \widehat{K}^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ be the Artin reciprocity law, and denote by σ_t the image of $t \in \widehat{K}^\times$. Let $P_0 = [\tau, 1]$ be the CM point on X_Γ^0.

Theorem 2.3.

1. *The point $P_0 \in X_\Gamma^0(H_{9p})$ satisfies*
$$P_0^{\sigma_{1+3\omega_3}} = [\omega^2]P_0$$
and
$$P_0^{\sigma_{\omega_3}} = \begin{cases} [\omega^2]P_0 + (0, 4\sqrt{-3}), & p \equiv 4 \bmod 9, \\ [\omega]P_0 + (0, 4\sqrt{-3}), & p \equiv 7 \bmod 9. \end{cases}$$
2. *Suppose that $p \equiv 7 \bmod 9$. We have*
$$\overline{P_0} = [\omega^{\frac{p-7}{9}}]P_0 - (0, 4\sqrt{-3}).$$

Proof. By Shimura's reciprocity law [Shi94, Theorems 6.31 and 6.38], we have

$$P_0^{\sigma_t} = P_0^t = [\tau, t], \qquad t \in \widehat{K}^\times.$$

Since $\widehat{K}^\times \cap U_0 = \widehat{\mathcal{O}_{9p}}^\times$, we see that P_0 is defined over the ring class field H_{9p}, and the Galois actions of σ_{ω_3} and $\sigma_{1+3\omega_3}$ are clear from Theorem 2.2. □

Proposition 2.4.

1. *We have $H_{9p} = H_{3p}(\sqrt[3]{3})$ with $\mathrm{Gal}(H_{9p}/H_{3p}) = \langle \sigma_{1+3\omega_3} \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, and*
$$\left(\sqrt[3]{3}\right)^{\sigma_{1+3\omega_3}-1} = \omega^2.$$
2. *We have $\left(\sqrt[3]{3}\right)^{\sigma_{\omega_3}-1} = 1$ and*
$$(\sqrt[3]{p})^{\sigma_{\omega_3}-1} = \begin{cases} \omega^2, & p \equiv 4 \bmod 9, \\ \omega, & p \equiv 7 \bmod 9. \end{cases}$$

Proof. For any place w of K, let K_w denote the completion of K at the place w, and let $\left(\frac{\cdot,\cdot}{K_w;3}\right)$ be the third Hilbert symbol over K_w; see, for example, [Neu99, Chapter V, Section 3]. We have the decomposition of ideal $7\mathcal{O}_K = (1+3\omega)(1+3\omega^2)$. Let v be the place corresponding to the prime ideal $(1+3\omega)$. Then

$$\left(\sqrt[3]{3}\right)^{\sigma_{1+3\omega_3}-1} = \left(\frac{1+3\omega_3, 3}{K_3; 3}\right).$$

It is an important property of the Hilbert symbol that

$$\prod_w \left(\frac{1+3\omega_w, 3}{K_w; 3}\right) = 1,$$

where ω_w denotes the image of ω in K_w and w runs through all places of K. Since the symbol is trivial whenever $w \neq 3, v$, we have by [Neu99, Chapter V, Proposition 3.4] that

$$\left(\sqrt[3]{3}\right)^{\sigma_{1+3\omega_3}-1} = \left(\frac{1+3\omega_3, 3}{K_3; 3}\right) = \left(\frac{1+3\omega_v, 3}{K_v; 3}\right)^{-1} = 3^{-2} \bmod (1+3\omega) = \omega^2.$$

Since $p \equiv 1 \bmod 3$, the prime p splits in K. Let v and $\overline{v}$ be the two places of K above p. Then similarly,

$$(\sqrt[3]{p})^{\sigma_{\omega_3}-1} = \left(\frac{\omega_3, p}{K_3; 3}\right) = \left(\frac{\omega_v, p}{K_v; 3}\right)^{-1} \cdot \left(\frac{\omega_{\overline{v}}, p}{K_{\overline{v}}; 3}\right)^{-1} = \omega^{-\frac{p-1}{3}}. \qquad \square$$

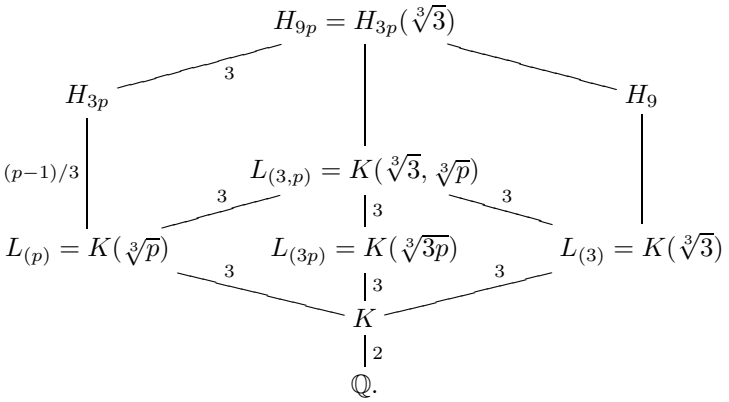
The elliptic curve E_1 has Weierstrass equation $y^2 = x^3 - 432$. Consider the isomorphism

$$\phi : E_9 \longrightarrow E_1, \qquad (x, y) \mapsto ((\sqrt[3]{3})^2 x, 3y).$$

We have the following commutative diagram:

$$\begin{array}{ccc} E_9(H_{9p})^{\sigma_{1+3\omega_3}=\omega^2} & \xrightarrow{\mathrm{Tr}_{H_{9p}/L_{(3,p)}}} & E_9(L_{(3,p)})^{\sigma_{1+3\omega_3}=\omega^2} \\ \downarrow \phi & & \downarrow \phi \\ E_1(H_{3p}) & \xrightarrow{\mathrm{Tr}_{H_{3p}/L_{(p)}}} & E_1(L_{(p)}), \end{array}$$

where the field extension diagram is as follows:



Put $Q = \phi(P_0)$ and $R = \mathrm{Tr}_{H_{3p}/L_{(p)}} Q$.

Corollary 2.5. *The point $R \in E_1(L_{(p)})$ and satisfies*

$$R^{\sigma_{\omega_3}} = \begin{cases} [\omega^2]R + (0, 12\sqrt{-3}), & p \equiv 4 \bmod 9, \\ [\omega]R + (0, -12\sqrt{-3}), & p \equiv 7 \bmod 9, \end{cases}$$

and if $p \equiv 7 \bmod 9$,

$$\overline{R} = [\omega^{\frac{p-7}{9}}]R + (0, 12\sqrt{-3}).$$

Proof. This is a consequence of Theorem 2.3, Proposition 2.4, and the fact that

$$\mathrm{Tr}_{H_{3p}/L_{(p)}}(0, 12\sqrt{-3}) = \frac{p-1}{3}(0, 12\sqrt{-3}).$$

Recall that the cusp $(0, 12\sqrt{-3})$ is a 3-torsion. $\square$

3. Nondivisibility of Heegner points

By the assumption that 3 mod p is not a cubic residue, we decompose $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ so that

$$3^{\frac{p-1}{3}} \equiv \omega \bmod \mathfrak{p}, \qquad 3^{\frac{p-1}{3}} \equiv \omega^2 \bmod \overline{\mathfrak{p}}. \tag{3.1}$$

Since H_{3p}/K is totally ramified at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, let $\mathfrak{P}$ and $\overline{\mathfrak{P}}$ be the primes of H_{3p} above $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, respectively. We have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p} \bigoplus \mathcal{O}_K/\overline{\mathfrak{p}} \subset \mathcal{O}_{H_{3p}}/\mathfrak{P} \bigoplus \mathcal{O}_{H_{3p}}/\overline{\mathfrak{P}}.$$

The main result (Proposition 5.2.8) in [DV18] states that if 3 is not a cube modulo p, the reduction

$$(R \bmod \mathfrak{P}, R \bmod \overline{\mathfrak{P}}) \in E_1(\mathbb{F}_p)^2$$

is not equal to the image of any torsion point in $E_1(L_{(p)})$, and hence the Heegner point R is of infinite order.

We sketch their strategy briefly. Note that the CM points P_0 considered in this paper are exactly those considered in [DV18]. We will use the explicit coordinates of R modulo p later, so we record them in the following lemma.

Lemma 3.1. *Under the Weierstrass equation $y^2 = x^3 - 432$ for E_1,*

$$R \equiv \begin{cases} (12\omega^{i+2}, -36) \bmod \mathfrak{P}, \\ (12\omega^{i+1}, -36) \bmod \overline{\mathfrak{P}}, \end{cases}$$

where $i = 0, 1, 2$ depends on p.

Proof. As in the proof of [DV18, Proposition 5.2.8],

$$R = \mathrm{Tr}_{H_{3p}/L_{(p)}} Q \equiv \frac{p-1}{3} Q \equiv \begin{cases} Q, & p \equiv 4 \bmod 9, \\ -Q, & p \equiv 7 \bmod 9. \end{cases} \tag{3.2}$$

By [DV18, Proposition 5.2.1 and Lemma 5.2.4], the x-coordinate $x(Q)$ is p-adic integral and satisfies the following congruence (see [DV18, (5.2.6)]):

$$x(Q) \equiv x(Q)^p \equiv 12^p \omega^i (-3)^{(p-1)/6} \bmod p\overline{\mathbb{Z}}, \tag{3.3}$$

where $\overline{\mathbb{Z}}$ denotes the ring of integral algebraic numbers and $i = 0, 1, 2$ depends on p (see [DV18, Lemma 5.1.3]). Note that Dasgupta and Voight [DV18] used the Weierstrass equation $y^2 + y = 3x^3 - 1$ for E_1, and we have adapted the coordinates to the equation $y^2 = x^3 - 432$. Since $-3 \in \mathbb{F}_p^\times$ is a square, $(-3)^{\frac{p-1}{6}}$ is a third root of unity modulo p. Note also that $\frac{p-1}{3}$ is always even in our case. Therefore, by (3.1) and (3.3), we conclude that

$$x(Q) \equiv \begin{cases} 12\omega^{i+2} \bmod \mathfrak{P}, \\ 12\omega^{i+1} \bmod \overline{\mathfrak{P}}. \end{cases} \tag{3.4}$$

By Theorem 2.3, we have

$$[1 - \omega^\alpha]Q \equiv (0, 12\sqrt{-3}) \bmod \mathfrak{P} \qquad (\text{resp., } \overline{\mathfrak{P}}),$$

where $\alpha = 2$ if $p \equiv 4 \bmod 9$, and $\alpha = 1$ if $p \equiv 7 \bmod 9$. This implies that $(Q \bmod \mathfrak{P})$ and $(Q \bmod \overline{\mathfrak{P}})$ both belong to $E_1(\mathbb{F}_p)[3]$. It follows that

$$Q \equiv \begin{cases} (12\omega^{i+2}, (-1)^{\alpha-1} \cdot 36) \bmod \mathfrak{P}, \\ (12\omega^{i+1}, (-1)^{\alpha-1} \cdot 36) \bmod \overline{\mathfrak{P}}. \end{cases} \tag{3.5}$$

Then the lemma follows from (3.2) and (3.5). □

Consider the reduction map

$$\mathrm{Red} : E_1(L_{(p)})\backslash\{O\} \longrightarrow \mathcal{O}_{H_{3p}}/\mathfrak{P} \bigoplus \mathcal{O}_{H_{3p}}/\overline{\mathfrak{P}}, \quad T \mapsto (x(T) \bmod \mathfrak{P}, x(T) \bmod \overline{\mathfrak{P}}).$$

By [DV18, Lemma 5.2.9], we have $E_1(L_{(p)})_{\mathrm{tor}} = E_1(K)_{\mathrm{tor}}$. Let D be the image of $E_1(L_{(p)})_{\mathrm{tor}}\backslash\{O\}$ under the reduction map. Then

$$D = \{(0,0), (12\omega^i, 12\omega^i)_{i=0,1,2}\} \subset \mathcal{O}_K/\mathfrak{p} \bigoplus \mathcal{O}_K/\overline{\mathfrak{p}}.$$

On the other hand, by Lemma 3.1, the reduction $\mathrm{Red}(R)$ is not trivial and also does not lie in D. Hence, the Heegner point R is not torsion.

Put $T = (12\omega^{i+2}, -36)$, which satisfies the relations

$$T = \begin{cases} [\omega^2]T + (0, 12\sqrt{-3}), \\ [\omega]T + (0, -12\sqrt{-3}). \end{cases}$$

Let $\alpha = 2$ or 1, according to $p \equiv 4$ or $7 \bmod 9$, respectively. By Theorem 2.5, the point $Y = R - T$ belongs to $E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha}$, which is identified with $E_p(K)$ under the isomorphism $(x, y) \mapsto ((\sqrt[3]{p})^2 x, py)$ defined over $L_{(p)}$. Then the point $Y + \overline{Y}$ is identified with an element in $E_p(\mathbb{Q})$.

Proposition 3.2. *The point Y is not divisible by $\sqrt{-3}$ in $E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha}$. More precisely, there exists no point $X \in E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha}$ and $S \in E_1(L_{(p)})_{\mathrm{tor}}^{\sigma_{\omega_3}=\omega^\alpha}$ such that*

$$Y = \sqrt{-3}X + S.$$

Proof. Suppose that

$$Y = \sqrt{-3}X + S \tag{3.6}$$

for some $X \in E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha}$ and $S \in E_1(L_{(p)})_{\mathrm{tor}}^{\sigma_{\omega_3}=\omega^\alpha}$. Since H_{3p}/K is totally ramified at $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, we have

$$Y^{\sigma_{\omega_3}} \equiv Y,\ X^{\sigma_{\omega_3}} \equiv X,\ S^{\sigma_{\omega_3}} \equiv S \bmod \mathfrak{P} \text{ (resp., } \bmod \overline{\mathfrak{P}}).$$

From the formulae

$$Y^{\sigma_{\omega_3}} = [\omega^\alpha]Y, \quad X^{\sigma_{\omega_3}} = [\omega^\alpha]X, \quad S^{\sigma_{\omega_3}} = [\omega^\alpha]S,$$

we have

$$[\sqrt{-3}]Y = [\sqrt{-3}]X = [\sqrt{-3}]S \equiv O \bmod \mathfrak{P} \text{ (resp., } \bmod \overline{\mathfrak{P}}).$$

By (3.6) and our choice of T, we have

$$S \equiv Y \equiv \begin{cases} O, & \bmod \mathfrak{P}, \\ [1-\omega](12\omega^{i+1}, -36), & \bmod \overline{\mathfrak{P}}, \end{cases}$$

which implies that $(x(S) \bmod \mathfrak{P}, x(S) \bmod \overline{\mathfrak{P}})$ does not lie in the subset D, and this contradicts the fact that S is a torsion point. This proves that Y is not divisible by $\sqrt{-3}$ in $E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha}$. □

By the work of Dasgupta and Voight [DV18], we know that the free component of $E_p(K)$ has rank 1 over $\mathcal{O}_K$, and we have

$$K \otimes_{\mathcal{O}_K} E_p(K) \simeq K.$$

Proposition 3.3. *As elements in $K \otimes_{\mathcal{O}_K} E_p(K)$, we have*

$$\overline{Y} = \left(\omega^i \frac{\gamma}{\overline{\gamma}}\right) \otimes Y,$$

where $i = 0, 1, 2$, $\gamma \in \mathcal{O}_K$ is a nonzero element satisfying $(\overline{\gamma}, \gamma) = 1$, and all primes of γ are factors of rational primes which are split in K.

Proof. Recall that if we set $\alpha = 2$ or 1 according to $p \equiv 4$ or 7 mod 9, respectively, then $E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha}$ is identified with $E_p(K)$ under the real morphism

$$\varphi : E_1 \to E_p, \qquad (x, y) \mapsto ((\sqrt[3]{p})^2 x, py).$$

Since R and $\overline{R}$ have the same height, as elements in

$$K \otimes_{\mathcal{O}_K} E_1(L_{(p)})^{\sigma_{\omega_3}=\omega^\alpha},$$

there exists a $\beta \in K^\times$ such that

$$\mathrm{N}_{K/\mathbb{Q}}(\beta) = 1$$

and

$$\overline{R} = \beta \otimes R.$$

By Hilbert satz 90, we may assume that

$$\beta = u \cdot \frac{\gamma}{\bar{\gamma}},$$

where $u \in \mathcal{O}_K^\times$, $\gamma \in \mathcal{O}_K$ such that $(\overline{\gamma}, \gamma) = 1$, and all primes of γ are factors of rational primes which are split in K.

Then as usual points, there exists an $S \in E_1(L_{(p)})_{\mathrm{tor}}^{\sigma_{\omega_3}=\omega^\alpha} = E_1(K)_{\mathrm{tor}}$ such that

$$\overline{[\gamma]R} = [u\gamma]R + S.$$

Since $Y = \varphi(R - T)$, we have

$$\overline{[\gamma]Y} = [u\gamma]Y + S'$$

for some $S' \in E_p(K)_{\mathrm{tor}}$.

It remains to prove that u is a third root of unity. We have

$$\overline{[\gamma]R} + [\gamma]R = [(u+1)\gamma]R + S. \tag{3.7}$$

We claim that if u is a primitive sixth root of unity or -1, then $[(u+1)\gamma]R$ has the same coordinates modulo both $\mathfrak{P}$ and $\overline{\mathfrak{P}}$. The case $u = -1$ is obvious. Suppose that u is a primitive sixth root of unity. Then $u + 1 = \sqrt{-3}\omega^j$ for some $j = 1, 2$. By Lemma 3.1, we have

$$[u+1]R \equiv \begin{cases} [\omega^{j+i+2}][\sqrt{-3}](12, -36) \bmod \mathfrak{P}, \\ [\omega^{j+i+1}][\sqrt{-3}](12, -36) \bmod \overline{\mathfrak{P}}. \end{cases}$$

Since $[\sqrt{-3}](12, -36) = (0, -12\sqrt{-3})$, we see that $[u+1]R$ has the same coordinates when modulo both $\mathfrak{P}$ and $\overline{\mathfrak{P}}$; consequently, so does $[\gamma(1+u)]R$. Since S is a K-point, the right-hand side (RHS) of (3.7) has the same coordinates when modulo both $\mathfrak{P}$ and $\overline{\mathfrak{P}}$.

On the other hand, we will show that the left-hand side (LHS) of (3.7) has distinct coordinates when modulo $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, respectively. To do this, it is enough to show

that $\overline{[2\gamma]R} + [2\gamma]R$ has distinct coordinates when modulo $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, respectively. Write $2\gamma = a + b\sqrt{-3}$, with $a, b \in \mathbb{Z}$. Then

$$\overline{[2\gamma]R} + [2\gamma]R = [a](R + \overline{R}) + [b\sqrt{-3}](R - \overline{R}).$$

By Lemma 3.1, $R+\overline{R}$ has distinct coordinates when modulo $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, respectively, and $R - \overline{R} \equiv [1-\omega^i]R$ for some $i = 0, 1, 2$ when modulo $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, respectively.

Note that R mod $\mathfrak{P}$ (resp., $\overline{\mathfrak{P}}$) is of order 3 in $E_1(\mathbb{F}_p)$. Since $a \equiv 1, 2 \bmod 3$, we know that $[a](R+\overline{R})$ has distinct coordinates when modulo $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, respectively. Since $\sqrt{-3} \mid (1-\omega^i)$, we conclude that

$$[b\sqrt{-3}](R - \overline{R}) \equiv 0 \bmod \mathfrak{P} \text{ (resp., } \overline{\mathfrak{P}}).$$

So we conclude that that $\overline{[2\gamma]R}+[2\gamma]R$, and hence the LHS of (3.7), has distinct coordinates when modulo $\mathfrak{P}$ and $\overline{\mathfrak{P}}$, respectively. Therefore, if u is a primitive sixth root of unity or -1, we come to a contradiction, and hence u must be a third root of unity. □

Remark 3.4. If $p \equiv 7 \bmod 9$, it follows from Corollary 2.5 that

$$\overline{Y} \equiv [\omega^{\frac{p-7}{9}}]Y \bmod \text{torsion}.$$

Theorem 3.5. *The point $Y + \overline{Y} \in E_p(\mathbb{Q})$ is not divisible by* 3.

Proof. In the following, all points are viewed as elements in

$$K \otimes_{\mathcal{O}_K} E_p(K) \simeq K.$$

By Proposition 3.3, there exists a $\gamma \in \mathcal{O}_K$ satisfying $(\overline{\gamma}, \gamma) = 1$, and all primes of γ are factors of rational primes which are split in K such that

$$Y + \overline{Y} = \left(1 + u\frac{\gamma}{\overline{\gamma}}\right) \otimes Y.$$

Consider $\gamma + \overline{\gamma}$ as an element in $\mathcal{O}_{K,3} = \mathbb{Z}_3[\sqrt{-3}]$. Suppose that $\gamma = a + b\sqrt{-3}$, with $a, b \in \mathbb{Z}_3$. Since γ is a 3-adic unit, we have $a \in \mathbb{Z}_3^\times$. Then

$$1 + u\frac{\gamma}{\overline{\gamma}} = 1 + \frac{\gamma}{\overline{\gamma}} + (u-1)\frac{\gamma}{\overline{\gamma}} = \frac{2a}{\gamma} + (u-1)\frac{\gamma}{\overline{\gamma}}$$

is a 3-adic unit since $\sqrt{-3} \mid (u-1)$. Then the 3-nondivisibility follows from Proposition 3.2. □

4. The explicit Gross–Zagier formulae

4.1. **Test vectors and the explicit Gross–Zagier formulae.** Let π be the automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ corresponding to $E_{9/\mathbb{Q}}$. Then π is only ramified at 3 with conductor 3^5. For $n \in \mathbb{Q}^\times$, let $\chi_n : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathbb{C}^\times$ be the cubic character given by $\chi_n(\sigma) = (\sqrt[3]{n})^{\sigma-1}$. Define

$$L(s, E_9, \chi_n) := L(s - 1/2, \pi_K \otimes \chi_n), \qquad \epsilon(E_9, \chi_n) := \epsilon(1/2, \pi_K \otimes \chi_n),$$

where π_K is the base change of π to $\mathrm{GL}_2(\mathbb{A}_K)$.

Let $p \equiv 4, 7 \bmod 9$ be a prime number, and put $\chi = \chi_{3p}$. From the Artin formalism, we have

$$L(s, E_9, \chi) = L(s, E_p)L(s, E_{3p^2}).$$

By [Liv95], we have the epsilon factors $\epsilon(E_{3p^2}) = +1$ and $\epsilon(E_p) = -1$, and hence the epsilon factor

$$\epsilon(E_9, \chi) = \epsilon(E_p)\epsilon(E_{3p^2}) = -1.$$

For a quaternion algebra $\mathbb{B}_{\mathbb{A}}$, we define its ramification index $\epsilon(\mathbb{B}_v) = +1$ for any place v of $\mathbb{Q}$ if the local component $\mathbb{B}_v$ is split, and $\epsilon(\mathbb{B}_v) = -1$ otherwise.

Proposition 4.1. *The incoherent quaternion algebra $\mathbb{B}$ over $\mathbb{A}$, which satisfies*

$$\epsilon(1/2, \pi_v, \chi_v) = \chi_v(-1)\epsilon_v(\mathbb{B})$$

for all places v of $\mathbb{Q}$, is ramified only at the infinity place.

Proof. Since π is unramified at finite places $v \nmid 3$, χ is unramified at finite places $v \nmid 3p$, and p is split in K, by [Gro88, Proposition 6.3], we get $\epsilon(1/2, \pi_v, \chi_v) = +1$ for all finite $v \neq 3$. Again by [Gro88, Proposition 6.5], we also know that $\epsilon(1/2, \pi_\infty, \chi_\infty) = -1$. Since $\epsilon(1/2, \pi, \chi) = -1$, we see that $\epsilon(1/2, \pi_3, \chi_3) = +1$. Since χ is a cubic character, $\chi_v(-1) = 1$ for any v. Hence, $\mathbb{B}$ is ramified only at the infinity place. □

Let $\mathbb{B}_f^\times = \mathrm{GL}_2(\mathbb{A}_f)$ be the finite part of $\mathbb{B}^\times$. For any open compact subgroup $U \subset \mathbb{B}_f^\times$, the Shimura curve X_U associated with $\mathbb{B}$ of level U is the usual modular curve with complex uniformization

$$X_U(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})^+ \backslash \left(\mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q})\right) \times \mathrm{GL}_2(\mathbb{A}_f)/U.$$

Let

$$\pi_{E_9} = \varinjlim_U \mathrm{Hom}^0_{\xi_U}(X_U, E_9),$$

where $\mathrm{Hom}^0_{\xi_U}(X_U, E_9)$ denotes the morphisms in $\mathrm{Hom}_{\mathbb{Q}}(X_U, E_9) \otimes_{\mathbb{Z}} \mathbb{Q}$ using the Hodge class ξ_U as a base point. Then π_{E_9} is an automorphic representation of $\mathbb{B}^\times$ over $\mathbb{Q}$. Let π be the Jacquet–Langlands correspondence of $\pi_{E_9} \otimes_{\mathbb{Q}} \mathbb{C}$ on $\mathrm{GL}_2(\mathbb{A})$. By Proposition 4.1 and a theorem of Tunnell and Saito [YZZ13, Theorem 1.4.1], the space

$$\mathrm{Hom}_{\mathbb{A}_K^\times}(\pi_{E_9} \otimes \chi, \mathbb{C}) \otimes \mathrm{Hom}_{\mathbb{A}_K^\times}(\pi_{E_9} \otimes \chi^{-1}, \mathbb{C})$$

is one dimensional with a generator $\beta = \otimes\beta_v$ where, for each place v of $\mathbb{Q}$, the bilinear form

$$\beta_v : \pi_{E_9,v} \otimes \pi_{E_{9,v}} \longrightarrow \mathbb{C}$$

is given by

$$\beta_v(\varphi_1, \varphi_2) = \int_{\mathbb{Q}_v^\times \backslash K_v^\times} (\pi_{E_9,v}(t)\varphi_1, \varphi_2)\chi_v(t)dt, \qquad \varphi_1, \varphi_2 \in \pi_{E_9,v}. \tag{4.1}$$

Here $(\cdot,\cdot)_v$ is a $\mathbb{B}_v^\times$-invariant pairing on $\pi_{E_9,v} \times \pi_{E_9,v}$, and dt is a Haar measure on $K_v^\times/\mathbb{Q}_v^\times$. For later application of the explicit Gross–Zagier formula in [CST14], if $(\varphi_1, \varphi_2)_v \neq 0$, we also define the normalized toric integral

$$\beta_v^0(\varphi_1, \varphi_2) = \int_{\mathbb{Q}_v^\times \backslash K_v^\times} \frac{(\pi(t)\varphi_1, \varphi_2)_v \chi_v(t)}{(\varphi_1, \varphi_2)_v} dt. \tag{4.2}$$

For more details, we refer the reader to [YZZ13, Section 1.4], [CST14, Section 3].

The elliptic curve E_9 has conductor 3^5. Let $f : X_0(3^5) \to E_9$ be a nontrivial modular parametrization which sends the infinity cusp $[\infty]$ to the zero element

O. Explicitly, we may take f to be the quotient map $X_0(3^5) \to X_\Gamma = E_9$, as in Proposition 2.1. Let

$$\mathcal{R} = \begin{pmatrix} \widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \\ 3^5 \cdot \widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \end{pmatrix} \subset \mathbb{B}_f(\widehat{\mathbb{Z}}) = \mathrm{M}_2(\widehat{\mathbb{Z}})$$

be the Eichler order of discriminant 3^5. Then $U_0(3^5) = \mathcal{R}^\times$, and by the newform theory [Cas73], the invariant subspace $\pi_{E_9}^{\mathcal{R}^\times}$ has dimension 1 and is generated by f.

Proposition 4.2. *The modular parametrization $f : X_0(3^5) \to E_9$ is a test vector for the pair (π_{E_9}, χ), i.e., $\beta(f, f) \neq 0$.*

Proof. Let $\mathcal{R}'$ be the admissible order for the pair (π_{E_9}, χ) in the sense of [CST14, Definition 1.3]. Since $\mathcal{R}'$ and $\mathcal{R}$ differs only at 3, it suffices to verify that $\beta_3(f_3, f_3) \neq 0$, which is given by [HSY17, Corollary 7.10]. □

Let ω_{E_n} be the invariant differential on the minimal model of E_n. Define the minimal real period Ω_n of E_n by

$$\Omega_n = \int_{E_n(\mathbb{R})} |\omega_{E_n}|.$$

By [ZK87, Formula (9)], we have

$$\Omega_p \Omega_{3p^2} = (3p)^{-1} \Omega_9^2. \tag{4.3}$$

Using SageMath, we compute that $\{\Omega_9, \Omega_9 \cdot (\frac{1}{2} + \frac{\sqrt{-3}}{2})\}$ is a $\mathbb{Z}$-basis of the period lattice L of the minimal model of E_9. So

$$\sqrt{3}\Omega_9^2 = 2 \int_{\mathbb{C}/L} dxdy = \int_{E(\mathbb{C})} |\omega_{E_9} \wedge \overline{\omega}_{E_9}| = \frac{1}{6} \cdot 8\pi^2 (\phi, \phi)_{\Gamma_0(3^5)}, \tag{4.4}$$

where ϕ is the newform of level 3^5 and weight 2 associated with E_9, and $(\phi, \phi)_{\Gamma_0(3^5)}$ is the Petersson norm of ϕ defined by

$$(\phi, \phi)_{\Gamma_0(3^5)} = \int \int_{X_0(3^5)} |\phi(z)|^2 dxdy, \qquad z = x + iy.$$

Recall $\tau = (2p\omega - 9)/(9p\omega - 36) \in \mathcal{H}$, let $P_1 = [\tau, 1]_{U_0(3^5)}$ be the CM point on $X_0(3^5)(H_{9p})$, and note that $f(P_1) = P_0$. Define the Heegner point

$$R_1 = \mathrm{Tr}_{H_{9p}/L_{(3,p)}} P_0 \in E_9(L_{(3,p)}).$$

Theorem 4.3. *For primes $p \equiv 4, 7 \bmod 9$, we have the following explicit formula of Heegner points:*

$$\frac{L'(1, E_p) L(1, E_{3p^2})}{\Omega_p \Omega_{3p^2}} = 2^\alpha \cdot 9 \cdot \widehat{h}_{\mathbb{Q}}(R_1),$$

where $\alpha = 0$ if $p \equiv 4 \bmod 9$, and $\alpha = -1$ if $p \equiv 7 \bmod 9$.

Proof. We note that the conductor of π is 3^5 and the conductor of χ is $9p$. Let $\mathcal{R}'$ be the admissible order for the pair (π_{E_9}, χ), and let $f' \neq 0$ be a test vector in $V(\pi_{E_9}, \chi)$ which is defined in [CST14, Definition 1.4]. The newform f differs from f' only at the local place 3. Define the Heegner cycle

$$P_\chi^0(f) = \frac{\sharp \mathrm{Pic}(\mathcal{O}_p)}{\mathrm{Vol}(\widehat{K}^\times / K^\times \widehat{\mathbb{Q}}^\times, dt)} \int_{K^\times \widehat{\mathbb{Q}}^\times \backslash \widehat{K}^\times} f(P_1)^{\sigma_t} \chi(t) dt,$$

and define $P^0_{\chi^{-1}}(f)$ as in [CST14, Theorem 1.6]. According to [HSY17, Corollary 7.10], we have

$$\frac{\beta_3^0(f_3', f_3')}{\beta_3^0(f_3, f_3)} = 2^{\alpha+2},$$

where $\alpha = 0$ if $p \equiv 4 \bmod 9$, and $\alpha = -1$ if $p \equiv 7 \bmod 9$. By [CST14, Theorem 1.6], we have

$$L^{(3)'}(1, E_9, \chi) = 2^{\alpha+1} \cdot \frac{(8\pi^2) \cdot (\phi, \phi)_{\Gamma_0(3^5)}}{\sqrt{3}p \cdot (f, f)_{\mathcal{R}'}} \cdot \left\langle P^0_\chi(f), P^0_{\chi^{-1}}(f) \right\rangle_{K,K},$$

where $L^{(3)}$ denotes the partial L-function with the 3-adic local factor removed, $(\cdot,\cdot)_{\mathcal{R}'}$ is the pairing on $\pi_{E_9} \times \pi_{E_9{}^\vee}$ defined as in [CST14, page 789], and $\langle \cdot, \cdot \rangle_{K,K}$ is a pairing from $E_9(\overline{K})_{\mathbb{Q}} \times_K E_9(\overline{K})_{\mathbb{Q}}$ to $\mathbb{C}$ such that $\langle \cdot, \cdot \rangle_K = \mathrm{Tr}_{\mathbb{C}/\mathbb{R}} \langle \cdot, \cdot \rangle_{\mathrm{N}}$ is the Néron–Tate height over the base field K; see [CST14, page 790]. The local representation $\pi_{K,3} \otimes \chi_3$ is the principal series induced from the pair $(\Theta_3\chi_3, \overline{\Theta_3}\chi_3)$, where Θ is the Hecke character over K associated with E_9 via the CM theory. By [HSY17, Lemma 7.5], [HSY17, Lemma 7.6], the characters $\Theta_3\chi_3, \overline{\Theta_3}\chi_3$ are both ramified. Hence, the 3-adic local L-factor of $L(s, E_9, \chi)$ is trivial, and we have

$$L'(1, E_9, \chi) = L^{(3)'}(1, E_9, \chi).$$

In our case, by [CST14, Lemmas 2.2 and 3.5],

$$(f, f)_{\mathcal{R}'} = \frac{\mathrm{Vol}(X_{\mathcal{R}'^\times})}{\mathrm{Vol}(X_{\mathcal{R}^\times})} \deg f = 6 \cdot \frac{\mathrm{Vol}(\mathcal{R}^\times)}{\mathrm{Vol}(\mathcal{R}'^\times)} = 4.$$

So we get

$$L'(1, E_9, \chi) = 2^{\alpha-1} \frac{(8\pi^2) \cdot (\phi, \phi)_{\Gamma_0(3^5)}}{\sqrt{3p^2}} \cdot \left\langle P^0_\chi(f), P^0_{\chi^{-1}}(f) \right\rangle_{K,K}. \tag{4.5}$$

On the other hand,

$$P^0_\chi(f) = \frac{\#\mathrm{Pic}(\mathcal{O}_p)}{\#\mathrm{Pic}(\mathcal{O}_{9p})} \sum_{t \in \mathrm{Pic}(\mathcal{O}_{9p})} f(P_1)^{\sigma_t} \chi(t).$$

Since

$$\frac{\#\mathrm{Pic}(\mathcal{O}_p)}{\#\mathrm{Pic}(\mathcal{O}_{9p})} = [K^\times \widehat{\mathcal{O}}_p^\times : K^\times \widehat{\mathcal{O}}_{9p}^\times]^{-1} = \frac{1}{9},$$

we have

$$P^0_\chi(f) = \frac{1}{9} \sum_{t \in \mathrm{Pic}(\mathcal{O}_{9p})} f(P_1)^{\sigma_t} \chi(t).$$

If we put

$$R_2 = \sum_{\sigma \in \mathrm{Gal}(H_{9p}/L_{(3p)})} f(P_1)^\sigma \chi(\sigma) = 3R_1 \in E_9(L_{(3p)}),$$

then

$$\begin{aligned} \langle P^0_\chi(f), P^0_{\chi^{-1}}(f) \rangle_{K,K} &= \frac{1}{9^2} \langle \sum_{\sigma \in \mathrm{Gal}(L_{(3p)}/K)} R_2^\sigma \chi(\sigma), \sum_{\sigma \in \mathrm{Gal}(L_{(3p)}/K)} R_2^\sigma \chi^{-1}(\sigma) \rangle_{K,K} \\ &= \frac{1}{27} \langle R_2, \sum_{\sigma \in \mathrm{Gal}(L_{(3p)}/K)} R_2^\sigma \chi^{-1}(\sigma) \rangle_{K,K} \end{aligned} \tag{4.6}$$

$$\begin{aligned}
&= \frac{1}{27}(\langle R_2, R_2\rangle_{K,K} + \chi^{-1}(\sigma')\langle R_2, R_2^{\sigma'}\rangle_{K,K} \\
&\quad + \chi^{-1}(\sigma'^2)\langle R_2, R_2^{\sigma'^2}\rangle_{K,K}) \qquad (4.7)\\
&= \frac{1}{27}\left(\langle R_2, R_2\rangle_{K,K} - \left\langle R_2, R_2^{\sigma'}\right\rangle_{K,K}\right),
\end{aligned}$$

where σ' is a generator of $\mathrm{Gal}(L_{(3p)}/K)$. In the last equality, we use the fact that $\langle R_2, R_2^{\sigma'}\rangle_{K,K} = \langle R_2, R_2^{\sigma'^2}\rangle_{K,K}$ since $\langle , \rangle_{K,K}$ is symmetric and Galois invariant. By Theorem 2.3 and Corollary 2.5, we can assume that $R_2^{\sigma'} = [\omega]R_2$. Then

$$\left\langle R_2, R_2^{\sigma'}\right\rangle_{K,K} = \frac{1}{2}\left(\widehat{h}_K([1+\omega]R_2) - \widehat{h}_K([\omega]R_2) - \widehat{h}_K(R_2)\right).$$

Since $|1+\omega| = |\omega| = 1$, by definition, $\widehat{h}_K([1+\omega]R_2) = \widehat{h}_K([\omega]R_2) = \widehat{h}_K(R_2)$. Then

$$\left\langle R_2, R_2^{\sigma'}\right\rangle_{K,K} = -\frac{1}{2}\widehat{h}_K(R_2),$$

and hence

$$\left\langle P_\chi^0(f), P_{\chi^{-1}}^0(f)\right\rangle_{K,K} = \frac{1}{18}\widehat{h}_K(R_2) = \frac{1}{9}\widehat{h}_{\mathbb{Q}}(R_2) = \widehat{h}_{\mathbb{Q}}(R_1). \qquad (4.8)$$

Finally, combining (4.3)–(4.8), we get

$$\frac{L'(1, E_p)L(1, E_{3p^2})}{\Omega_p\Omega_{3p^2}} = 2^\alpha \cdot 9 \cdot \widehat{h}_{\mathbb{Q}}(R_1). \qquad \square$$

Recall that there is an isomorphism

$$\phi : E_9 \longrightarrow E_1, \qquad (x, y) \mapsto \left(\left(\sqrt[3]{3}\right)^2 x, 3y\right),$$

and we have the following commutative diagram:

$$\begin{array}{ccc}
E_9(H_{9p})^{\sigma_{1+3\omega_3}=\omega^2} & \xrightarrow{\mathrm{Tr}_{H_{9p}/L_{(3,p)}}} & E_9(L_{(3,p)})^{\sigma_{1+3\omega_3}=\omega^2} \\
\downarrow \phi & & \downarrow \phi \\
E_1(H_{3p}) & \xrightarrow{\mathrm{Tr}_{H_{3p}/L_{(p)}}} & E_1(L_{(p)}).
\end{array}$$

In particular, we have $\phi(R_1) = R$, and hence the following.

Corollary 4.4. *For primes $p \equiv 4, 7 \bmod 9$, we have*

$$\frac{L'(1, E_p)L(1, E_{3p^2})}{\Omega_p\Omega_{3p^2}} = 2^\alpha \cdot 9 \cdot \widehat{h}_{\mathbb{Q}}(R),$$

where $\alpha = 0$ if $p \equiv 4 \bmod 9$, and $\alpha = -1$ if $p \equiv 7 \bmod 9$.

Proof. This is immediate from Theorem 4.3. $\square$

Recall that Dasgupta and Voight [DV18] proved that the Heegner point R is not torsion. By the above Gross–Zagier formula and the work of Kolyvagin [Kol90], we know that

$$\mathrm{rank}_{\mathbb{Z}} E_p(\mathbb{Q}) = \mathrm{ord}_{s=1} L(s, E_p) = 1, \qquad \mathrm{rank}_{\mathbb{Z}} E_{3p^2}(\mathbb{Q}) = \mathrm{ord}_{s=1} L(s, E_{3p^2}) = 0.$$

5. The 3-part of the BSD conjectures

Let F be a number field. Let $\phi : A \to A'$ be an isogeny of elliptic curves over F of degree m, and let ϕ' be its dual isogeny. The commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A[\phi] & \longrightarrow & A & \xrightarrow{\phi} & A' & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow{\scriptstyle \phi'} & & \\
0 & \longrightarrow & A[m] & \longrightarrow & A & \xrightarrow{[m]} & A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \| & & \\
0 & \longrightarrow & A'[\phi'] & \longrightarrow & A' & \xrightarrow{\phi'} & A & \longrightarrow & 0
\end{array}$$

induces the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & A'[\phi'](F)/\phi A[m](F) & \xrightarrow{=} & A'[\phi'](F)/\phi A[m](F) & \longrightarrow & 0 & & \\
 & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi'} & & \downarrow & & \\
0 & \longrightarrow & A'(F)/\phi A(F) & \longrightarrow & \mathrm{Sel}_\phi(A/F) & \longrightarrow & Ш(A/F)[\phi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi'} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A(F)/mA(F) & \longrightarrow & \mathrm{Sel}_m(A/F) & \longrightarrow & Ш(A/F)[m] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \\
0 & \longrightarrow & A(F)/\phi' A'(F) & \longrightarrow & \mathrm{Sel}_{\phi'}(A'/F) & \longrightarrow & Ш(A'/F)[\phi'] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & \mathrm{Sel}_{\phi'}(A'/F)/\phi\mathrm{Sel}_m(A/F) & \xrightarrow{\simeq} & Ш(A'/F)[\phi']/\phi Ш(A/F)[m] & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

From this diagram, we immediately have the following.

Lemma 5.1. *Let A, A' and ϕ, ϕ' be as above:*

$$|\mathrm{Sel}_m(A/F)| = \frac{|\mathrm{Sel}_\phi(A/F)||\mathrm{Sel}_{\phi'}(A'/F)|}{|A'[\phi'](F)/\phi A[m](F)||Ш(A'/F)[\phi']/\phi Ш(A/k)[m]|}.$$

Let n be a positive cube-free integer, and let E'_n be the elliptic curve given by the Weierstrass equation $y^2 = x^3 + (4n)^2$. Then there is a unique isogeny $\phi_n : E_n \to E'_n$ of degree 3 up to $[\pm 1]$, and denote ϕ'_n as its dual isogeny.

Proposition 5.2. *Let $p \equiv 4, 7 \bmod 9$ be primes such that $3 \bmod p$ is not a cubic residue. Then*

$$\dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_p(\mathbb{Q})) \le 1, \qquad \dim_{\mathbb{F}_3} \mathrm{Sel}_3(E_{3p^2}(\mathbb{Q})) = 0.$$

Proof. By [Sat86, Theorem 2.9], we know that

$$\mathrm{Sel}_{\phi_p}(E_p(\mathbb{Q})) = \mathrm{Sel}_{\phi'_p}(E'_p(\mathbb{Q})) = \mathbb{Z}/3\mathbb{Z}$$

and

$$\mathrm{Sel}_{\phi_{3p^2}}(E_{3p^2}(\mathbb{Q})) = \mathbb{Z}/3\mathbb{Z}, \qquad \mathrm{Sel}_{\phi'_{3p^2}}(E'_{3p^2}(\mathbb{Q})) = 0.$$

Note that $E_p[3](\mathbb{Q})$ and $E_{3p^2}[3](\mathbb{Q})$ are trivial and that $|E'_p[\phi'_p](\mathbb{Q})|=|E'_{3p^2}[\phi'_{3p^2}](\mathbb{Q})| = 3$. By Lemma 5.1, the proposition follows. □

Now we are ready to give the proof of Theorem 1.4.

Proof of Theorem 1.4. By [ZK87, Table 1], we know that $c_p(E_p) = 3$, $c_3(E_p) = 1$ or 2 depending on p congruent to 4 or 7 modulo 9, respectively, and that $c_\ell(E_p) = 1$ for primes $\ell \neq 3, p$, while $c_p(E_{3p^2}) = 3$, $c_\ell(E_{3p^2}) = 1$ for primes $\ell \neq p$.

Let P be the generator of the free part of $E_p(\mathbb{Q})$. Then the BSD conjecture predicts that

$$\frac{L'(1, E_p)}{\Omega_p} = 2^m \cdot 3 \cdot |Ш(E_p)| \cdot \widehat{h}_{\mathbb{Q}}(P),$$

where $m = 0$ if $p \equiv 4 \bmod 9$, and 1 if $p \equiv 7 \bmod 9$, and where

$$\frac{L(1, E_{3p^2})}{\Omega_{3p^2}} = 3 \cdot \left|Ш(E_{3p^2})\right|.$$

Combining these two, we get

$$\frac{L'(1, E_p)}{\Omega_p} \cdot \frac{L(1, E_{3p^2})}{\Omega_{3p^2}} = 2^m \cdot 9 \cdot |Ш(E_p)| \cdot |Ш(E_{3p^2})| \cdot \widehat{h}_{\mathbb{Q}}(P).$$

By Theorem 4.3 and Corollary 4.4, we expect that

$$|Ш(E_p)| \cdot |Ш(E_{3p^2})| = 2^i \frac{\widehat{h}_{\mathbb{Q}}(R)}{\widehat{h}_{\mathbb{Q}}(P)}, \tag{5.1}$$

where $i = 0$ (resp., $i = -2$) if $p \equiv 4 \bmod 9$ (resp., $p \equiv 7 \bmod 9$). Note that the RHS of (5.1) is a nonzero rational number.

By Proposition 5.2, with E_p being rank 1 and the exact sequence

$$0 \longrightarrow E(\mathbb{Q})/3E(\mathbb{Q}) \longrightarrow Sel_3(E(\mathbb{Q})) \longrightarrow Ш(E)[3] \longrightarrow 0\ ,$$

we know directly that

$$|Ш(E_p)[3^\infty]| = |Ш(E_{3p^2})[3^\infty]| = 1. \tag{5.2}$$

In order to prove the 3-part of (5.1), it suffices to prove that

$$\widehat{h}_{\mathbb{Q}}(P) = u\widehat{h}_{\mathbb{Q}}(R_1) = u\widehat{h}_{\mathbb{Q}}(R)$$

for some $u \in \mathbb{Z}_3^\times \cap \mathbb{Q}$. However, it follows from Proposition 3.2 and Theorem 3.5 that

$$\widehat{h}_{\mathbb{Q}}(P) = w\widehat{h}_{\mathbb{Q}}(\overline{Y} + Y) = w\widehat{h}_{\mathbb{Q}}(\overline{R} + R) = u\widehat{h}_{\mathbb{Q}}(R)$$

for some $u, w \in \mathbb{Z}_3^\times \cap \mathbb{Q}$, where the last equality follows from Lemma 3.3. Indeed, we note that a similar formula for the complex conjugation is valid for R in the proof of Lemma 3.3. □

Acknowledgments

The authors would like to thank Professor Ye Tian for useful conversations and encouragement. We also would like to thank John Voight and Samit Dasgupta, who sent their unpublished work and provided many useful discussions and much help. We also thank Li Cai, who provided many discussions about the matrix coefficients of supercuspidal representations, and Jianing Li, who provided much help on the SageMath systems. We would like to thank the referee for helpful advice which motivated us to improve the treatments for 3-nondivisibility of the Heegner points and treat the technical local period integrals in an independent paper.

References

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(N)$., Math. Ann. **185** (1970), 134–160.

[CST17] L. Cai, J. Shu, and Y. Tian, *Cube sum problem and an explicit Gross-Zagier formula*, Am. J. Math. **139** (2017), no. 3, 785–816.

[CST14] 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

[Cas73] William Casselman, *On some results of Atkin and Lehner*, Math. Ann. **201** (1973), 301–314, DOI 10.1007/BF01428197. MR0337789

[DV18] Samit Dasgupta and John Voight, *Sylvester's problem and mock Heegner points*, Proc. Amer. Math. Soc. **146** (2018), no. 8, 3257–3273, DOI 10.1090/proc/14008. MR3803653

[DV09] Samit Dasgupta and John Voight, *Heegner points and Sylvester's conjecture*, Arithmetic geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, pp. 91–102. MR2498056

[Gro88] Benedict H. Gross, *Local orders, root numbers, and modular curves*, Amer. J. Math. **110** (1988), no. 6, 1153–1182, DOI 10.2307/2374689. MR970123

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series.*, Invent. Math. **84** (1986), 225–320.

[HSY17] Yueke Hu, Jie Shu, and Hongbo Yin, *An explicit Gross-Zagier formula related to the Sylvester conjecture*, arXiv:1708.05266v2 (2017).

[KM88] M. A. Kenku and Fumiyuki Momose, *Automorphism groups of the modular curves* $X_0(N)$, Compositio Math. **65** (1988), no. 1, 51–80. MR930147

[Kob13] Shinichi Kobayashi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629, DOI 10.1007/s00222-012-0400-9. MR3020170

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR1106906

[LLT16] Yongxiong Li, Yu Liu, and Ye Tian, *On the Birch and Swinnerton-Dyer conjecture for CM elliptic curves over* $\mathbb{Q}$, arXiv:1605.01481 (2016).

[Liv95] Eric Liverance, *A formula for the root number of a family of elliptic curves*, J. Number Theory **51** (1995), no. 2, 288–305, DOI 10.1006/jnth.1995.1048. MR1326750

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859

[Ogg80] A. P. Ogg, *Modular functions*, Santa cruz conference on finite groups, 1980, pp. 521–532. MR2137353

[PR87] 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

[Sat86] Philippe Satgé, *Groupes de Selmer et corps cubiques* (French), J. Number Theory **23** (1986), no. 3, 294–317, DOI 10.1016/0022-314X(86)90075-2. MR846960

[Sel51] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$ (French), Acta Math. **87** (1951), 203–362.

[Shi94] 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

[Syl79] J. J. Sylvester, *On certain tenary cubic-form equations* (French), Am. J. Math. **2** (1879), no. 4, 357–393.

[YZZ13] 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

[ZK87] D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. (N.S.) **52** (1987), 51–69 (1988). MR989230

Department of Mathematics, ETH, Zurich, Switzerland
Email address: huyueke2012@gmail.com

School of Mathematical Sciences, Tongji University, Shanghai 200092, People's Republic of China
Email address: shujie@tongji.edu.cn

School of Mathematics, Shandong University, Jinan 250100, People's Republic of China
Email address: yhb2004@mail.sdu.edu.cn