Journal of Number Theory 224 (2021) 142–164

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Quadratic twists of $X_0(14)$

Junhwa Choi [a,*], Yongxiong Li [b]

[a] School of Mathematics, Korea Institute for Advanced Study, 85 Hoegi-ro, Dongdaemun-gu, Seoul 02455, Republic of Korea
[b] Yau Mathematical Sciences Center, Tsinghua University, Beijing, China

ARTICLE INFO

Article history:
Received 18 June 2020
Received in revised form 7 January 2021
Accepted 24 January 2021
Available online 22 February 2021
Communicated by F. Pellarin

MSC:
primary 11G40, 11G05

Keywords:
Waldspurger formula
Elliptic curves
Birch and Swinnerton-Dyer conjecture

ABSTRACT

In the present paper, we prove the 2-part of Birch and Swinnerton-Dyer conjecture for an explicit infinite family of rank 0 quadratic twists of the modular elliptic curve $X_0(14)$, using an explicit form of the Waldspurger formula. We also give an explicit infinite family of rank 1 quadratic twists of $X_0(14)$ whose Tate–Shafarevich group is of odd cardinality.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $L(E,s)$ be the complex L-series of E. For each square free non-zero integer $d \neq 1$, we write $E^{(d)}$ for the twist of E by the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, and $L(E^{(d)},s)$ for its complex L-series. It has been proved in [2] that there are infinitely many d such that $L(E^{(d)},s)$ is non-vanishing at $s=1$, and infinitely many d such that $L(E^{(d)},s)$ has a simple zero at $s=1$. Thanks to

* Corresponding author.
E-mail addresses: jhchoi.math@gmail.com (J. Choi), liyx_1029@tsinghua.edu.cn (Y. Li).

https://doi.org/10.1016/j.jnt.2021.01.011
0022-314X/

the results of Gross–Zagier and Kolyvagin, we know that for those d such that $L(E^{(d)}, s)$ has a zero at $s = 1$ of order 0 or 1, the rank of $E^{(d)}(\mathbb{Q})$ is equal to the order of this zero at $s = 1$ and the Tate–Shafarevich group $Ш(E^{(d)})$ of $E^{(d)}$ is finite. It is therefore natural to ask whether $L(E^{(d)}, s)$ has a zero at $s = 1$ of order 0 or 1 as d varies.

For the remainder of this section, we assume that $L(E, 1) \neq 0$. Let $C(E)$ denote the conductor of E, and let $\Omega_\infty(E)$ denote the fundamental real period of the Néron differential on E. We define

$$L^{(\mathrm{alg})}(E, 1) = L(E, 1)/\Omega_\infty(E),$$

which is a non-zero rational number. Let $c_\infty(E)$ denote the number of connected components of $E(\mathbb{R})$, and for each prime q dividing $C(E)$, let $c_q(E) = [E(\mathbb{Q}_q) : E_0(\mathbb{Q}_q)]$, where $E_0(\mathbb{Q}_q)$ is the subgroup of points in $E(\mathbb{Q}_q)$ with non-singular reduction modulo q. The conjectural Birch and Swinnerton-Dyer formula is then given by

$$L^{(\mathrm{alg})}(E, 1) = c_\infty(E) \prod_{q|C(E)} c_q(E) \cdot \frac{\#(Ш(E))}{(\#E(\mathbb{Q}))^2}. \tag{1.1}$$

For each prime p, the equality of the p-primary parts of the two sides of (1.1) is called the p-part of Birch and Swinnerton-Dyer formula. While E has complex multiplication, Rubin [14] proved that the p-part of Birch and Swinnerton-Dyer formula for E is valid for all primes $p \geq 5$. On the other hand, the results of Skinner–Urban [17] and Kato [11] on Iwasawa theory give the p-part of Birch and Swinnerton-Dyer formula for all elliptic curves E without complex multiplication and for all primes p but a finite number of primes p, including $p = 2, 3$ always. The aim of the present paper is to prove the remaining 2-part of Birch and Swinnerton-Dyer formula for an infinite family of quadratic twists of the elliptic curve

$$A = X_0(14) : y^2 + xy + y = x^3 + 4x - 6.$$

We know that $A(\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$, the discriminant of A is $-2^6 \cdot 7^3$, the j-invariant of A is $2^{-6} \cdot 5^3 \cdot 7^{-3} \cdot 43^3$ and its Néron differential $\omega = dx/(2y + x)$ has the fundamental real period $\Omega_\infty(A) = 1.98134\cdots$. Moreover, we have

$$L^{(\mathrm{alg})}(A, 1) = 1/6.$$

It is also known that the Tate–Shafarevich group of A is trivial and that $c_2(A) = 2$, $c_7(A) = 3$ and $c_\infty(A) = 1$. Therefore the full Birch and Swinnerton-Dyer conjecture is valid for A. However, the full Birch and Swinnerton-Dyer conjecture is still unknown for arbitrary quadratic twists of A that have non-vanishing L-values at $s = 1$. The following main theorem gives a family of quadratic twists of A for which the 2-part of Birch and Swinnerton-Dyer conjecture is valid.

Theorem 1.1. *Let $r \geq 0$ be an integer. Let $M = \epsilon q_1 \cdots q_r$ be a square free integer, where each q_i is a prime which is inert both in $\mathbb{Q}(\sqrt{-7})$ and in $\mathbb{Q}(\sqrt{2})$, and the sign $\epsilon = \pm 1$ is chosen so that $M \equiv 1 \bmod 4$. Then $L(A^{(M)}, 1) \neq 0$, $A^{(M)}(\mathbb{Q})$ is finite, the Tate–Shafarevich group of $A^{(M)}$ is finite of odd cardinality, and the 2-part of Birch and Swinnerton-Dyer formula is valid for $A^{(M)}$.*

We remark that, using modular symbols, Cai–Li–Zhai [5] also proved this theorem in the special case when $M = q_1 \cdots q_r$, where each q_i is a prime $\equiv 5 \bmod 8$ which is inert in $\mathbb{Q}(\sqrt{-7})$. In this paper, the main tool to prove Theorem 1.1 is an explicit form of the Waldspurger formula given in [6]. The key to establishing this formula is an explicit calculation on the test vector associated to A. For this, we will use the test vector theory in [10] and the explicit description in [1] of the Hecke action on the Shimura set associated to A.

This paper is motivated from the subsequent papers [18], [7] and [3]. They proved the 2-part of Birch and Swinnerton-Dyer formula for certain families of quadratic twists of elliptic curves with complex multiplication, which have minimal Weierstrass equations

$$E : y^2 = x^3 - x, \quad X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1 \quad \text{and} \quad X_0(36) : y^2 = x^3 + 1.$$

A new feature of this paper is that our elliptic curve $A = X_0(14)$ does not have complex multiplication, and that there is no $\mathbb{Q}$-isogenous quadratic twist of A. Thus the induction methods of [7], [4], [3], [18] cannot directly apply to A, in a sense that one can only get the 2-part of Birch and Swinnerton-Dyer formula for a product of two quadratic twists of A. To overcome this difficulty, we will use both the induction method via the Euler system of Gross points [3], and the induction method via the unramified periods [18], [7]. In the former induction method, we will use both the inert and the split Kolyvagin primes' Euler system properties (see also [4] for the case of Heegner points), and some 2-adic properties of the Fourier coefficients of the newform associated to A at these primes (see Lemma 3.1) play an essential role in our whole argument.

Overview of the paper. To compute the 2-Selmer groups, we introduce a classical 2-descent method in §2. In §3, as an application of Corollary 2.4, we give an infinite family of the rank 1 twists whose Tate–Shafarevich group is of odd cardinality. Most of the rest of the paper is devoted to the L-series. We establish an explicit form of the Waldspurger formula in §4, and use induction arguments to obtain the 2-adic valuation of the L-values at $s = 1$ in §5. Finally, in §6, we compute Tamagawa factors and prove Theorem 1.1.

Acknowledgments

The authors would like to thank John Coates for suggesting this problem. The first author is supported by a KIAS Individual Grant MG070401 at Korea Institute for Advanced Study. The second author would like to thank Myungjun Yu to invite him to a workshop held at KIAS in November 2019 for providing us with an excellent opportunity to discuss some ideas developed here. The second author is supported by NSFC-11901332.

2. Classical 2-descents

In this section, we will compute the 2-Selmer groups for a certain family of quadratic twists of A. We will use a classical 2-descent method (see Chapter X of [15] for details).

For a classical 2-descent method, we first give another expression for A and $A^{(M)}$. By changing of variables, A is given by the equation

$$A : y^2 = x^3 + 13x^2 + 128x.$$

Let M be a square free non-zero integer $\neq 1$ with $M \equiv 1 \bmod 4$ and $(M, 7) = 1$. Let $A^{(M)}$ be the twist of M by the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. The equation for $A^{(M)}$ is then given by

$$A^{(M)} : y^2 = x^3 + 13Mx^2 + 128M^2x$$

and, dividing this curve by the subgroup generated by the point $(0, 0)$, we obtain the new elliptic curve

$$A'^{(M)} : y^2 = x^3 - 26Mx^2 - 343M^2x.$$

The 2-isogenies between these elliptic curves are explicitly given by

$$\phi : A^{(M)} \longrightarrow A'^{(M)}, \quad (x, y) \longmapsto \left(y^2/x^2, y(128M^2 - x^2)/x^2\right).$$
$$\hat{\phi} : A'^{(M)} \longrightarrow A^{(M)}, \quad (x, y) \longmapsto \left(y^2/x^2, y(-343M^2 - x^2)/x^2\right).$$

We write $S^{(\phi)}(A^{(M)})$ and $S^{(\hat{\phi})}(A'^{(M)})$ for the Selmer groups of the isogenies ϕ and $\hat{\phi}$, respectively. Let S be the set of primes dividing $14M$, and let $\mathbb{Q}(S, 2)$ be the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ defined by

$$\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \mid \mathrm{ord}_v(b) \equiv 0 \bmod 2 \text{ for all } v \notin S\}.$$

The homogeneous space C_d for $A^{(M)}$ is given by the equation

$$C_d : dw^2 = d^2 - 26dMz^2 - 343M^2z^4,$$

and then $S^{(\phi)}(A^{(M)})$ can be identified with the subgroup of all d in $\mathbb{Q}(S, 2)$ such that $C_d(\mathbb{Q}_v)$ is non-empty for all $v \in S$. Similarly, the homogeneous space C'_d for $A'^{(M)}$ is given by the equation

$$C'_d : dw^2 = d^2 + 52dMz^2 + 2048M^2z^4,$$

and $S^{(\hat{\phi})}(A'^{(M)})$ can be identified with the subgroup of all d in $\mathbb{Q}(S, 2)$ such that $C'_d(\mathbb{Q}_v)$ is non-empty for all $v \in S$. Hence one can easily compute the Selmer groups $S^{(\phi)}(A^{(M)})$ and $S^{(\hat{\phi})}(A'^{(M)})$ by checking whether their homogeneous spaces have a $\mathbb{Q}_v$-rational point

or not. The proofs of the following propositions are similar to those of Proposition 3.1 and Proposition 3.3 in [7].

Proposition 2.1. *Let M be a square free non-zero odd integer $\neq 1$ with $(M,7)=1$. The Selmer group $S^{(\phi)}(A^{(M)})$ consists of the classes in $\mathbb{Q}(S,2)$ represented by integers d, $-7d$, where d runs over all integers dividing M such that*

(1) $\left(\frac{d}{7}\right)=1$ *if* $\left(\frac{M}{7}\right)=-1$;
(2) $d\equiv 1 \bmod 8$, *or* $d\equiv 7 \bmod 8$ *and* $\frac{M}{d}\equiv 5 \bmod 8$;
(3) *for all primes $q \mid M$ which are split in $\mathbb{Q}(\sqrt{-7})$ and $q \nmid d$, we have* $\left(\frac{d}{q}\right)=1$; *and*
(4) *for all primes $q \mid M$ with $q \mid d$, we have* $\left(\frac{2}{q}\right)=1$, *and moreover if* $\left(\frac{-7}{q}\right)=1$, $\left(\frac{13\pm 16a}{q}\right)=\left(\frac{M/d}{q}\right)$ *where a is any integer such that $a^2\equiv 2 \bmod q$.*

Proposition 2.2. *Assume that M is a square free odd integer $\neq 1$, prime to 7, with $M\equiv 1 \bmod 4$. Then $S^{(\hat{\phi})}(A'^{(M)})$ consists of the classes in $\mathbb{Q}(S,2)$ represented by integers d, $2d$, where d runs over all integers dividing M such that*

(1) $d>0$ *and* $\left(\frac{d}{7}\right)=1$;
(2) *for all primes $q \mid M$ which are split in $\mathbb{Q}(\sqrt{2})$ and $q \nmid d$, we have* $\left(\frac{d}{q}\right)=1$; *and*
(3) *for all primes $q \mid M$ with $q \mid d$, we have* $\left(\frac{-7}{q}\right)=1$, *and moreover if* $\left(\frac{2}{q}\right)=1$, $\left(\frac{13\pm 7a}{q}\right)=\left(\frac{-M/d}{q}\right)$ *where a is an integer such that $a^2\equiv -7 \bmod q$.*

We now give corollaries of Proposition 2.1 and Proposition 2.2. Recall that M is a square free non-zero integer $\neq 1$, with $M\equiv 1 \bmod 4$ and $(M,7)=1$. Let $S^{(2)}(A^{(M)})$ denote the classical Selmer group of $A^{(M)}$ for the endomorphism given by multiplication by 2. We have the exact sequence

$$0 \to \frac{A'^{(M)}(\mathbb{Q})[\hat{\phi}]}{\phi\left(A^{(M)}(\mathbb{Q})[2]\right)} \to S^{(\phi)}(A^{(M)}) \to S^{(2)}(A^{(M)}) \to S^{(\hat{\phi})}(A'^{(M)}).$$

We define $\mathfrak{S}^{(\phi)}(A^{(M)})$ and $\mathfrak{S}^{(2)}(A^{(M)})$ to be the quotients of $S^{(\phi)}(A^{(M)})$ and $S^{(2)}(A^{(M)})$ by the images of the torsion subgroups of $A'^{(M)}(\mathbb{Q})$ and $A^{(M)}(\mathbb{Q})$, respectively. By the fact that the 2-primary part of $A^{(M)}(\mathbb{Q})$ and $A'^{(M)}(\mathbb{Q})$ are both of order 2, it easily follows that we have the exact sequence

$$0 \to \mathfrak{S}^{(\phi)}(A^{(M)}) \to \mathfrak{S}^{(2)}(A^{(M)}) \to S^{(\hat{\phi})}(A'^{(M)}). \tag{2.1}$$

This enables us to compute $\mathfrak{S}^{(2)}(A^{(M)})$, once we can compute both $S^{(\phi)}(A^{(M)})$ and $S^{(\hat{\phi})}(A'^{(M)})$. We note that the weak parity theorem of Dokchitser brothers [9] shows that $\mathfrak{S}^{(2)}(A^{(M)})$ has even or odd $\mathbb{F}_2$-dimension according as the root number is $+1$ or

-1. Moreover, we can easily obtain the root number for quadratic twists of an elliptic curve. If the conductor of quadratic character χ_M of $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$ is prime to the conductor $C(E)$ of an elliptic curve $E/\mathbb{Q}$, the root number for $E^{(M)}$ is given by

$$w_{E^{(M)}} = \chi_M(-C(E))w_E. \tag{2.2}$$

Corollary 2.3. *Assume that $M = \epsilon q_1 \cdots q_r$, where each q_i is a prime which is inert both in $\mathbb{Q}(\sqrt{-7})$ and in $\mathbb{Q}(\sqrt{2})$, and the sign $\epsilon = \pm 1$ is chosen so that $M \equiv 1 \bmod 4$. Then $\mathfrak{S}^{(2)}(A^{(M)}) = 0$.*

Proof. The above two propositions show that $\mathfrak{S}^{(\phi)}(A^{(M)}) = 0$ and $S^{(\hat{\phi})}(A'^{(M)})$ has order 2. Since $A^{(M)}$ has root number $+1$, by (2.1) $\mathfrak{S}^{(2)}(A^{(M)})$ should have even $\mathbb{F}_2$-dimension. □

Corollary 2.4. *Assume that $M = \epsilon \ell_0 q_1 \cdots q_r$, where ℓ_0 is a prime which is inert in $\mathbb{Q}(\sqrt{-7})$ and is $\equiv 7 \bmod 8$, and each prime q_i and ϵ are defined as in Corollary 2.3. Then $\mathfrak{S}^{(2)}(A^{(M)})$ has order 2.*

Proof. By the above propositions, we have

$$S^{(\phi)}(A^{(M)}) = \{1, -7, -\ell_0, 7\ell_0\} \quad \text{and} \quad S^{(\hat{\phi})}(A'^{(M)}) = \{1, 2\}.$$

The assertion of the corollary follows from the exact sequence (2.1). □

Corollary 2.3 implies that $A^{(M)}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and $Ш(A^{(M)}/\mathbb{Q})(2) = 0$. We will prove in the following sections that

$$\operatorname{ord}_2(L^{(\mathrm{alg})}(A^{(M)}, 1)) = r - 1, \tag{2.3}$$

and that the 2-part of Birch and Swinnerton-Dyer conjecture is valid for $A^{(M)}$ for all those M. Similarly, Corollary 2.4 would imply that $A^{(M)}(\mathbb{Q}) = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $Ш(A^{(M)}/\mathbb{Q})(2) = 0$ if $Ш(A^{(M)}/\mathbb{Q})(2)$ is finite. In the next section §3, we will prove that $L(A^{(M)}, s)$ has a simple zero at $s = 1$ in a special case for those M.

3. Rank 1 twists

In this section, we will briefly discuss an application of Corollary 2.4, using Theorem 2.5 in [7]. We remark that for those M in Corollary 2.4, the formula (2.2) shows that $A^{(M)}$ has root number -1. Among those quadratic twists $A^{(M)}$, we will find the family of the twists which have a simple zero at $s = 1$.

Let $\ell_0 > 3$ be a prime $\equiv 3 \bmod 4$ and let

$$L = \mathbb{Q}(\sqrt{-\ell_0})$$

be the imaginary quadratic field. A *sensitive supersingular prime* for an elliptic curve E is defined to be a good supersingular prime q_1 for E where $q_1 \equiv 1 \bmod 4$ and $C(E)$ is a square modulo q_1. For example, there are sensitive supersingular primes for A

$$q_1 = 5, 101, 1637, 10589, 12101, \cdots .$$

We now assume that E has a sensitive supersingular prime q_1. For each integer $r \geq 2$, we define the set Σ_r consisting of all prime $q \neq q_1$ such that (i) $q \equiv 1 \bmod 4$, (ii) $a_q \equiv 0 \bmod 2^r$, (iii) $(q, C(E)) = 1$ and $C(E)$ is a square modulo q, and (iv) q is inert in L. Lemma 2.4 of [7] shows that the set Σ_r is infinite of positive density. In order to connect our primes in Corollary 2.4 with a sensitive supersingular prime and the primes in Σ_r, we have the following lemma (see also Theorem 6.1 of [5]).

Lemma 3.1. *Let q be an odd prime $\neq 2, 7$. The Fourier coefficients of the newform associated to A are given by*

$$a_2 = -1, \quad a_7 = 1,$$

and

$$a_q \equiv \begin{cases} 2 \bmod 4 \text{ if } q \equiv 1 \bmod 8, \\ 0 \bmod 4 \text{ if } q \equiv 7 \bmod 8, \\ 0 \bmod 4 \text{ if } q \equiv 3 \bmod 8 \text{ and } q \text{ is split in } \mathbb{Q}(\sqrt{-7}), \\ 2 \bmod 4 \text{ if } q \equiv 3 \bmod 8 \text{ and } q \text{ is inert in } \mathbb{Q}(\sqrt{-7}), \\ 2 \bmod 4 \text{ if } q \equiv 5 \bmod 8 \text{ and } q \text{ is split in } \mathbb{Q}(\sqrt{-7}), \\ 0 \bmod 4 \text{ if } q \equiv 5 \bmod 8 \text{ and } q \text{ is inert in } \mathbb{Q}(\sqrt{-7}). \end{cases}$$

Proof. The assertions for a_2 and a_7 follow from the fact that A has non-split multiplicative reduction at 2 and split multiplicative reduction at 7.

For other a_q's, we first note that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{2})$ and that both A and A' have the same Fourier coefficients. If $q \equiv \pm 1 \bmod 8$, then $A'(\mathbb{F}_q)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and hence we have $4 \mid \#A'(\mathbb{F}_q)$. Applying $a_q = q + 1 - \#A'(\mathbb{F}_q)$, the assertions follow for these cases. On the other hand, if $q \equiv \pm 3 \bmod 8$, $A'(\mathbb{F}_q)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. Using the duplication formula, it is easy to compute that $\mathbb{Q}(\sqrt{-7})$ is contained in $\mathbb{Q}(A'[4]^*)$, where $A'[4]^*$ is one of the 4-division points which comes from the non-trivial rational 2-torsion point of $A(\mathbb{Q})$. This implies that if q is inert (resp. split) in $\mathbb{Q}(\sqrt{-7})$, then $A'(\mathbb{F}_q)[4] \simeq \mathbb{Z}/2\mathbb{Z}$ (resp. $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), and hence $2 \mid \#A'(\mathbb{F}_q)$ but $4 \nmid \#A'(\mathbb{F}_q)$ (resp. $4 \mid \#A'(\mathbb{F}_q)$). It follows the remainder of the assertions. This completes the proof of the lemma. □

In particular, if q_1 is a sensitive supersingular prime for A and if $q_2, \cdots, q_r \in \Sigma_r$, then all of the primes should be inert both in $\mathbb{Q}(\sqrt{-7})$ and in $\mathbb{Q}(\sqrt{2})$. By Theorem 2.5 of [7], we obtain the following result.

Theorem 3.2. *Let $r \geq 2$ be an integer and let $M = -\ell_0 q_1 \cdots q_r$ be a square free integer which satisfies*

(1) *ℓ_0 is a prime which is inert in $\mathbb{Q}(\sqrt{-7})$ and is $\equiv 7 \bmod 8$,*
(2) *q_1 is a sensitive supersingular prime which is inert in L,*
(3) *The $q_2, \cdots, q_r$ are distinct primes in Σ_r.*

Then $L(A^{(M)}, s)$ has a simple zero at $s = 1$, $A^{(M)}(\mathbb{Q})$ has rank 1, and the Tate–Shafarevich group of $A^{(M)}$ is finite of odd cardinality.

Proof. Let $R = q_1 \cdots q_r$. By Theorem 2.5 in [7], there exists a point

$$y_R := \sum_{\sigma \in G} \chi_R(\sigma) f(P_R)^\sigma \in E(\mathbb{Q}(\sqrt{M})),$$

which is of infinite order. Here G is the Galois group of the ring class field H_R over L of conductor R, χ_R is the quadratic character of $L(\sqrt{R})/L$, f is a modular parametrization of A, and P_R is the Heegner point on $X_0(14)$ of conductor R. It follows that $L(A/L, \chi_R, s)$ has a simple zero at $s = 1$. However,

$$L(A/L, \chi_R, s) = L(A^{(M)}, s) L(A^{(R)}, s)$$

and $A^{(M)}$ and $A^{(R)}$ have root number -1 and $+1$, respectively. Hence $L(A^{(M)}, s)$ must have a simple zero at $s = 1$ and the twist $A^{(M)}$ has rank 1, and the Tate–Shafarevich group of $A^{(M)}$ is finite. Moreover, by Corollary 2.4, the Tate–Shafarevich group of $A^{(M)}$ is odd. □

4. Explicit form of the Waldspurger formula

In this section, we will establish the explicit Waldspurger formula for the quadratic twists of A in Theorem 1.1. We begin with a brief review of the test vector theory in [10] to get an appropriate test vector for the formula.

If W is any abelian group, we will denote $\hat{W}$ by the tensor product over $\mathbb{Z}$ of W with $\hat{\mathbb{Z}} = \prod_{\ell < \infty} \mathbb{Z}_\ell$, and W_ℓ by $W \otimes \mathbb{Z}_\ell$. Let B be a definite quaternion algebra over $\mathbb{Q}$, and let U be an open subgroup of $\hat{B}^\times$. Let X denote the finite set $B^\times \backslash \hat{B}^\times / U$, and write $g_1, \cdots, g_n$ for a set of representatives of X and $[g_1] \cdots, [g_n]$ for their classes in X. Denote by $\mathbb{Z}[X]$ the free $\mathbb{Z}$-module of formal sums $\sum_{i=1}^n a_i [g_i]$ with $a_i \in \mathbb{Z}$, and $\mathbb{Z}[X]^0$ the degree-0 submodule of $\mathbb{Z}[X]$. Here the degree of $\sum a_i [g_i]$ is defined to be $\sum a_i$. We define

$$w_i = \#\Gamma_i \text{ where } \Gamma_i = (B^\times \cap g_i U g_i^{-1})/\{\pm 1\}, \tag{4.1}$$

and let $\langle\ ,\ \rangle$ be the $\mathbb{Z}$-bilinear pairing on $\mathbb{Z}[X]$ defined by $\langle [g_i], [g_j]\rangle = \delta_{ij} w_i$. Let $\Pi = \otimes_v \Pi_v$ be the automorphic representation of $B_{\mathbb{A}}^{\times}$ associated to A via the Jacquet–Langlands correspondence. There is a natural embedding

$$\Pi^U \longrightarrow \mathbb{C}[X]^0 = \mathbb{Z}[X]^0 \otimes_{\mathbb{Z}} \mathbb{C}, \quad f \mapsto \sum_{i=1}^{n} f([g_i])[g_i]. \tag{4.2}$$

For our purpose, we will consider two quaternion algebras over $\mathbb{Q}$. Throughout this section, we write $\{P, Q\} = \{2, 7\}$. Let B be the quaternion algebra over $\mathbb{Q}$ ramified exactly at ∞ and Q.

- When $Q = 2$, we have $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ with $i^2 = -1$, $j^2 = -1$ and $ij = -ji = k$. The maximal order $\mathcal{O}_B$ of B is given by

$$\mathcal{O}_B = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}.$$

  The unit group $\mathcal{O}_B^{\times} = \langle i, j, (1+i+j+k)/2\rangle$ is of order 24.
- When $Q = 7$, we have $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ with $i^2 = -1$, $j^2 = -7$ and $ij = -ji = k$. The maximal order $\mathcal{O}_B$ of B is given by

$$\mathcal{O}_B = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{i+j}{2} + \mathbb{Z}\frac{1+k}{2}.$$

  The unit group $\mathcal{O}_B^{\times} = \langle i\rangle$ is of order 4.

The representation Π is naturally realized as a subspace of the space of smooth complex-valued functions on $B^{\times}\backslash \hat{B}^{\times}/\hat{\mathbb{Q}}^{\times}$. By [10], the local representations Π_v can be determined as follows.

1. Π_∞ is trivial.
2. Π_ℓ is spherical if $\ell \neq 14 \cdot \infty$, i.e. $\Pi_\ell^{\mathcal{O}_{B_\ell}^{\times}}$ is of dimension one.
3. Π_Q has conductor with exponent 0, i.e. $\Pi_Q^{\mathcal{O}_{B_Q}^{\times}} \neq 0$.
4. Π_P has conductor P, i.e. there is an order R_P in $\mathcal{O}_{B_P}$ such that it is isomorphic to the Eichler order of level P

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_P) : c \equiv 0 \bmod P \right\} \subset M_2(\mathbb{Z}_P) \simeq \mathcal{O}_{B_P}, \tag{4.3}$$

   and that $\Pi_P^{R_P^{\times}}$ is of dimension one.

Let $U = \prod_\ell U_\ell$ be the open compact subgroup of $\hat{B}^{\times}$ defined by $U_\ell = \mathcal{O}_{B_\ell}^{\times}$ for all $\ell \neq P$ and $U_P = R_P^{\times}$. By the Propositions 8.4 and 6.4 of [10], we know that the representation Π^U is of dimension one.

Next, we will compute an explicit basis of Π^U. Our approach is to analyze the action of Hecke operators on $X = B^\times \backslash \hat{B}^\times / U$ via Bruhat–Tits trees. We remark that this idea is presented and discussed in [1]. Since $\mathbb{Q}$ has class number 1, X can be rewritten as

$$X = B^\times \backslash (\hat{\mathbb{Q}}^\times \backslash \hat{B}^\times / U),$$

and $\hat{\mathbb{Q}}^\times \backslash \hat{B}^\times / U$ is the product of local spaces $\mathbb{Q}_\ell^\times \backslash B_\ell^\times / U_\ell$ for all primes ℓ. For each $\ell \nmid 14$, we know that

$$\mathcal{T}_\ell = \mathbb{Q}_\ell^\times \backslash B_\ell^\times / U_\ell = \mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$$

is the Bruhat–Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. This is a graph whose vertices are in one-to-one correspondence with the homothety classes of $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$. Two vertices are joined by an edge if they can be represented by lattices Λ_1 and Λ_2 such that $\Lambda_2 \subset \Lambda_1$ and Λ_1/Λ_2 is cyclic of order ℓ. Given a vertex $x \in \mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$, the $\ell+1$ neighbors $x \cdot z_0, \cdots, x \cdot z_{l-1}$ and $x \cdot z_\infty$ are given by

$$z_i = \begin{pmatrix} \ell & i \\ 0 & 1 \end{pmatrix}, \quad i = 0, \cdots, \ell - 1, \quad z_\infty = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}.$$

The correspondence T_ℓ is defined by

$$T_\ell(x) = x \cdot \left(\sum_{i=0}^{\ell-1} z_i + z_\infty \right).$$

One extends it to the product tree $\hat{\mathbb{Q}}^\times \backslash \hat{B}^\times / U$, and hence to X. We call it the Hecke operator on X.

Proposition 4.1. *The one-dimensional space Π^U has a basis f as follows. There is a natural bijection*

$$\Lambda := \mathcal{O}_B^\times \backslash \mathcal{O}_{B_P}^\times / U_P \xrightarrow{\sim} B^\times \backslash \hat{B}^\times / \hat{\mathbb{Q}}^\times U$$

induced by the embedding $\mathcal{O}_{B_P}^\times \subset B_P^\times \hookrightarrow \hat{B}^\times$. The set Λ is of order 2, say $\{g_1, g_2\}$. A basis f is determined by $f(g_1) = 1$ and $f(g_2) = -1$. Such a basis is unique up to multiplication by ± 1.

Proof. As remarked before, we already know that the dimension of Π^U is one, but we will reprove it by an explicit calculation. First, we fix an isomorphism ϕ_P of B_P onto $M_2(\mathbb{Q}_P)$ such that $\phi_P(\mathcal{O}_{B_P}) = M_2(\mathbb{Z}_P)$ as follows.

- When $P = 7$, we denote by $\rho = \zeta_3$ a primitive cube root of unity in $\mathbb{Z}_7$. Then

$$\phi_7(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \phi_7(j) = \begin{pmatrix} \rho & \rho+1 \\ \rho+1 & -\rho \end{pmatrix}, \quad \phi_7(k) = \begin{pmatrix} \rho+1 & -\rho \\ -\rho & -\rho-1 \end{pmatrix}.$$

- When $P = 2$, we denote by $\rho = \sqrt{-7}$ in $\mathbb{Z}_2$. Then

$$\phi_2(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \phi_2(j) = \begin{pmatrix} 0 & \rho \\ \rho & 0 \end{pmatrix}, \quad \phi_2(k) = \begin{pmatrix} \rho & 0 \\ 0 & -\rho \end{pmatrix}.$$

Since $\mathcal{O}_B$ has class number 1, every element of X can be written as (u_ℓ) with $u_\ell \in \mathcal{O}_{B_\ell}^\times$. The idéle $u = (u_\ell)$ is then uniquely represented by the element $\phi_P(u_P)$ in the coset $\phi_P(\mathcal{O}_B^\times)\backslash \mathrm{GL}_2(\mathbb{Z}_P)/U_P \simeq \Lambda$. The space $\mathrm{GL}_2(\mathbb{Z}_P)/U_P$ is identified with the projective line $\mathbb{P}^1(\mathbb{F}_P)$ via $\gamma \mapsto \gamma \cdot \infty$. The group $\phi_P(\mathcal{O}_B^\times)$ act on $\mathbb{P}^1(\mathbb{F}_P)$ via the linear fractional transformation.

When $P = 7$ and $Q = 2$, recall that $\mathcal{O}_B^\times$ is a group of order 24. There are exactly two $\phi_7(\mathcal{O}_B^\times)$-orbits on $\mathbb{P}^1(\mathbb{F}_7)$, $\{\infty, 0, 2, 3\}$ and $\{1, 4, 5, 6\}$. The stabilizers Γ_1 and Γ_2 of each orbit are of order 3 in $\mathcal{O}_B^\times/\{\pm 1\}$, and hence $w_1 = w_2 = 3$. Let Y_1, Y_2 be the two components of X corresponding to these orbits. For $P = (u_\ell) \in X$ with $u_\ell \in \mathcal{O}_{B_\ell}^\times$, we have $P \in Y_1$ or Y_2 according as $\phi_7(u_7) \cdot \infty = \infty, 0, 2, 3$ or $\phi_7(u_7) \cdot \infty = 1, 4, 5, 6$. Hence we have $\mathbb{Z}[X] = \mathbb{Z}g_1 + \mathbb{Z}g_2$ where the g_i correspond to the Y_i such that $\langle g_i, g_j \rangle = \delta_{ij} w_i$. The Hecke operator T_3 acts on g_1 and g_2 by

$$T_3 g_1 = g_1 + 3g_2, \quad T_3 g_2 = 3g_1 + g_2.$$

Hence the elements

$$v_0 = g_1 + g_2, \quad v_1 = g_1 - g_2$$

give an eigenbasis of $\mathbb{Z}[X]$ for the Hecke operator T_3. Since v_0 corresponds to the Eisenstein series of weight 2, by (4.2) we know that v_1 lies in the one-dimensional line Π^U.

When $P = 2$ and $Q = 7$, we have $\mathcal{O}_B^\times = \langle i \rangle$. There are exactly two $\phi_2(\mathcal{O}_B^\times)$-orbits on $\mathbb{P}^1(\mathbb{F}_2)$, $\{\infty, 0\}$ and $\{1\}$. Similarly, we have $w_1 = 1$ and $w_2 = 2$, and $\mathbb{Z}[X] = \mathbb{Z}g_1 + \mathbb{Z}g_2$. Here the Hecke operator T_3 acts on g_1 and g_2 by

$$T_3(g_1) = 2g_1 + 2g_2, \quad T_3(g_2) = 4g_1,$$

and the elements

$$v_0 = 2g_1 + g_2, \quad v_1 = g_1 - g_2$$

give an eigenbasis of $\mathbb{Z}[X]$ for the Hecke operator T_3. Again, since v_0 corresponds to the Eisenstein series of weight 2, the element v_1 lies in the one-dimensional line Π^U. □

Recall that $M = q_1 q_2 \cdots q_r$, where each q_i is a prime congruent to 5 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. Let p be any prime congruent to 3 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. We denote by K the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ or $\mathbb{Q}(\sqrt{-pM})$. Let $d \mid M$ be a positive integer, and let χ be the quadratic character of K, say of conductor c, corresponding to the extension $K(\sqrt{d})/K$. The L-series $L(A/K, \chi, s)$ has the following properties.

- When $K = \mathbb{Q}(\sqrt{-p})$, we have $c = d$ and

$$L(A/K, \chi, s) = L(A^{(d)}, s) L(A^{(-pd)}, s).$$

- When $K = \mathbb{Q}(\sqrt{-pM})$, we have $c = 1$ and

$$L(A/K, \chi, s) = L(A^{(d)}, s) L(A^{(-pM/d)}, s).$$

Let $\mathcal{R}$ be the global order of B given by

$$\mathcal{R} = \mathcal{O}_B \cap \left(\prod_{\ell \nmid P} \mathcal{O}_{B_\ell} \times R_P \right) \tag{4.4}$$

so that $U = \hat{\mathcal{R}}^\times$. We fix an embedding of K into B such that $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ is equal to $\mathcal{R} \cap K$ (for the existence of such an embedding, see [10]). This embedding induces a homomorphism ι of $\hat{K}^\times$ into $\hat{B}^\times$.

For our later induction arguments in the next section, we introduce the notion of primitive integral Gross–Prasad test vector.

Definition 4.2. We say that any non-zero vector f in the space Π^U is a primitive integral Gross–Prasad test vector for (A, χ) if

1. For $\ell \nmid 14$, f is a simultaneous eigenvector for T_ℓ with the same eigenvalue a_ℓ of the newform associated to A.
2. The values of f are integers that generates $\mathbb{Z}$.

Of course, by definition the f in Proposition 4.1 is a primitive integral Gross–Prasad test vector for (A, χ). For our purpose (see the assumption (ii) of Theorem 1.2 of [6]), we should take the quaternion algebra $B/\mathbb{Q}$ and the vector f as follows.

- If $K = \mathbb{Q}(\sqrt{-p})$, we take the quaternion algebra $B/\mathbb{Q}$ ramified exactly at $\Sigma(B) = \{\infty, 2\}$.
- If $K = \mathbb{Q}(\sqrt{-pM})$, we take the quaternion algebra $B/\mathbb{Q}$ ramified exactly at $\Sigma(B) = \{\infty, 2\}$ or $\{\infty, 7\}$, according as the number r of the prime factor of M is even or odd.

Let H_c be the ring class field of K of conductor c. Then $\mathrm{Gal}(H_c/K) \simeq \mathrm{Pic}(\mathcal{O}_c) = K^\times \backslash \hat{K}^\times / \hat{\mathcal{O}}_c^\times$, and the embedding $\iota : \hat{K}^\times \to \hat{B}^\times$ induces a map

$$K^\times \backslash \hat{K}^\times / \hat{\mathcal{O}}_c^\times \to B^\times \backslash \hat{B}^\times / U = X.$$

We now define the period by

$$P_\chi(f) = \sum_{t \in \mathrm{Pic}(\mathcal{O}_c)} f(t)\chi(t).$$

Proposition 4.3 *(Explicit Waldspurger formula for (A, χ)). Let M and d be defined as above. Let f be a primitive integral Gross–Prasad test vector for (A, χ).*

1. *If $K = \mathbb{Q}(\sqrt{-p})$, we have*

$$L^{(\mathrm{alg})}(A^{(d)}, 1) L^{(\mathrm{alg})}(A^{(-pd)}, 1) = \frac{|P_\chi(f)|^2}{6}.$$

2. *If $K = \mathbb{Q}(\sqrt{-pM})$, we have*

$$L^{(\mathrm{alg})}(A^{(d)}, 1) L^{(\mathrm{alg})}(A^{(-pM/d)}, 1) = \frac{|P_\chi(f)|^2}{C}$$

where the constant C is 6 or 3, according as r is even or odd.

Proof. It follows from the explicit Waldspurger formula of Theorem 1.2 of [6]

$$L(A/K, \chi, 1) = \frac{8\pi^2 (\phi_A, \phi_A)_{\Gamma_0(14)}}{c\sqrt{|D|}} \cdot \frac{|P_\chi(f)|^2}{\langle f, f \rangle}.$$

Here ϕ_A is the newform associated to A, D is the discriminant of K, $\langle f, f \rangle$ is the pairing defined by the map (4.2), and $(\phi_A, \phi_A)_{\Gamma_0(14)}$ is the Petersson inner product defined by

$$(\phi_A, \phi_A)_{\Gamma_0(14)} = \iint\limits_{\Gamma_0(14)\backslash \mathcal{H}} |\phi_A(x + iy)|^2 dx dy.$$

Let $A(\mathbb{C})^\pm$ denote the $\pm$ eigen-subgroups of $A(\mathbb{C})$ under the action of the complex conjugation. Thus $A(\mathbb{C})^+ = A(\mathbb{R})$ and $A(\mathbb{C})^- = A'(\mathbb{R})$, where A' is the twist of A by $\mathbb{C}/\mathbb{R}$. Recall that ω is the Néron differential on A, and that we have

$$\Omega_\infty(A) = \int\limits_{A(\mathbb{C})^+} \omega.$$

If we define

$$\Omega_\infty(A)^- = \int_{A(\mathbb{C})^-} \omega,$$

then we have

$$-i\Omega_\infty(A)\Omega_\infty(A)^- = \iint_{A(\mathbb{C})} |\omega \wedge \bar{\omega}| = 8\pi^2(\phi_A, \phi_A)_{\Gamma_0(14)}.$$

The Main Result 1.1 of [13] tells us that

1. If $D = -p$, we have $\Omega_\infty(A^{(d)})\Omega_\infty(A^{(Dd)}) = \Omega_\infty(A)\Omega_\infty(A)^-/d\sqrt{D}$.
2. If $D = -pM$, we have $\Omega_\infty(A^{(d)})\Omega_\infty(A^{(D/d)}) = \Omega_\infty(A)\Omega_\infty(A)^-/\sqrt{D}$.

Hence we have

$$\frac{8\pi^2(\phi_A, \phi_A)_{\Gamma_0(14)}}{c\sqrt{|D|}} = \begin{cases} \Omega_\infty(A^{(d)})\Omega_\infty(A^{(-pd)}) & \text{if } D = -p, \\ \Omega_\infty(A^{(d)})\Omega_\infty(A^{(-pM/d)}) & \text{if } D = -pM. \end{cases}$$

Finally, by Proposition 4.1, we have $\langle f, f\rangle = 6$ if $\Sigma(B) = \{\infty, 2\}$, and $\langle f, f\rangle = 3$ if $\Sigma(B) = \{\infty, 7\}$. This concludes the proof of the proposition. □

5. Induction methods

5.1. Induction method via Euler system of Gross points

In this subsection, we will use an induction argument of the Euler system of Gross points to compute the 2-adic valuation of the product $L^{(\mathrm{alg})}(A^{(M)}, 1)L^{(\mathrm{alg})}(A^{(-pM)}, 1)$. We keep the notation of the previous section, but we take $K = \mathbb{Q}(\sqrt{-p})$. Recall that B is the quaternion algebra over $\mathbb{Q}$ ramified exactly at ∞ and 2, that $\mathcal{R}$ is the global order as given in (4.4), and that $U = \hat{\mathcal{R}}^\times$. We fix an embedding of K into B such that $K \cap \mathcal{R} = \mathcal{O}_K$, which induces a homomorphism of $\hat{K}^\times$ into $\hat{B}^\times$.

Definition 5.1. For a positive integer m coprime to $2, 3, 7, p$, we say that a point $x_m \in K^\times \backslash \hat{B}^\times / U$ is a Gross point of conductor m if $x_m U x_m^{-1} \cap \hat{K}^\times = \hat{\mathcal{O}}_m^\times$. Here, for a positive integer c, we recall that $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$.

Note that $\mathrm{Gal}(H_m/K) \simeq K^\times \backslash \hat{K}^\times / \hat{\mathcal{O}}_m^\times$ acts on x_m by left multiplication.

We will construct a Gross point x_m as follows. For any prime $\ell \neq 2, 3, 7, p$, we fix an isomorphism $\phi_\ell : B_\ell \xrightarrow{\sim} M_2(\mathbb{Q}_\ell)$ such that $\phi_\ell(\mathcal{R}_\ell) = M_2(\mathbb{Z}_\ell)$. Then we have

- $\phi_\ell(K_\ell) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q}_\ell \right\}$ if ℓ is split in K.

- $\phi_\ell(K_\ell) = \left\{ \begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} : a, b \in \mathbb{Q}_\ell \right\}$ for some $\delta \in \mathbb{Z}_\ell^\times / (\mathbb{Z}_\ell^\times)^2$ if ℓ is inert in K.

For any positive integer m coprime to $2 \cdot 3 \cdot 7 \cdot p$, we define $x_m \in \hat{B}^\times$ by taking the ℓ-part of x_m to be $\phi_\ell^{-1} \begin{pmatrix} \ell^{\mathrm{ord}_\ell(m)} & 0 \\ 0 & 1 \end{pmatrix}$ or 1, according as $\ell \mid m$ or $\ell \nmid m$. The image of x_m in $K^\times \backslash \hat{B}^\times / U$, also denoted by x_m, is a Gross point of conductor m.

As a shorthand notation, we will also denote by x_m the image of x_m in $X = B^\times \backslash \hat{B}^\times / U$. The Euler system of Gross points is the following theorem.

Theorem 5.2. *For any prime $\ell \neq 2, 3, 7, p$ and for any positive integer m coprime to $2 \cdot 3 \cdot 7 \cdot p$, we have*

$$u_m \cdot \sum_{\sigma \in \mathrm{Gal}(H_{m\ell}/H_m)} \sigma \cdot x_{m\ell} = \begin{cases} T_\ell(x_m) & \text{if } \ell \text{ is inert in } K, \\ T_\ell(x_m) - \sum_{\mathfrak{l} \mid \ell} \mathrm{Frob}_\mathfrak{l}(x_m) & \text{if } \ell \text{ is split in } K, \end{cases}$$

where $\mathrm{Frob}_\mathfrak{l}$ *is the Frobenius at* $\mathfrak{l} \mid \ell$ *in* $\mathrm{Gal}(H_m/K)$*, and* $u_m = 1$ *if* $m \neq 1$*, and* $u_1 = [\mathcal{O}_K^\times : \mathbb{Z}^\times]$.

Proof. See Proposition 4.8 of [12]. □

Now, let $d = q_1 \cdots q_k$ where each q_i is a prime congruent to 5 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. For each q_i, we take an isomorphism $\phi_{q_i} : B_{q_i} \xrightarrow{\sim} M_2(\mathbb{Q}_{q_i})$ given by

$$i \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, k \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}.$$

In particular, $\phi_{q_i}(\mathcal{O}_{B_{q_i}}) = M_2(\mathbb{Z}_{q_i})$. Let $x_{q_i} \in B_q^\times$ be the element such that $\phi_{q_i}(x_{q_i}) = \begin{pmatrix} q_i & 0 \\ 0 & 1 \end{pmatrix}$, and let $x_d = \prod_{i=1}^k x_{q_i} \in \hat{B}^\times$. Then $x_d U x_d^{-1} \cap \hat{K}^\times = \hat{\mathcal{O}}_d^\times$. Let f be an explicit basis of Π^U constructed in Proposition 4.1. We define

$$f_d = r(x_d) f,$$

where $r(x_d)$ is the right multiplication by x_d map, i.e. $(r(x_d)f)(b) = f(bx_d)$ for all $b \in \hat{B}^\times$. The f_d is then a primitive integral Gross–Prasad test vector for (A, χ_d), recalling that χ_d is the quadratic character over K of conductor d corresponding to the extension $K(\sqrt{d})/K$. By Proposition 4.3, we have

$$L^{(\mathrm{alg})}(A^{(d)}, 1) L^{(\mathrm{alg})}(A^{(-pd)}, 1) = \frac{|P_{\chi_d}(f_d)|^2}{6}.$$

We can now state the main result of this subsection. For the moment, we assume that

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-p)}, 1)) = 0, \tag{5.1}$$

which will be proved later (see Proposition 5.5).

Theorem 5.3. *Let p be a prime congruent to 3 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. Let $M = q_1 \cdots q_r$ be a square free integer, where each q_i is a prime congruent to 5 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. Then we have*

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(M)}, 1)L^{(\mathrm{alg})}(A^{(-pM)}, 1)) = 2r - 1.$$

Proof. Let M_+ (respectively, M_-) denote the product of the primes dividing M, which are split (respectively, inert) in K. Let $\mu(M)$ be the number of the prime factors of M, and let $s(M)$ be the number of the prime factors of M_+. We will use induction on both $s(M)$ and $\mu(M)$. For any divisor $d \mid M$, we define

$$y_d = \sum_{\sigma \in \mathrm{Gal}(H_M/K)} f_M(\sigma)\chi_d(\sigma). \tag{5.2}$$

Then the assertion of the theorem is equivalent to saying that $\mathrm{ord}_2(y_M) = r$.

We first assume that $s(M) = 0$. When $\mu(M) = 0$, the result holds because we know that $L^{(\mathrm{alg})}(A, 1) = 1/6$ and by the assumption (5.1) that

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A, 1)L^{(\mathrm{alg})}(A^{(-p)}, 1)) = -1.$$

We now assume that $\mu(M) = r > 0$ and that the result holds for every divisor $d \mid M$ with $d \neq M$. Let

$$H_M^0 = K(\sqrt{q_1}, \cdots, \sqrt{q_r})$$

be the subfield of H_M. Then we have $[H_M : H_M^0] = w \cdot \prod_{i=1}^{r}(q_i + 1)/2$, which is odd, where $w = 1/3$ if $p = 3$, and $w = 1$ otherwise. We have

$$\sum_{d \mid M} \chi_d(\sigma) = \begin{cases} 2^r & \text{if } \sigma \in \mathrm{Gal}(H_M/H_M^0), \\ 0 & \text{otherwise,} \end{cases}$$

which follows that

$$\sum_{d \mid M} y_d = 2^r y^0, \quad \text{where } y^0 = \sum_{\sigma \in \mathrm{Gal}(H_M/H_M^0)} f_M(\sigma). \tag{5.3}$$

We claim that $\mathrm{ord}_2(y_d) \geq r + 1$ for all $d \neq M$. Indeed, for any prime $q \mid M$ with $qd \mid M$, we have

$$\begin{aligned} y_d &= \sum_{\sigma\in \mathrm{Gal}(H_{M/q}/K)} x_d(\sigma) \sum_{\tau\in \mathrm{Gal}(H_M/H_{M/q})} f_M(\sigma\tau) \\ &= \sum_{\sigma\in \mathrm{Gal}(H_{M/q}/K)} x_d(\sigma) \sum_{\tau\in \mathrm{Gal}(H_M/H_{M/q})} f(\sigma\tau x_M) \\ &= \sum_{\sigma\in \mathrm{Gal}(H_{M/q}/K)} x_d(\sigma)\cdot u_{M/q}^{-1}\cdot a_q f(\sigma x_{M/q}) \end{aligned} \tag{5.4}$$

The last equality comes from Theorem 5.2. Moreover, if there exists a prime $q' \mid M/q$ with $q'd \mid M/q$, the same argument shows that

$$y_d = u_{M/q}^{-1}u_{M/qq'}^{-1}\cdot a_q a_q' \cdot \sum_{\sigma\in \mathrm{Gal}(H_{M/qq'}/K)} x_d(\sigma) f(\sigma x_{M/qq'}).$$

Thus we have

$$y_d = u\cdot \left(\prod_{q\mid M/d} a_q\right)\cdot P_{\chi_d}(f_d) \quad \text{for some } u\in 2\mathbb{Z}+1.$$

By induction hypothesis, we know that $\mathrm{ord}_2(P_{\chi_d}(f_d)) = \mu(d)$. By Lemma 3.1, we have $a_q \equiv 0 \bmod 4$ so that

$$\mathrm{ord}_2(y_d) \geq 2\mu(M/d) + \mu(d) \geq r+1.$$

Then the equation (5.3) gives

$$y_M \equiv 2^r y^0 \bmod 2^{r+1}.$$

Finally, since f_M takes values ± 1, we have that $y^0 \equiv [H_M : H_M^0] \equiv 1 \bmod 2$. Hence we conclude that $\mathrm{ord}_2(y_M) = r$.

We now assume that $s(M) > 0$ and that the result holds for every divisor $d \mid M$ with $s(d) < s(M)$. Similarly, we have

$$\sum_{d\mid M} y_d = \sum_{\substack{d\mid M \\ M_-\mid d}} y_d + \sum_{\substack{d\mid M \\ M_-\nmid d}} y_d = 2^r y^0. \tag{5.5}$$

However, there exists at least one prime $q \mid M_+$ so that $[H_M : H_M^0]$ is divided into $(q-1)/2$, and hence $y^0 \equiv [H_M : H_M^0] \equiv 0 \bmod 2$. Hence the equation (5.5) gives

$$\sum_{\substack{d\mid M \\ M_-\mid d}} y_d + \sum_{\substack{d\mid M \\ M_-\nmid d}} y_d \equiv 0 \bmod 2^{r+1}. \tag{5.6}$$

For each $d \mid M$ with $M_- \mid d$ and $d \neq M$, by a similar calculation as in (5.4), Theorem 5.2 tells us that

$$y_d = \prod_{q|\mathfrak{M}_d} (a_q - \mathrm{Frob}_{\mathfrak{q}} - \mathrm{Frob}_{\bar{\mathfrak{q}}}) \cdot P_{\chi_d}(f_d), \tag{5.7}$$

where $\mathfrak{M}_d = M_+/(d, M_+)$ and $\mathfrak{q}$, $\bar{\mathfrak{q}}$ are the primes of K above q. We have

$$\mathrm{Frob}_{\mathfrak{q}} \cdot P_{\chi_d}(f_d) = \sum_{\sigma \in \mathrm{Gal}(H_M/K)} f_d(\mathrm{Frob}_{\mathfrak{q}} \cdot \sigma)\chi_d(\sigma) = \chi_d(\mathrm{Frob}_{\mathfrak{q}}) P_{\chi_d}(f_d)$$

and similarly

$$\mathrm{Frob}_{\bar{\mathfrak{q}}} \cdot P_{\chi_d}(f_d) = \chi_d(\mathrm{Frob}_{\bar{\mathfrak{q}}}) P_{\chi_d}(f_d).$$

By the fact that $\chi_d(\mathrm{Frob}_{\mathfrak{q}}) = \chi_d(\mathrm{Frob}_{\bar{\mathfrak{q}}})$ and that $a_q \equiv 0 \bmod 4$, the equation (5.7) gives

$$y_d \equiv 2^{\mu(\mathfrak{M}_d)} P_{\chi_d}(f_d) \bmod 2^{r+1}.$$

By the induction hypothesis, we have $\mathrm{ord}_2(P_{\chi_d}(f_d)) = \mu(d)$, and hence $\mathrm{ord}_2(y_d) = \mu(\mathfrak{M}_d) + \mu(d) = r$.

On the other hand, for each $d \mid M$ with $M_- \nmid d$, there exists at least one prime $q \mid M_-$ with $q \mid (M/d)$. By a similar argument as in (5.4) and (5.7), we see that

$$\mathrm{ord}_2(y_d) \geq r + 1.$$

Thus the congruence (5.6) becomes

$$y_M + \sum_{\substack{d|M \\ M_-|d,\ d \neq M}} y_d \equiv 0 \bmod 2^{r+1}.$$

Since the number of $d \mid M$ such that $M_- \mid d$ and $d \neq M$ is odd, we conclude that $\mathrm{ord}_2(y_M) = r$. □

5.2. Induction method via the unramified periods

Combining with Theorem 5.3, we will now compute the 2-adic valuation of both $L^{(\mathrm{alg})}(A^{(M)}, 1)$ and $L^{(\mathrm{alg})}(A^{(-pM)}, 1)$, using an induction argument of unramified periods. In this subsection, we take $K = \mathbb{Q}(\sqrt{-pM})$. Recall that B is the quaternion algebra over $\mathbb{Q}$ ramified exactly at $\Sigma(B) = \{\infty, 2\}$ or $\{\infty, 7\}$, according as r is even or odd. Let $\mathcal{R}$ be the global order as given in (4.4), and let $U = \hat{\mathcal{R}}^\times$. We fix an embedding of K into B such that $K \cap \mathcal{R} = \mathcal{O}_K$, which induces a homomorphism of $\hat{K}^\times$ into $\hat{B}^\times$.

Let f be a primitive integral Gross–Prasad test vector for (A, χ_d). Note that χ_d corresponds to the unramified extension $K(\sqrt{d})/K$, i.e. its conductor c is equal to 1. In this manner, the period

$$P_{\chi_d}(f) = \sum_{t \in \mathrm{Pic}(\mathcal{O}_K)} f(t)\chi_d(t)$$

is called an unramified period. By Proposition 4.3, we recall

$$L^{(\mathrm{alg})}(A^{(d)},1)L^{(\mathrm{alg})}(A^{(-pM/d)},1)=\frac{|P_{\chi_d}(f)|^2}{C}, \tag{5.8}$$

where $C=6$ or 3, according as r is even or odd.

Theorem 5.4. *Let p be a prime congruent to 3 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. Let $M=q_1\cdots q_r$ be a square free integer, where each q_i is a prime congruent to 5 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. Then we have*

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(M)},1))=r-1,\quad \mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-pM)},1))=r.$$

Proof. We will use induction on $r=\mu(M)$. When $r=0$, the result holds because we know by the assumption (5.1) that

$$L^{(\mathrm{alg})}(A,1)=1/6,\quad \mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-p)},1))=0.$$

We now assume that $r>0$ is even and that the result holds for every divisor $d\mid M$ with $d\neq M$. By a similar calculation as in (5.3), we have

$$\sum_{d|M}P_{\chi_d}(f)=2^r\mathfrak{y}^0,\quad \mathfrak{y}^0=\sum_{\sigma\in\mathrm{Gal}(H/H^0)}f(\sigma),$$

where $H^0=K(\sqrt{q_1},\cdots,\sqrt{q_r})$. Remark that $\mathfrak{y}^0$ is usually called the genus period (see [18]). It follows that

$$P_{\chi_1}(f)+P_{\chi_M}(f)+\sum_{\substack{d|M\\ d\neq 1,M}}P_{\chi_d}(f)\equiv 0 \bmod 2^r. \tag{5.9}$$

By the induction hypothesis and the formula (5.8), for all $d\neq 1,M$, we have

$$\mathrm{ord}_2(P_{\chi_d}(f))=\frac{1}{2}\left((\mu(d)-1)+(\mu(-pM/d)-1)+1\right)=\frac{r}{2}.$$

The number of $d\mid M$ with $d\neq 1,M$ is even, and hence the congruence (5.9) gives

$$P_{\chi_1}(f)+P_{\chi_M}(f)\equiv 0 \bmod 2^{r/2}. \tag{5.10}$$

Applying the formula (5.8), we have

$$\frac{1}{6}|P_{\chi_1}(f)|^2=L^{(\mathrm{alg})}(A,1)L^{(\mathrm{alg})}(A^{(-pM)},1),$$
$$\frac{1}{6}|P_{\chi_M}(f)|^2=L^{(\mathrm{alg})}(A^{(M)},1)L^{(\mathrm{alg})}(A^{(-p)},1).$$

If we denote by $x = \mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(M)}, 1))$ and $y = \mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-pM)}, 1))$, then we have

$$\mathrm{ord}_2(P_{\chi_1}(f)) = \frac{y}{2}, \quad \mathrm{ord}_2(P_{\chi_M}(f)) = \frac{x+1}{2}.$$

Theorem 5.3 tells us that $x + y = 2r - 1$. By (5.10), we conclude that $x = r - 1$ and $y = r$. This completes the proof of the theorem for r even.

For r odd, one can prove the assertion using a similar argument as above. We omit the details. □

Finally, we shall prove the assumption (5.1) to complete the proofs of Theorem 5.3 and Theorem 5.4.

Proposition 5.5. *Let p be a prime congruent to 3 mod 8 which is inert in $\mathbb{Q}(\sqrt{-7})$. Then we have*

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-p)}, 1)) = 0.$$

Proof. The proof is similar to that of Theorem 5.3 and Theorem 5.4. Take $M = 5$. In the setting of Theorem 5.3, the equation (5.3) is given by

$$y_1 + y_5 = 2y^0 \equiv \begin{cases} 2 \bmod 4 & \text{if 5 is inert in } K, \\ 0 \bmod 4 & \text{if 5 is split in } K. \end{cases}$$

Since the class number of K is odd, we know that $\mathrm{ord}_2(P_{\chi_1}(f_1)) = 0$. If 5 is inert in K, by (5.4) we have $y_1 \equiv a_5 \cdot P_{\chi_1}(f_1) \equiv 0 \bmod 4$, and if 5 is split in K, by (5.7) we have $y_1 \equiv 2 \cdot P_{\chi_1}(f_1) \equiv 2 \bmod 4$. Thus we have $\mathrm{ord}_2(y_5) = 1$ and $\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(5)}, 1)L^{(\mathrm{alg})}(A^{(-5p)}, 1)) = 1$. Since $L^{(\mathrm{alg})}(A^{(5)}, 1) = 3$, we have

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-5p)}, 1)) = 1. \tag{5.11}$$

On the other hand, in the setting of Theorem 5.4, the congruence (5.9) is given by

$$P_{\chi_1}(f) + P_{\chi_5}(f) \equiv 0 \bmod 2.$$

Applying the formula (5.8), we have

$$\frac{1}{3}|P_{\chi_1}(f)|^2 = L^{(\mathrm{alg})}(A, 1)L^{(\mathrm{alg})}(A^{(-5p)}, 1), \quad \frac{1}{3}|P_{\chi_5}(f)|^2 = L^{(\mathrm{alg})}(A^{(5)}, 1)L^{(\mathrm{alg})}(A^{(-p)}, 1),$$

noting that r is odd in this case. By (5.11), we conclude that $\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(-p)}, 1)) = 0$. □

5.3. More twists

We will now consider a square free integer M in the main theorem of this paper, say

$$M = (-1)^t \cdot q_1 \cdots q_r \cdot p_1 \cdots p_t,$$

where the primes $q_i \equiv 5 \bmod 8$ and the primes $p_j \equiv 3 \bmod 8$ are inert in $\mathbb{Q}(\sqrt{-7})$. For the cases where $t = 0, 1$, we obtained the desired results in Theorem 5.4. We will use similar arguments as above, but we should note that $a_{p_j} \equiv 2 \bmod 4$, see Lemma 3.1. The following theorem proves (2.3).

Theorem 5.6. *Let $M = (-1)^t \cdot q_1 \cdots q_r \cdot p_1 \cdots p_t$ be a square free integer, where the primes $q_i \equiv 5 \bmod 8$ and the primes $p_j \equiv 3 \bmod 8$ are inert in $\mathbb{Q}(\sqrt{-7})$. Then we have*

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(A^{(M)}, 1)) = r + t - 1.$$

Proof. We will use induction on t. When $t = 0$, the assertion has been proved in Theorem 5.4. We now assume that $t > 0$ and that the result holds for every divisor $d \mid M$ with $d \neq M$.

For t even, we take $K = \mathbb{Q}(\sqrt{-p_1})$ and χ to be the quadratic character over K associated to the extension $K(\sqrt{M})/K$. Note that the conductor of χ is equal to $M' = M/p_1$ so that we write $\chi = \chi_{M'}$. As in Proposition 4.3, we have the explicit Waldspurger formula for $(A, \chi_{M'})$

$$L^{(\mathrm{alg})}(A^{(M)}, 1) L^{(\mathrm{alg})}(A^{(-M/p_1)}, 1) = \frac{|P_{\chi_{M'}}(f)|^2}{6},$$

where f is a primitive integral Gross–Prasad test vector for $(A, \chi_{M'})$. By the induction hypothesis, it suffices to show that $\mathrm{ord}_2(P_{\chi_{M'}}(f)) = r + t$. Let

$$y_d = \sum_{\sigma \in \mathrm{Gal}(H_{M'}/K)} f(\sigma) \chi_d(\sigma)$$

so that $y_{M'} = P_{\chi_{M'}}(f)$, and let $H^0_{M'} = K(\sqrt{q_1}, \cdots, \sqrt{q_r}, \sqrt{-p_2}, \cdots, \sqrt{-p_t})$ be the subfield of $H_{M'}$. Note that its index $[H_{M'} : H^0_{M'}]$ is even. As (5.3), we have

$$\sum_{d \mid M'} y_d = 2^{r+t} y^0 \equiv 0 \bmod 2^{r+t+1}. \tag{5.12}$$

To simplify the notation, we write $R = q_1 \cdots q_r$ and $N = p_2 \cdots p_r$ so that $M' = RN$. We also write R_+ (respectively, R_-) for the product of the primes dividing R, which are split (respectively, inert) in K, and similarly for N_+ and N_-. If there exists a prime $q \mid R_-$ such that $qd \mid M'$, then the argument (5.4) shows that

$$\mathrm{ord}_2(y_d) \geq r + t + 1.$$

On the other hand, if there exists a prime $p \mid N_+$ such that $pd \mid M'$, then the argument (5.7) also shows that

$$\mathrm{ord}_2(y_d) \geq r + t + 1.$$

Hence the congruence (5.12) becomes

$$y_{M'} + \sum_{\substack{d \mid M' \\ R_- N^+ \mid d,\ d \neq M'}} y_d \equiv 0 \bmod 2^{r+t+1}.$$

Similarly, the arguments (5.4) and (5.7) show that $\mathrm{ord}_2(y_d) = r + t$ for all y_d in the summation. Hence we conclude that $\mathrm{ord}_2(y_{M'}) = r + t$.

For t odd, we take $K = \mathbb{Q}(\sqrt{-p_1})$, $M'' = -M/p_1$, and $\chi = \chi_{M''}$ to be the quadratic character over K associated to the extension $K(\sqrt{M''})/K$. We also have the explicit Waldspurger formula for $(A, \chi_{M''})$

$$L^{(\mathrm{alg})}(A^{(M'')}, 1) L^{(\mathrm{alg})}(A^{(M)}, 1) = \frac{|P_{\chi_{M''}}(f)|^2}{6},$$

and hence it suffices to show that $\mathrm{ord}_2(P_{\chi_{M''}}(f)) = r + t$. The proof is similar as above. We omit the proof of this case. □

6. Proof of the main theorem

The 2-adic valuations (2.3) of the L-values for the quadratic twists $A^{(M)}$ have been computed in the previous section. To complete the proof of Theorem 1.1, we should compute the Tamagawa factors for $A^{(M)}$. In this section, we assume that M is an arbitrary square free non-zero odd integer with $(M, 7) = 1$. Let $c_p(A^{(M)})$ denote the Tamagawa factor for $A^{(M)}$ at a finite prime p, and let $c_\infty(A^{(M)})$ be the number of connected components of $A^{(M)}$. The $A^{(M)}$ has bad additive reduction at all primes dividing M. We have (cf. Lemma 37 of [8])

$$\mathrm{ord}_2(c_p(A^{(M)})) = \mathrm{ord}_2(A(\mathbb{Q}_p)[2]) \tag{6.1}$$

for all $p \mid M$. The following proposition (see also Proposition 6.3 of [5]) computes all Tamagawa factors for $A^{(M)}$, and in particular, it completes the proof of Theorem 1.1.

Proposition 6.1. *Let M be a square free odd non-zero integer. Then we have*

(1) $A^{(M)}(\mathbb{R})$ *has only one connected component,*
(2) $c_2(A^{(M)})$ *is equal to* 2, 6 *or* 4, *according as* $M \equiv 1, 5 \bmod 8$ *or otherwise,*
(3) $c_7(A^{(M)})$ *is equal to* 1, 3 *or* 4, *according as* $\left(\frac{M}{7}\right) = -1, 1$ *or* 0,
(4) $c_q(A^{(M)}) = 2$ *if q is a prime dividing M which is inert in* $\mathbb{Q}(\sqrt{-7})$, *and*

(5) $c_q(A^{(M)}) = 4$ *if* q *is a prime dividing* M *which is split in* $\mathbb{Q}(\sqrt{-7})$.

Proof. The assertion (1) is clear from the fact that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{-7})$. For any prime $q \mid M$, we have $c_q(A^{(M)}) \leq 4$. Hence the assertions (4) and (5) follows immediately from (6.1), noting that $A(\mathbb{Q}_q)[2]$ is of order 2 or 4, according as q is inert or split in $\mathbb{Q}(\sqrt{-7})$. For $c_7(A^{(M)})$, Tate's algorithm (see Chapter IV of [16]) shows that its Kodaira symbol is I_3 or I_3^*, according as M is divisible by 7 or not. Moreover, $A^{(M)}$ has split multiplicative reduction at 7 if and only if $\left(\frac{M}{7}\right) = 1$. Note that the j-invariant is equal to $2^{-6}5^3 7^{-3} 43^3$. This implies the assertion (3). Similarly, for $c_2(A^{(M)})$, the Kodaira symbol is I_{14}^*, I_6 or I_{10}^* according as M is even, $\equiv 1$ or $\equiv 3 \bmod 4$. Further if $M \equiv 1 \bmod 4$, $A^{(M)}$ has split multiplicative reduction at 2 if and only if $M \equiv 1 \bmod 8$. This proves the assertion (2). □

References

[1] M. Bertolini, H. Darmon, Heegner points on Mumford–Tate curves, Invent. Math. 126 (3) (1996) 413–456.
[2] D. Bump, S. Friedberg, J. Hoffstein, Non-vanishing theorems for L-functions for modular forms and their derivatives, Invent. Math. 102 (1990) 543–618.
[3] L. Cai, Y. Chen, Y. Liu, Heegner points on modular curves, Trans. Am. Math. Soc. 370 (5) (2018) 3721–3743.
[4] L. Cai, Y. Li, Z. Wang, Special automorphisms on Shimura curves and non-triviality of Heegner points, Sci. China Math. 59 (7) (2016) 1307–1326.
[5] L. Cai, C. Li, S. Zhai, On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves, J. Lond. Math. Soc. 101 (2) (2020) 714–734.
[6] L. Cai, J. Shu, Y. Tian, Explicit Gross–Zagier formula and Waldspurger formulae, Algebra Number Theory 8 (10) (2014) 2523–2572.
[7] J. Coates, Y. Li, Y. Tian, S. Zhai, Quadratic twists of elliptic curves, Proc. Lond. Math. Soc. (3) 110 (2) (2015) 357–394.
[8] J. Coates, Lectures on the Birch-Swinnerton-Dyer conjecture, in: Notices of the ICCM, 2013.
[9] T. Dokchitser, V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, Ann. Math. 172 (2010) 567–596.
[10] B. Gross, Local orders, root numbers, and modular curves, Am. J. Math. 110 (6) (1988) 1153–1182.
[11] K. Kato, p-adic Hodge theory and values of zeta functions and modular forms, in: Cohomologies p-adiques et applications arithmétiques. III, in: Astérisque, vol. 295, 2004, ix, 117–290.
[12] J. Nekovář, The Euler System Method for CM Points on Shimura Curves, L-Functions and Galois Representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 471–547.
[13] V. Pal, Periods of quadratic twists of elliptic curves, with an appendix by Amod Agashe, Proc. Am. Math. Soc. 140 (5) (2012) 1513–1525.
[14] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math. 103 (1991) 25–68.
[15] J. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts Math., vol. 106, Springer, 2009.
[16] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts Math., vol. 151, Springer, 1994.
[17] C. Skinner, E. Urban, The Iwasawa main conjecture for GL_2, Invent. Math. 195 (2014) 1–277.
[18] Y. Tian, X. Yuan, S. Zhang, Genus periods, genus points and congruent number problem, Asian J. Math. 21 (4) (2017) 721–773.