ON THE 2-PART OF THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR QUADRATIC TWISTS OF ELLIPTIC CURVES

LI CAI, CHAO LI, SHUAI ZHAI

Abstract. In the present paper, we prove, for a large class of elliptic curves defined over $\mathbb{Q}$, the existence of an explicit infinite family of quadratic twists with analytic rank 0. In addition, we establish the 2-part of the conjecture of Birch and Swinnerton-Dyer for many of these infinite families of quadratic twists. Recently, Xin Wan has used our results to prove for the first time the full Birch–Swinnerton-Dyer conjecture for some explicit infinite families of elliptic curves defined over $\mathbb{Q}$ without complex multiplication.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor C, and complex L-series $L(E,s)$. The Birch and Swinnerton-Dyer conjecture asserts that the rank of $E(\mathbb{Q})$ is equal to its analytic rank $r_{\mathrm{an}} := \mathrm{ord}_{s=1}L(E,s)$. It furthermore predicts that the Tate–Shafarevich group $Ш(E)$ is always finite, and that

$$\frac{L^{(r_{\mathrm{an}})}(E,1)}{r_{\mathrm{an}}!\Omega(E)R(E)} = \frac{\prod_\ell c_\ell(E)\cdot |Ш(E)|}{|E(\mathbb{Q})_{\mathrm{tor}}|^2}, \tag{1.1}$$

where $\Omega(E)$ is the Tamagawa factor at infinity, $R(E)$ is the regulator formed with the Néron–Tate pairing, $E(\mathbb{Q})_{\mathrm{tor}}$ is the torsion subgroup of $E(\mathbb{Q})$, and the $c_\ell(E)$ are the Tamagawa factors (see [18], for example). In fact, the finiteness of $Ш(E)$ is only known at present when r_{an} is at most 1, in which case it is also known that r_{an} is equal to the rank of $E(\mathbb{Q})$ (see [10], for example).

If p is any prime number, the equality of the powers of p occurring on the two sides of (1.1) is called the p-part of the exact Birch–Swinnerton-Dyer formula (but we should remember that the left hand side of (1.1) is only known at present to be a rational number when r_{an} is at most 1). We stress that, up until now, the full Birch–Swinnerton-Dyer conjecture had never been proven for infinitely many elliptic curves without complex multiplication. Roughly speaking, our present knowledge of Iwasawa theory shows that for a given E, the p-part of the Birch–Swinnerton-Dyer conjecture is valid for all sufficiently large primes p when $r_{\mathrm{an}} \leq 1$. But there are real technical difficulties at present in using Iwasawa theory to prove, in particular, the 2-part of the Birch–Swinnerton-Dyer conjecture. However, we can apply rather classical results on modular symbols to derive the precise 2-adic valuation of the algebraic part of the value of the complex L-series at $s = 1$ in the family of quadratic twists of certain optimal elliptic curves E over $\mathbb{Q}$ with $r_{\mathrm{an}} = 0$ and $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. In particular, for all of these twists, our results show that $r_{\mathrm{an}} = 0$, whence the Mordell–Weil group and the Tate–Shafarevich group of these twists are both finite by the celebrated theorems of

2010 *Mathematics Subject Classification.* 11G05, 11G40.

Li Cai was supported by NSFC (Grants No. 11601255 & 11671380). Chao Li was partially supported by the NSF grant DMS-1802269. Shuai Zhai was supported by NSFC (Grant No. 11601272).

Gross–Zagier and Kolyvagin. Moreover, we can prove the 2-part of exact Birch–Swinnerton-Dyer formula for some of these twists. Happily, Xin Wan has now used some of our results in this paper, combined with deep arguments from Iwasawa theory to prove for the first time the validity of the full Birch–Swinnerton-Dyer conjecture for infinitely many elliptic curves over $\mathbb{Q}$ without complex multiplication (see [19, Appendix]). He employs deep and complicated arguments from Iwasawa theory to establish the p-part of the Birch–Swinnerton-Dyer conjecture for all odd primes p for the elliptic curves in these families. However, it is still not known how to extend these Iwasawa-theoretic arguments to the prime $p = 2$, whereas our elementary arguments work well for $p = 2$. For the current progress on the Birch and Swinnerton-Dyer conjecture, one can see the survey article by Coates [6].

We now denote the left-hand-side of (1.1) by $L^{(alg)}(E, 1)$. In particular, when $r_{\mathrm{an}} = 0$,

$$L^{(alg)}(E, 1) := L(E, 1)/\Omega_E,$$

where Ω_E is equal to Ω_E^+ or $2\Omega_E^+$, depending on whether or not $E(\mathbb{R})$ is connected, and here Ω_E^+ is the least positive real period of a Néron differential on a global minimal Weierstrass equation for E. For each discriminant m of a quadratic extension of $\mathbb{Q}$, we write $E^{(m)}$ for the twist of E by this quadratic extension, and write $L(E^{(m)}, s)$ for its complex L-series. Let ord_2 for the order valuation of $\mathbb{Q}$ at the prime 2, normalized by $ord_2(2) = 1$, and with $ord_2(0) = \infty$. If q be any prime of good reduction for E, let a_q be the trace of Frobenius at q on E, so that $N_q = 1 + q - a_q$ is the number of $\mathbb{F}_q$-points on the reduction of E modulo q. We shall always assume that $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, and we write $E' := E/E(\mathbb{Q})[2]$ for the 2-isogenous curve of E. For each integer $n > 1$, write $E[n]$ for the Galois module of n-division points on E. Let $\mathcal{S}$ be the set of primes

$$\mathcal{S} = \{q \equiv 1 \bmod 4 : q \nmid C, ord_2(N_q) = 1\}.$$

Theorem 1.1. *Let E be an optimal elliptic curve over $\mathbb{Q}$ with conductor C. Assume that*

(1) *E has odd Manin constant;*
(2) *$E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$;*
(3) *$ord_2(L^{(alg)}(E, 1)) = -1$.*

Let $M = q_1 q_2 \cdots q_r$ be a product of r distinct primes in $\mathcal{S}$. Then $L(E^{(M)}, 1) \neq 0$, and we have

$$ord_2(L^{(alg)}(E^{(M)}, 1)) = r - 1.$$

In particular, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are both finite.

Remark 1.2. This theorem generalises [5, Theorem 1.2] (where $E = X_0(49)$) and [1, Theorem 1.3] (where $E = X_0(36)$) to a much wider class of elliptic curves E, with no hypothesis of complex multiplication. It also generalises [20, Theorem 1.5 and 1.7] and [14], where only prime twists are considered. For similar results for E without rational 2-torsion, see [20] and [13]. In the presence of rational 2-torsion, the methods of [20] and [14] cannot easily treat twists by non-prime quadratic discriminants, because the obvious induction argument fails. We overcome this difficulty by introducing a new integrality argument to make the induction work.

Remark 1.3. If $\mathcal{S}$ is non-empty, we must have $E(\mathbb{Q})[2] \cong E'(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, which is also equivalent to the assertion that q is inert in both the 2-division field $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E'[2])$ (see [14, Lemma 4.1]), where as before $E' := E/E(\mathbb{Q})[2]$. Thus, by Chebotarev's density theorem, the set of primes $\mathcal{S}$ has positive density.

Remark 1.4. We suppose that the Manin constant of E has to be odd, which will be fully discussed in Section 2. However, we can remove the Manin constant assumption when $4 \nmid C$ by the recent work of Česnavičius [3]. Moreover, the conjecture that the Manin constant is always ± 1 has been proved by Cremona for all optimal elliptic curves of conductor less than 390000 (see [8]).

Our second main result is a proof of the 2-part of the Birch and Swinnerton-Dyer conjecture for many of the twists in Theorem 1.1. As before, let $E' := E/E(\mathbb{Q})[2]$ be the 2-isogenous curve of E.

Theorem 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) $Ш(E')[2] = 0$;
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

Remark 1.6. In view of our assumption that $\#(E(\mathbb{Q})[2]) = 2$, the 2-part of the Birch and Swinnerton-Dyer conjecture for E would show that our hypothesis that $ord_2(L^{(alg)}(E,1)) = -1$ implies that $Ш(E)[2] = 0$, but it is still not known how to prove this at present. However, if we assume that the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E, as well as the hypotheses of Theorem 1.1, we will have $Ш(E)[2] = 0$. Moreover, if we assume two more conditions on $Ш(E')[2]$ and ℓ, then we can compare the local conditions of the Selmer groups of E and $E^{(M)}$, and get the triviality of $Ш(E^{(M)})[2]$.

Remark 1.7. The 2-part of Birch–Swinnerton-Dyer conjecture for a single elliptic curve (of small conductor) can be verified by numerical calculation when $r_{\mathrm{an}} = 0$. Theorem 1.5 then allows one to deduce the 2-part of Birch–Swinnerton-Dyer conjecture for many of its quadratic twists (of arbitrarily large conductor).

Remark 1.8. We emphasize that the theorem applies to elliptic curves with various different reduction types at 2, such as $X_0(14)$ with non-split multiplicative reduction at 2, "$34A1$" with split multiplicative reduction at 2, and "$99C1$" with good ordinary reduction at 2 (we use Cremona's label for each curve). We emphasize that it also applies to elliptic curves with potentially supersingular reduction at 2, such as $X_0(36)$ and "$56B1$". We will give a detailed descriptions of quadratic twists of $X_0(14)$ and some numerical examples in Section 6. Of course, the theorem could apply more families of elliptic curves, such as quadratic twists of "$46A1$", $X_0(49)$, "$66A1$", "$66C1$" and so on.

Recently, a remarkable preprint of Smith [17] uses some arithmetic properties of elliptic curves at the prime 2 to establish some deep results conjectured by Goldfeld (in particular, that the set of all square free congruent numbers congruent to $1, 2, 3$ modulo 8 has natural density zero). However, Smith's analytic arguments at present seem only valid for elliptic curves with full rational 2-torsion. We should mention that the non-vanishing result presented in this paper could give a much weaker result in the direction of Goldfeld's conjecture for the family of elliptic curves in Theorem 1.1. We also remark that it would be possible to prove analogous results to those established here for rank one quadratic twists of elliptic curves, by combining the Heegner points arguments (see [5]) and the explicit Gross–Zagier formula (see [2]).

Acknowledgments. We would like to thank John Coates for very helpful discussions, advices and comments, thank Jack Thorne for his useful comments and suggestions, and thank Jianya Liu and Ye Tian for their encouragement, and thank the referee for the useful comments. The second-named author (CL) and the third-named author (SZ) would also like to thank X. Wan and the Morningside Center of Mathematics for the hospitality during their visits.

2. Modular symbols

Modular symbols were first used by Birch, and a little later by Manin [15]. They subsequently became the basic tool in Cremona's construction of his remarkable tables of elliptic curves and their arithmetic invariants [7]. We shall show in this paper that they are also very useful in studying the 2-part of the conjecture of Birch and Swinnerton-Dyer. We first recall some basic results of modular symbols, for more details, one can see [20], but we shall give these results as well for reading convenience.

For each integer $C \geq 1$, let $S_2(\Gamma_0(C))$ be the space of cusp forms of weight 2 for $\Gamma_0(C)$. In what follows, f will always denote a normalized primitive eigenform in $S_2(\Gamma_0(C))$, all of whose Fourier coefficients belong to $\mathbb{Q}$. Thus f will correspond to an isogeny class of elliptic curves defined over $\mathbb{Q}$, and we will denote by E the unique *optimal* elliptic curve in the $\mathbb{Q}$-isogeny class of E. The complex L-series $L(E,s)$ will then coincide with the complex L-series attached to the modular form f. Moreover, there will be a non-constant rational map defined over $\mathbb{Q}$

$$\varphi : X_0(C) \to E,$$

which does not factor through any other elliptic curve in the isogeny class of E. Let ω denote a Néron differential on a global minimal Weierstrass equation for E. Then, writing $\varphi^*(\omega)$ for the pull back of ω by φ, there exists $\nu_E \in \mathbb{Q}^\times$ such that

$$\nu_E f(\tau) d\tau = \varphi^*(\omega). \tag{2.1}$$

The rational number ν_E is called the *Manin constant*. It is well known to lie in $\mathbb{Z}$, and it is conjectured to always be equal to 1. Moreover, it is known to be odd whenever the conductor C of E is odd. Let $\mathcal{H}$ be the upper half plane, and put $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Let g be any element of $\Gamma_0(C)$. Let α, β be two points in $\mathcal{H}^*$ such that $\beta = g\alpha$. Then any path from α to β on $\mathcal{H}^*$ is a closed path on $X_0(C)$ whose homology class only depends on α and β. Hence it determines an integral homology class in $H_1(X_0(C), \mathbb{Z})$, and we denote this homology class by the *modular symbol* $\{\alpha, \beta\}$. We can then form the modular symbol

$$\langle \{\alpha, \beta\}, f \rangle := \int_\alpha^\beta 2\pi i f(z) dz.$$

The period lattice Λ_f of the modular form f is defined to be the set of these modular symbols for all such pairs $\{\alpha, \beta\}$. It is a discrete subgroup of $\mathbb{C}$ of rank 2. If $\mathfrak{L}_E$ denotes the period lattice of a Néron differential ω on E, it follows from (2.1) that

$$\mathfrak{L}_E = \nu_E \Lambda_f. \tag{2.2}$$

Define Ω_E^+ (resp. $i\Omega_E^-$) to be the least positive real (resp. purely imaginary) period of a Néron differential of a global minimal equation for E, and Ω_f^+ (resp. $i\Omega_f^-$) to be the least positive real (resp. purely imaginary) period of f. Thus, by (2.2), we have

$$\Omega_E^+ = \nu_E \Omega_f^+, \quad \Omega_E^- = \nu_E \Omega_f^-. \tag{2.3}$$

In this section, we will carry out all of our computations with the period lattice Λ_f, but whenever we subsequently translate them into assertions about the conjecture of Birch and Swinnerton-Dyer for the elliptic curve E, we must switch to the period lattice $\mathfrak{L}_E$ by making use of (2.2).

More generally, if α, β are any two elements of $\mathcal{H}^*$, and g is any element of $S_2(\Gamma_0(C))$, we put $\langle\{\alpha,\beta\}, g\rangle := \int_\alpha^\beta 2\pi i g(z)dz$. This linear functional defines an element of $H_1(X_0(C), \mathbb{R})$, which we also denote by $\{\alpha, \beta\}$.

Let m be a positive integer satisfying $(m, C) = 1$. Let a_m be the Fourier coefficient of the modular form f attached to E. According to Birch, Manin [15, Theorem 4.2] and Cremona [7, Chapter 3], we have the following formulae:-

$$(\sum_{l|m} l - a_m)L(E,1) = -\sum_{\substack{l|m \\ k \bmod l}} \langle\{0, \frac{k}{l}\}, f\rangle; \tag{2.4}$$

here l runs over all positive divisors of m; and

$$L(E,\chi,1) = \frac{g(\bar{\chi})}{m}\sum_{k \bmod m} \chi(k)\langle\{0,\frac{k}{m}\}, f\rangle; \tag{2.5}$$

here χ is any primitive Dirichlet character modulo m, and $g(\bar{\chi}) = \sum_{k \bmod m} \bar{\chi}(k)e^{2\pi i\frac{k}{m}}$.

For each odd square-free positive integer m, we define $r(m)$ to be the number of prime factors of m. Also, in what follows, we shall always only consider the positive divisors of m, and define χ_m to be the primitive quadratic character modulo m. Define

$$S_m := \sum_{k=1}^{m}\langle\{0,\frac{k}{m}\}, f\rangle, \quad S'_m := \sum_{\substack{k=1 \\ (k,m)=1}}^{m} \langle\{0,\frac{k}{m}\}, f\rangle, \quad T_m := \sum_{k=1}^{m}\chi_m(k)\langle\{0,\frac{k}{m}\}, f\rangle.$$

Recall that (see [20, Lemma 2.2]), for each odd square-free positive integer $m > 1$, we have

$$\sum_{l|m} S_l = \sum_{d=1}^{r(m)} 2^{r(m)-d} \sum_{\substack{n|m \\ r(n)=d}} S'_n. \tag{2.6}$$

We repeatedly use the above identity to prove the following lemma.

Lemma 2.1. *Let E be the optimal elliptic curve over $\mathbb{Q}$ attached to f. Let m be any integer of the form $m = q_1q_2\cdots q_{r(m)}$, with $(m, C) = 1$, $r(m) \geq 1$, and $q_1, \ldots, q_{r(m)}$ arbitrary distinct odd primes. Then we have*

$$N_{q_1}N_{q_2}\cdots N_{q_{r(m)}}L(E,1) = \sum_{d=1}^{r(m)}\sum_{\substack{n|m \\ r(n)=d}} b_n S'_n,$$

where $b_n = (-1)^{r(m)}\prod_{q|\frac{m}{n}}(1-q)$, here q runs over the prime factors of $\frac{m}{n}$.

Proof. We give the proof of the lemma by induction on $r(m)$, the number of prime factors of m. The assertion is true for $r(m) = 1$ by (2.4). Assume next that $r(m) = 2$. Note that

$$\begin{aligned} N_{q_1}N_{q_2} &= -((1+q_1)(1+q_2) - (1+q_1-N_{q_1})(1+q_2-N_{q_2})) + (1+q_2)N_{q_1} + (1+q_1)N_{q_2} \\ &= -((1+q_1)(1+q_2) - a_{q_1}a_{q_2}) + (1+q_2)N_{q_1} + (1+q_1)N_{q_2}, \end{aligned}$$

and in view of (2.4) and (2.6), we then have that

$$\begin{aligned} N_{q_1}N_{q_2}L(E,1) &= \sum_{l|q_1q_2} S_l - ((1+q_2)S_{q_1} + (1+q_1)S_{q_2}) \\ &= (1-q_2)S_{q_1} + (1-q_1)S_{q_2} + S'_{q_1q_2}, \end{aligned}$$

as required. Now assume that $r(m) > 2$, and that the lemma is true for all divisors $n > 1$ of m with $n \neq m$. We then consider the case $m = q_1q_2\cdots q_{r(m)}$. First note that

$$\begin{aligned} N_{q_1}N_{q_2}\cdots N_{q_{r(m)}} =& (-1)^{r(m)-1}((1+q_1)(1+q_2)\cdots(1+q_{r(m)}) - a_{q_1}a_{q_2}\cdots a_{q_{r(m)}}) \\ &+ (-1)^{r(m)-2}\sum_{i=1}^{r(m)} N_{q_i}\prod_{\substack{k=1\\k\neq i}}^{r(m)}(1+q_k) + (-1)^{r(m)-3}\sum_{i,j=1}^{r(m)} N_{q_i}N_{q_j}\prod_{\substack{k=1\\k\neq i,j}}^{r(m)}(1+q_k) \\ &+ \cdots + (-1)\sum_{i,j=1}^{r(m)}(1+q_i)(1+q_j)\prod_{\substack{k=1\\k\neq i,j}}^{r(m)} N_{q_k} + \sum_{i=1}^{r(m)}(1+q_i)\prod_{\substack{k=1\\k\neq i}}^{r(m)} N_{q_k}. \end{aligned}$$

Without loss of generality, here we can just consider the coefficients of S'_{q_1}, $S'_{q_1q_2}$, …, $S'_{q_1q_2\cdots q_{r(m)}}$ in the identity of the lemma, i.e. b_{q_1}, $b_{q_1q_2}$, …, $b_{q_1q_2\cdots q_{r(m)}}$. By our assumption, and again in view of (2.4) and (2.6), we conclude that

$$\begin{aligned} b_{q_1} =& -(-1)^{r(m)-1}2^{r(m)-1} + (-1)^{r(m)-1}\prod_{i=2}^{r(m)}(1+q_i) + (-1)^{r(m)-1}\sum_{i=2}^{r(m)}(1-q_i)\prod_{\substack{k=2\\k\neq i}}^{r(m)}(1+q_k) \\ &+ (-1)^{r(m)-1}\sum_{\substack{i,j=2\\i\neq j}}^{r(m)}(1-q_i)(1-q_j)\prod_{\substack{k=2\\k\neq i,j}}^{r(m)}(1+q_k) + \cdots + (-1)^{r(m)-1}\sum_{i=2}^{r(m)}(1+q_i)\prod_{\substack{k=2\\k\neq i}}^{r(m)}(1-q_k). \end{aligned}$$

Note that

$$-2^{r(m)-1} = -\prod_{i=2}^{r(m)}((1-q_i)+(1+q_i)),$$

hence we have

$$b_{q_1} = (-1)^{r(m)}\prod_{i=2}^{r(m)}(1-q_i).$$

Similar arguments hold for $b_{q_1q_2}, \ldots, b_{q_1q_2\cdots q_{r(m)-1}}$, and it is easy to see that

$$b_{q_1q_2\cdots q_{r(m)}} = (-1)^{r(m)}.$$

The proof of the lemma is complete. □

Lemma 2.2. *Let E be the optimal elliptic curve over $\mathbb{Q}$ with analytic rank zero attached to f. Let m be any integer of the form $m = q_1q_2\cdots q_{r(m)}$, with $(m, C) = 1$, $r(m) \geq 1$, and $q_1, \ldots, q_{r(m)}$ arbitrary distinct odd primes congruent to 1 modulo 4. If $ord_2(N_{q_i}) = 1$ holds for any $1 \leq i \leq r(m)$, then we have*

$$ord_2(S'_m/\Omega_f^+) = ord_2(N_{q_1}N_{q_2}\cdots N_{q_{r(m)}}L(E,1)/\Omega_f^+).$$

Proof. We give the proof of the lemma by induction on $r(m)$. The assertion is obviously true for $r(m) = 1$ according as (2.4). When $r(m) = 2$, say $m = q_1q_2$, by Lemma 2.1, we have that

$$N_{q_1}N_{q_2}L(E,1) = (1-q_2)S'_{q_1} + (1-q_1)S'_{q_2} + S'_{q_1q_2}.$$

The assertion for $r(m) = 2$ then follows by noting that $q_i \equiv 1 \bmod 4$ and the induction assumption. Now assume that $r(m) > 2$, and that the lemma is true for all divisors $n > 1$ of m with $n \neq m$. We then consider the case $m = q_1q_2\cdots q_{r(m)}$. According to Lemma 2.1, we have that

$$N_{q_1}N_{q_2}\cdots N_{q_{r(m)}}L(E,1) = \sum_{d=1}^{r(m)-1} \sum_{\substack{n|m \\ r(n)=d}} (-1)^{r(m)} \prod_{q|\frac{m}{n}} (1-q)S'_n + (-1)^{r(m)}S'_m.$$

By our assumption, it is not difficult to see that

$$ord_2(\prod_{q|\frac{m}{n}}(1-q)S'_n/\Omega_f^+) > ord_2(N_{q_1}N_{q_2}\cdots N_{q_{r(m)}}L(E,1)/\Omega_f^+)$$

holds for all divisors $n > 1$ of m with $n \neq m$. Then the assertion for $m = q_1q_2\cdots q_{r(m)}$ follows immediately. This completes the proof of the lemma. □

3. Integrality at 2

Let E be the optimal elliptic curve defined over $\mathbb{Q}$ with discriminant Δ_E and conductor C, which is attached to our modular form f. In this section, we will prove some results of integrality at 2, and apply them to get the non-vanishing results for some certain quadratic twists of elliptic curves, provided $L(E,1) \neq 0$. Recall that

$$\Omega_E^+ = \nu_E\Omega_f^+,$$

we then have

$$ord_2(L(E,1)/\Omega_E^+) = ord_2(L(E,1)/\Omega_f^+) - ord_2(\nu_E) = ord_2(L(E,1)/\Omega_f^+),$$

under our assumption on the Manin constant.

When the complex L-series of E does not vanish at $s = 1$, for every prime number p, the strong Birch–Swinnerton-Dyer conjecture predicts the following exact formula

$$ord_p(L^{(alg)}(E,1)) = ord_p(\#(Ш(E))) + ord_p(\prod_{\ell|C} c_\ell(E)) - 2ord_p(\#(E(\mathbb{Q}))),$$

We begin by establishing some preliminary results, which will be needed for the proof of the desired results. Throughout this section, we will always assume $m \equiv 1 \bmod 4$. Since the form of the period lattice of a Néron differential on E is different, according as the sign of the discriminant of E. We first consider the case when the discriminant of E is negative.

Recall that when the discriminant of E is negative, then $E(\mathbb{R})$ has only one real component, and so the period lattice $\mathfrak{L}$ of a Néron differential on E has a $\mathbb{Z}$-basis of the form

$$\left[\Omega_E^+, \frac{\Omega_E^+ + i\Omega_E^-}{2}\right],$$

where Ω_E^+ and Ω_E^- are both real, and the period lattice Λ_f of f has a $\mathbb{Z}$-basis of the form

$$\left[\Omega_f^+, \frac{\Omega_f^+ + i\Omega_f^-}{2}\right],$$

where Ω_f^+ and Ω_f^- are also both real. We can then write

$$\langle\{0, \frac{k}{m}\}, f\rangle = (s_{k,m}\Omega_f^+ + it_{k,m}\Omega_f^-)/2 \tag{3.1}$$

for any integer m coprime to C, where $s_{k,m}, t_{k,m}$ are integers of the same parity. Moreover, by the basic property of modular symbols, $\langle\{0, \frac{k}{m}\}, f\rangle$ and $\langle\{0, \frac{m-k}{m}\}, f\rangle$ are complex conjugate periods of f. Thus we obtain

$$S'_m/\Omega_f^+ = \sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2} s_{k,m}. \tag{3.2}$$

Similarly, when $m \equiv 1 \bmod 4$, we have

$$T_m/\Omega_f^+ = \sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2} \chi_m(k)s_{k,m}. \tag{3.3}$$

Moreover, in this case, by (3.2), we always have that

$$ord_2(N_q L(E,1)/\Omega_f^+) \geq 0,$$

for any prime q with $(q, C) = 1$. We define

$$T'_{d,m} = \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi_d(k)\langle\{0, \frac{k}{m}\}, f\rangle,$$

then we have the following theorem of integrality at 2.

Theorem 3.1. *Let E be an optimal elliptic curve over $\mathbb{Q}$ with $\Delta_E < 0$. Let m be any integer of the form $m = q_1q_2\cdots q_{r(m)}$, with $(m, C) = 1$, $r(m) \geq 1$, and $q_1, \ldots, q_{r(m)}$ arbitrary distinct odd primes in $\mathcal{S}$. Then*

$$\sum_{d|m} T'_{d,m}/\Omega_f^+ = 2^{r(m)}\Psi_m,$$

where Ψ_m is an integer.

Proof. It is easy to see that

$$\begin{aligned}\sum_{d|m} T'_{d,m} &= \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times}\sum_{d|m} \chi_d(k)\langle\{0, \frac{k}{m}\}, f\rangle\\ &= 2^{r(m)} \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times}^{*} \langle\{0, \frac{k}{m}\}, f\rangle,\end{aligned}$$

where $\sum^*$ means that k runs over all the elements in $(\mathbb{Z}/m\mathbb{Z})^\times$ such that $\chi_{q_i}(k) = 1$ for all $1 \leq i \leq r(m)$. Since $q_i \equiv 1 \bmod 4$, if k is of an element in the above summation, so is $m - k$.

Then by (3.1), we have that

$$\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times}^{*} \langle\{0,\frac{k}{m}\},f\rangle = \sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2,*} s_{k,m}\Omega_f^+.$$

Then the argument follows immediately if we define

$$\Psi_m = \sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2,*} s_{k,m},$$

which is an integer. □

When the discriminant of E is positive, then $E(\mathbb{R})$ has two real components, and so the period lattice $\mathfrak{L}$ of a Néron differential on E has a $\mathbb{Z}$-basis of the form

$$[\Omega_E^+, i\Omega_E^-],$$

with Ω_E^+ and Ω_E^- real numbers, and the period lattice Λ_f of f has a $\mathbb{Z}$-basis of the form

$$[\Omega_f^+, i\Omega_f^-],$$

with Ω_f^+ and Ω_f^- real numbers too. We can then write

$$\langle\{0,\frac{k}{m}\},f\rangle = s_{k,m}\Omega_f^+ + it_{k,m}\Omega_f^- \tag{3.4}$$

for any integer m coprime to C, where $s_{k,m}, t_{k,m}$ are integers. Similarly, we can obtain

$$S'_m/\Omega_f^+ = 2\sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2} s_{k,m}, \tag{3.5}$$

and when $m \equiv 1 \bmod 4$, we have

$$T_m/\Omega_f^+ = 2\sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2} \chi_m(k)s_{k,m}. \tag{3.6}$$

Moreover, in this case, by (3.5), we always have that

$$ord_2(N_qL(E,1)/\Omega_f^+) \geq 1,$$

for any prime q with $(q,C) = 1$. We then have the following parallel theorem of integrality at 2.

Theorem 3.2. *Let E be an optimal elliptic curve over $\mathbb{Q}$ with $\Delta_E > 0$. Let m be any integer of the form $m = q_1q_2\cdots q_{r(m)}$, with $(m,C) = 1$, $r(m) \geq 1$, and $q_1,\ldots,q_{r(m)}$ arbitrary distinct odd primes in $\mathcal{S}$. Then*

$$\sum_{d|m} T'_{d,m}/\Omega_f^+ = 2^{r(m)+1}\Psi_m,$$

where Ψ_m is an integer.

Proof. The proof of the above theorem is similar to Theorem 3.1. As usual, we have

$$\sum_{d|m} T'_{d,m} = \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} \sum_{d|m} \chi_d(k)\langle\{0,\frac{k}{m}\},f\rangle$$
$$= 2^{r(m)} \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times}^{*} \langle\{0,\frac{k}{m}\},f\rangle,$$

where $\sum^*$ means that k runs over all the elements in $(\mathbb{Z}/m\mathbb{Z})^\times$ such that $\chi_{q_i}(k)=1$ for all $1\le i\le r(m)$. Since $q_i\equiv 1 \bmod 4$, if k is of an element in the above summation, so is $m-k$. But when the discriminant is positive, by (3.4), we have

$$\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times}^{*} \langle\{0,\frac{k}{m}\},f\rangle = 2\sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2}{}^{*} s_{k,m}\Omega_f^+.$$

Then the argument follows immediately if we define

$$\Psi_m = \sum_{\substack{k=1\\(k,m)=1}}^{(m-1)/2}{}^{*} s_{k,m},$$

which is an integer. □

4. Non-vanishing results

The aim of this section is to apply the results of integrality at 2 in the previous section to obtain the corresponding non-vanishing results of quadratic twists of elliptic curves. Specifically, we prove the precise 2-adic valuation of the algebraic central value of these L-functions attached to some certain families of quadratic twists of elliptic curves. Moreover, one can use these non-vanishing theorems to verify the 2-part of the Birch and Swinnerton-Dyer conjecture. Throughout this section, we will always assume $m>0$ and $m\equiv 1 \bmod 4$.

Before proving our non-vanishing results, we will first prove the following lemma, in which the action of Hecke operator on modular symbols is involved. For each prime p not dividing the conductor C, the Hecke operator $\mathbb{T}_p$ acts on modular symbols $\{\alpha,\beta\}$ via

$$\mathbb{T}_p(\{\alpha,\beta\}) = \{p\alpha,p\beta\} + \sum_{k \bmod p} \{\frac{\alpha+k}{p},\frac{\beta+k}{p}\}.$$

In particular, we have

$$\langle\mathbb{T}_p(\{\alpha,\beta\}),f\rangle = \langle\{\alpha,\beta\},\mathbb{T}_p f\rangle = a_p\langle\{\alpha,\beta\},f\rangle,$$

since $\mathbb{T}_p f = a_p f$.

Lemma 4.1. *Let m be any integer of the form $m=q_1q_2\cdots q_{r(m)}$, with $(m,C)=1$, $r(m)\ge 2$, and $q_1,\dots,q_{r(m)}$ arbitrary distinct odd primes. Let $d>1$ be a positive integer dividing m and q be a prime dividing $\frac{m}{d}$, then we have*

$$T'_{d,m} = (a_q - 2\chi_d(q))T'_{d,\frac{m}{q}}.$$

Proof. Recall that

$$T'_{d,m} = \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi_d(k)\langle\{0,\frac{k}{m}\},f\rangle.$$

By the Chinese remainder theorem, we have

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times.$$

So we can write

$$T'_{d,m} = \sum_{k'\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k') \sum_{k\in\mathbb{Z}/q\mathbb{Z}} \langle\{0,\frac{\frac{m}{q}k+k'}{m}\},f\rangle - \sum_{k'\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k'q)\langle\{0,\frac{k'q}{m}\},f\rangle. \tag{4.1}$$

Let the Hecke operator $\mathbb{T}_q$ act on the modular symbol $\{0,\frac{k'}{m/q}\}$, we get that

$$\mathbb{T}_q(\{0,\frac{k'}{m/q}\}) = \{0,\frac{k'}{m}\} + \sum_{k \bmod q} \{0,\frac{\frac{k'}{m/q}+k}{q}\} - \sum_{k \bmod q} \{0,\frac{k}{q}\}.$$

Hence,

$$\sum_{k\in\mathbb{Z}/q\mathbb{Z}} \langle\{0,\frac{\frac{m}{q}k+k'}{m}\},f\rangle = a_q\langle\{0,\frac{k'}{m/q}\},f\rangle + \sum_{k\in\mathbb{Z}/q\mathbb{Z}} \langle\{0,\frac{k}{q}\},f\rangle - \langle\{0,\frac{k'}{m}\},f\rangle.$$

Then the first term of the right-hand side of (4.1) becomes

$$\sum_{k'\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k')(a_q\langle\{0,\frac{k'}{m/q}\},f\rangle + \sum_{k\in\mathbb{Z}/q\mathbb{Z}} \langle\{0,\frac{k}{q}\},f\rangle - \langle\{0,\frac{k'}{m}\},f\rangle),$$

which is equal to

$$\sum_{k\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k)(a_q\langle\{0,\frac{k}{m/q}\},f\rangle - \langle\{0,\frac{k}{m}\},f\rangle), \tag{4.2}$$

since

$$\sum_{k'\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k') = 0.$$

Then (4.2) becomes

$$a_q \sum_{k\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k)\langle\{0,\frac{k}{m/q}\},f\rangle - \sum_{k'\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k'q)\langle\{0,\frac{k'q}{m}\},f\rangle$$

if we substitute $k = k'q$ in the second term. We then have

$$T'_{d,m} = a_q \sum_{k\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k)\langle\{0,\frac{k}{m/q}\},f\rangle - 2\chi_d(q) \sum_{k'\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k')\langle\{0,\frac{k'}{m/q}\},f\rangle.$$

This completes the proof of the lemma by noting that

$$T'_{d,\frac{m}{q}} = \sum_{k\in(\mathbb{Z}/\frac{m}{q}\mathbb{Z})^\times} \chi_d(k)\langle\{0,\frac{k}{m/q}\},f\rangle.$$

□

Now we are ready to prove Theorem 1.1. When the discriminant of E is negative, we have the following result.

Theorem 4.2. *Let E be an optimal elliptic curve over $\mathbb{Q}$ with conductor C, and with odd Manin constant. Assume that E has negative discriminant, and satisfies $E(\mathbb{Q})[2] \neq 0$ and $ord_2(L(E,1)/\Omega_f^+) = -1$. Let m be any integer of the form $m = q_1 q_2 \cdots q_{r(m)}$, with $r(m) \geq 1$ and $q_1, \ldots, q_{r(m)}$ arbitrary distinct odd primes congruent to 1 modulo 4, and with $(m, C) = 1$. If $ord_2(N_{q_i}) = 1$ for $1 \leq i \leq r(m)$, then $L(E^{(m)}, 1) \neq 0$, and we have*

$$ord_2(L(E^{(m)}, 1)/\Omega^+_{E^{(m)}}) = r(m) - 1.$$

Proof. We will prove the theorem by induction on $r(m)$, of course we have got the argument when $r(m) = 1$ in [20, Theorem 1.5]. We firstly note that

$$\begin{aligned}\sum_{d|m} T'_{d,m} &= \sum_{d|m} \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi_d(k)\langle\{0, \frac{k}{m}\}, f\rangle \\ &= S'_m + \sum_{\substack{d|m \\ 1<d<m}} \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi_d(k)\langle\{0, \frac{k}{m}\}, f\rangle + T_m.\end{aligned}$$

By Lemma 4.1, it is easy to see that

$$T'_{d,m} = \prod_{q|\frac{m}{d}} (a_q - 2\chi_d(q)) \cdot T'_{d,d} = \prod_{q|\frac{m}{d}} (a_q - 2\chi_d(q)) \cdot T_d.$$

Hence,

$$\sum_{\substack{d|m \\ 1<d<m}} \sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi_d(k)\langle\{0, \frac{k}{m}\}, f\rangle = \sum_{\substack{d|m \\ 1<d<m}} \prod_{q|\frac{m}{d}} (a_q - 2\chi_d(q)) \cdot T_d.$$

We then apply Theorem 3.1 and get the following equation

$$S'_m/\Omega_f^+ + \sum_{\substack{d|m \\ 1<d<m}} \prod_{q|\frac{m}{d}} (a_q - 2\chi_d(q)) \cdot T_d/\Omega_f^+ + T_m/\Omega_f^+ = 2^{r(m)}\Psi_m,$$

where Ψ_m is an integer with $ord_2(\Psi_m) \geq 0$. Note that $ord_2(L(E,1)/\Omega_f^+) = -1$ and $ord_2(N_{q_i}) = 1$, we then have

$$ord_2(S'_m/\Omega_f^+) = r(m) - 1$$

by Lemma 2.2. Now assume that $r(m) \geq 2$, and that this theorem has been proved for all products of less than $r(m)$ such primes q_i, and note that we have assumed the Manin constant is odd, so we have that

$$ord_2(T_d/\Omega_f^+) = r(d) - 1,$$

with $1 < d < m$ and $d|m$. Moreover, we also have $ord_2(a_q - 2\chi_d(q)) = 1$. Consequently, we have that

$$ord_2(\prod_{q|\frac{m}{d}} (a_q - 2\chi_d(q)) \cdot T_d/\Omega_f^+) = r(m) - 1.$$

Hence we have that

$$ord_2(\sum_{\substack{d|m \\ 1<d<m}} \prod_{q|\frac{m}{d}} (a_q - 2\chi_d(q)) \cdot T_d/\Omega_f^+) = r(m),$$

by noting that the number of the terms in this summation is even. So we must have

$$ord_2(T_m/\Omega_f^+) = r(m) - 1,$$

that is

$$ord_2(L(E^{(m)}, 1)/\Omega^+_{E^{(m)}}) = r(m) - 1.$$

This completes the proof of this theorem. □

When the discriminant of E is positive, we have the following parallel result.

Theorem 4.3. *Let E be an optimal elliptic curve over $\mathbb{Q}$ with conductor C, and with odd Manin constant. Assume that E has positive discriminant, and satisfies $E(\mathbb{Q})[2] \neq 0$ and $ord_2(L(E,1)/\Omega_f^+) = 0$. Let m be any integer of the form $m = q_1 q_2 \cdots q_{r(m)}$, with $r(m) \geq 1$ and $q_1, \ldots, q_{r(m)}$ arbitrary distinct odd primes congruent to 1 modulo 4, and with $(m, C) = 1$. If $ord_2(N_{q_i}) = 1$ for $1 \leq i \leq r(m)$, then $L(E^{(m)}, 1) \neq 0$, and we have*

$$ord_2(L(E^{(m)}, 1)/\Omega^+_{E^{(m)}}) = r(m).$$

Proof. We will also prove the theorem by induction on $r(m)$, of course we have got the argument when $r(m) = 1$ in [20, Theorem 1.7]. Note that $ord_2(L(E,1)/\Omega_f^+) = 0$ and $ord_2(N_{q_i}) = 1$, we then have

$$ord_2(S'_m/\Omega_f^+) = r(m)$$

by Lemma 2.2. Now assume that $r(m) \geq 2$, and that this theorem has been proved for all products of less than $r(m)$ such primes q_i, and note that we have assumed the Manin constant is odd, so we have that

$$ord_2(T_d/\Omega_f^+) = r(d),$$

with $1 < d < m$ and $d|m$. Moreover, we also have $ord_2(a_q - 2\chi_d(q)) = 1$. Consequently, we have that

$$ord_2(\prod_{q|\frac{m}{d}}(a_q - 2\chi_d(q)) \cdot T_d/\Omega_f^+) = r(m).$$

Hence we have that

$$ord_2(\sum_{\substack{d|m \\ 1<d<m}} \prod_{q|\frac{m}{d}}(a_q - 2\chi_d(q)) \cdot T_d/\Omega_f^+) = r(m) + 1,$$

by noting that the number of the terms in this summation is even. So we must have

$$ord_2(T_m/\Omega_f^+) = r(m),$$

by the following equation

$$S'_m/\Omega_f^+ + \sum_{\substack{d|m \\ 1<d<m}} \prod_{q|\frac{m}{d}}(a_q - 2\chi_d(q)) \cdot T_d/\Omega_f^+ + T_m/\Omega_f^+ = 2^{r(m)+1}\Psi_m,$$

which is deduced from Theorem 3.2. Hence we have

$$ord_2(L(E^{(m)}, 1)/\Omega^+_{E^{(m)}}) = r(m).$$

This completes the proof of this theorem. □

This completes the proof of Theorem 1.1 by combining the above two theorems and the celebrated theorems of Gross–Zagier and Kolyvagin.

5. 2-part of the Birch–Swinnerton-Dyer conjecture

In this section, we will prove that the 2-part of the Birch–Swinnerton-Dyer conjecture holds for some certain families of the quadratic twists of elliptic curves in the previous section. In particular, we will prove the following result, combining with the non-vanishing result in Theorem 1.1, to give a proof of Theorem 1.5.

Proposition 5.1. *Let E be an elliptic curve over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Let $M = q_1 \cdots q_r$ be a square free product of r primes in $\mathcal{S}$.*

(1) *Then $E^{(M)}(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$.*

(2) *Let $\ell_0 | C$ be the prime such that $ord_2(c_{\ell_0}(E)) = 1$. Assume ℓ_0 splits in $\mathbb{Q}(\sqrt{M})$ and $ord_2(\prod_\ell c_\ell(E)) = 1$. Then*

$$ord_2(c_\ell(E^{(M)})) = \begin{cases} 0, & \text{if } \ell \neq \ell_0, \text{ and } \ell \nmid M, \\ 1, & \text{if } \ell = \ell_0, \text{ or } \ell | M. \end{cases}$$

In particular, $ord_2(\prod_\ell c_\ell(E^{(M)})) = r + 1$.

(3) *Assume further that $\mathrm{Sel}_2(E)[2] = \mathbb{Z}/2\mathbb{Z}$ and $Ш(E')[2] = 0$. If all primes $\ell | 2C$ split in $\mathbb{Q}(\sqrt{M})$, then $1 \leq \dim \mathrm{Sel}_2(E^{(M)}) \leq 2$. In particular, if $Ш(E^{(M)})$ is finite, then $Ш(E^{(M)})[2] = 0$ and $\mathrm{Sel}_2(E^{(M)}) = \mathbb{Z}/2\mathbb{Z}$.*

Proof. (1) It follows from the facts that $E[2] \cong E^{(M)}[2]$ as $G_{\mathbb{Q}}$-modules and $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$.

(2) First consider $\ell \neq \ell_0$ and $\ell \nmid M$. Let $\mathcal{E}$ and $\mathcal{E}^{(M)}$ be the Néron model over $\mathbb{Z}_\ell$ of E and $E^{(M)}$ respectively. Notice that $E^{(M)}/\mathbb{Q}_\ell$ is the unramified quadratic twist of $E^{(M)}$. Since Néron models commute with unramified base change, we know that the component groups $\Phi_{\mathcal{E}}$ and $\Phi_{\mathcal{E}^{(M)}}$ are quadratic twists of each other as $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$-modules. In particular, $\Phi_{\mathcal{E}}[2] \cong \Phi_{\mathcal{E}^{(M)}}[2]$ as $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$-modules and thus

$$\Phi_{\mathcal{E}}(\mathbb{F}_\ell)[2] \cong \Phi_{\mathcal{E}^{(M)}}(\mathbb{F}_\ell)[2].$$

It follows that $c_\ell(E)$ and $c_\ell(E^{(M)})$ have the same parity, and hence $c_\ell(E^{(M)})$ is odd.

Next consider $\ell | M$. Since $E^{(M)}$ has additive reduction at ℓ and ℓ is odd, we know that

$$\Phi_{\mathcal{E}^{(M)}}(\mathbb{F}_\ell)[2] \cong E^{(M)}(\mathbb{Q}_\ell)[2].$$

On the other hand, $E^{(M)}(\mathbb{Q}_\ell)[2] \cong E(\mathbb{Q}_\ell)[2] \cong E(\mathbb{F}_\ell)[2]$, which is $\mathbb{Z}/2\mathbb{Z}$ since $\ell \in \mathcal{S}$. Thus $ord_2(c_\ell(E^{(M)})) = 1$ for any $\ell | M$.

Finally consider $\ell = \ell_0$. By our extra assumption that ℓ_0 is split in $\mathbb{Q}(\sqrt{M})$, we know that $E^{(M)}/\mathbb{Q}_\ell$ and $E/\mathbb{Q}_\ell$ are isomorphic, hence $c_\ell(E^{(M)}) = c_\ell(E)$, which has 2-adic valuation 1.

(3) Let $\phi : E \to E'$ be the isogeny of degree 2, and $\hat{\phi} : E' \to E$ be the dual isogeny. We use the following well-known exact sequence relating the 2-Selmer group and ϕ, $\hat{\phi}$-Selmer groups (see [16, Lemma 6.1]):-

$$0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to \mathrm{Sel}_\phi(E) \to \mathrm{Sel}_2(E) \to \mathrm{Sel}_{\hat{\phi}}(E') \to Ш(E')[\hat{\phi}]/\phi(Ш(E)[2]) \to 0.$$

By our assumption $\mathrm{Sel}_2(E) = \mathbb{Z}/2\mathbb{Z}$ and $Ш(E')[2] = 0$, it follows from the above exact sequence that

$$\mathrm{Sel}_\phi(E) \cong E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{Sel}_{\hat{\phi}}(E') \cong \mathrm{Sel}_2(E) \cong \mathbb{Z}/2\mathbb{Z}.$$

By abuse of notation we denote the 2-isogeny $E^{(M)} \to E'^{(M)}$ again by ϕ (note that ${E^{(M)}}' = E'^{(M)}$).

We first claim that the isomorphism of $G_{\mathbb{Q}}$-representations $E^{(M)}[\phi] \cong E[\phi]$ induces an isomorphism of ϕ-Selmer groups

$$\mathrm{Sel}_{\phi}(E^{(M)}) \cong \mathrm{Sel}_{\phi}(E).$$

For v a place of $\mathbb{Q}$, we denote the local condition defining the ϕ-Selmer group $\mathrm{Sel}_{\phi}(E)$ to be

$$\mathcal{L}_v(E) := \mathrm{im}(E'(\mathbb{Q}_v)/\phi(E(\mathbb{Q}_v))) \subseteq H^1(\mathbb{Q}_v, E[\phi]).$$

To show the claim it suffices to prove for any v,

$$\mathcal{L}_v(E^{(M)}) = \mathcal{L}_v(E).$$

We now prove the claim by the following 4 cases.
(1) For $v \nmid 2CM\infty$, then both E and E' have good reduction at $v \neq 2$ and hence

$$\mathcal{L}_v(E^{(M)}) = \mathcal{L}_v(E) = H^1_{\mathrm{ur}}(\mathbb{Q}_v, E[\phi])$$

is the unramified condition.
(2) For $v|M$, the desired equality of local condition at v follows from [11, Lemma 6.8].
(3) For $v|2C$, by assumption we have v splits in $\mathbb{Q}(\sqrt{M})$, hence $E^{(M)}$ and E are isomorphic over $\mathbb{Q}_v$, and $E'^{(M)}$ and E' are isomorphic over $\mathbb{Q}_v$. The desired equality of local condition at v follows.
(4) For $v = \infty$, since $M > 0$, we know that $E^{(M)}$ and E are isomorphic over $\mathbb{R}$, and $E'^{(M)}$ and E' are isomorphic over $\mathbb{R}$. The desired equality of local condition at v again follows. This completes the proof of the claim.

Now by [11, Theorem 6.4], we have

$$\frac{|\mathrm{Sel}_{\phi}(E)|}{|\mathrm{Sel}_{\hat{\phi}}(E')|} = \prod_v \frac{|\mathcal{L}_v(E)|}{2}, \quad \frac{|\mathrm{Sel}_{\phi}(E^{(M)})|}{|\mathrm{Sel}_{\hat{\phi}}(E'^{(M)})|} = \prod_v \frac{|\mathcal{L}_v(E^{(M)})|}{2}.$$

Since we have shown that $\mathcal{L}_v(E) = \mathcal{L}_v(E^{(M)})$ for every place v of $\mathbb{Q}$, we obtain

$$\frac{|\mathrm{Sel}_{\phi}(E)|}{|\mathrm{Sel}_{\hat{\phi}}(E')|} = \frac{|\mathrm{Sel}_{\phi}(E^{(M)})|}{|\mathrm{Sel}_{\hat{\phi}}(E'^{(M)})|}.$$

Hence $\mathrm{Sel}_{\hat{\phi}}(E'^{(M)}) \cong \mathbb{Z}/2\mathbb{Z}$. Now the well-known exact sequence for $E^{(M)}$ implies that

$$\dim \mathrm{Sel}_2(E^{(M)}) \leq \dim \mathrm{Sel}_{\phi}(E^{(M)}) + \dim \mathrm{Sel}_{\hat{\phi}}(E'^{(M)}) = 1 + 1 = 2.$$

On the other hand, $E^{(M)}(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, so $\dim \mathrm{Sel}_2(E^{(M)}) \geq 1$. If $Ш(E^{(M)})[2]$ is finite, then by the Cassels–Tate pairing $Ш(E^{(M)})[2]$ has square order, hence by the previous bounds it must be 0, as desired. □

We are now ready to give the proof of Theorem 1.5.

Theorem 5.2. *(Theorem 1.5) Let E and M be as in Theorem 1.1. Assume further that*

(1) $Ш(E')[2] = 0$;
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

Proof. If the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E, then

$$ord_2\left(\frac{\prod_\ell c_\ell(E)\cdot Ш(E)}{|E(\mathbb{Q})_{\mathrm{tor}}|^2}\right)=-1.$$

Since $E(\mathbb{Q})[2]\cong\mathbb{Z}/2\mathbb{Z}$ and $Ш(E)[2]$ has square order, we know that $Ш(E)[2]=0$, $\mathrm{Sel}_2(E)=\mathbb{Z}/2\mathbb{Z}$ and $ord_2(\prod_\ell c_\ell(E))=1$. By Theorem 1.1, we have

$$ord_2(L^{(alg)}E^{(M)},1)=r-1,$$

and $Ш(E^{(M)})$ is finite. The assumptions of Proposition 5.1 are all satisfied, and hence

$$E^{(M)}(\mathbb{Q})[2]=\mathbb{Z}/2\mathbb{Z},\quad ord_2(\prod_{p|CM}(c_p(E^{(M)}))=r+1,\quad Ш(E^{(M)})[2]=0.$$

We then have

$$ord_2\left(\frac{\prod_p c_p(E^M)\cdot Ш(E^{(M)})}{|E^{(M)}(\mathbb{Q})_{\mathrm{tor}}|^2}\right)=r-1.$$

Therefore, the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$. □

6. Applications

In this section we will apply Theorem 1.1 and Theorem 1.5 to give some families of quadratic twists of elliptic curves which satisfy the 2-part of the exact Birch–Swinnerton-Dyer formula. In particular, we give a full discussion of quadratic twists of $X_0(14)$, and some analogous examples on the quadratic twists of "$34A1$", "$56B1$", and "$99C1$ (in Cremona's label), for which we will not give the proofs in details since they are similar to the case of $X_0(14)$, and all the numerical examples are verified by "Magma". Moreover, we also include a family of elliptic curves satisfying the full Birch–Swinnerton-Dyer conjecture. More examples have been included in Wan's paper [19].

In the following, we always denote A' to be the 2-isogenous curve of a given elliptic curve A defined over $\mathbb{Q}$. For each square free integer M, prime to the conductor of A, with $M\equiv 1 \bmod 4$, as usual, we define

$$L^{(alg)}(A^{(M)},1)=L(A^{(M)},1)/\Omega_{A^{(M)}}.$$

6.1. **Quadratic twists of $X_0(14)$.** Let A be the modular curve $X_0(14)$, which has genus 1, and which we view as an elliptic curve by taking $[\infty]$ to be the origin of the group law. It has a minimal Weierstrass equation given by

$$A: y^2+xy+y=x^3+4x-6,$$

which has non-split multiplicative reduction at 2. Moreover, $A(\mathbb{Q})=\mathbb{Z}/6\mathbb{Z}$. The discriminant of A is $-2^6\cdot 7^3$. Also, a simple computation shows that $\mathbb{Q}(A[2])=\mathbb{Q}(\sqrt{-7})$. Writing $L(A,s)$ for the complex L-series of A, we have

$$L(A,1)/\Omega_A^+=1/6.$$

Let $q_1,\dots,q_r$ be $r\geq 0$ distinct primes, which are all $\equiv 1 \bmod 4$.

Recall that the L-function of an elliptic curve E over $\mathbb{Q}$ is defined as an infinite Euler product

$$L(E,s)=\prod_{q\nmid C}(1-a_qq^{-s}+q^{1-2s})^{-1}\prod_{q|C}(1-a_qq^{-s})^{-1}=:\sum a_nn^{-s},$$

where

$$a_q=\begin{cases} q+1-\#E(\mathbb{F}_q) & \text{if } E \text{ has good reduction at } q,\\ 1 & \text{if } E \text{ has split multiplicative reduction at } q,\\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } q,\\ 0 & \text{if } E \text{ has additive reduction at } q.\end{cases}$$

Here we give a result of the behavior of the coefficients a_q of the L-function of elliptic curve A.

Theorem 6.1. *Let q be an odd prime with $(q,14)=1$. Then we have that*

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

and

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

Proof. The assertions for a_2 and a_7 are clear, since A has non-split multiplicative reduction at 2 and split multiplicative reduction at 7.

Let A' denote the 2-isogenous curve of A, which has a minimal Weierstrass equation given by

$$A': y^2+xy+y=x^3-36x-70.$$

It is easy to get that $\mathbb{Q}(A'[2])=\mathbb{Q}(\sqrt{2})$. For a_q, first note that the 2-division field $\mathbb{Q}(A[2])=\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(A'[2])=\mathbb{Q}(\sqrt{2})$, and we have the same L-function of A and A'. So we have that $A(\mathbb{F}_q)[2]\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ when q splits in $\mathbb{Q}(\sqrt{-7})$, and $A'(\mathbb{F}_q)[2]\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ when q splits in $\mathbb{Q}(\sqrt{2})$. Since $A(\mathbb{F}_q)[2]$ and $A'(\mathbb{F}_q)[2]$ are subgroups of $A(\mathbb{F}_q)$ and $A'(\mathbb{F}_q)$, respectively. We have that $4\mid\#A(\mathbb{F}_q)$ and $4\mid\#A'(\mathbb{F}_q)$. While for q is both inert in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-7})$, we have that $A(\mathbb{F}_q)[2]\cong\mathbb{Z}/2\mathbb{Z}$. It is easy to compute that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{Q}(A[4]^*)$, where $A[4]^*$ means any one of the 4-division points which is deduced from the non-trivial rational 2-torsion point of $A(\mathbb{Q})$. But q is inert in $\mathbb{Q}(\sqrt{2})$, that means $A(\mathbb{F}_q)[4]=A(\mathbb{F}_q)[2]\cong\mathbb{Z}/2\mathbb{Z}$. Hence $2\mid\#A(\mathbb{F}_q)$, but $4\nmid\#A(\mathbb{F}_q)$. Hence

$$N_q=\#A(\mathbb{F}_q)\equiv\begin{cases} 2 \mod 4 & \text{if } q \text{ is both inert in } \mathbb{Q}(\sqrt{2}) \text{ and } \mathbb{Q}(\sqrt{-7}),\\ 0 \mod 4 & \text{if } q \text{ splits in } \mathbb{Q}(\sqrt{2}) \text{ or } \mathbb{Q}(\sqrt{-7}).\end{cases}$$

Then all the assertions follow by applying $a_q=q+1-N_q$. This completes our proof. □

We then can apply Theorem 1.1 to get the following result.

Theorem 6.2. *Let M be any integer of the form $M=q_1q_2\cdots q_r$, $r\geq 1$, with $q_1,\ldots,q_r$ arbitrary distinct odd primes all congruent to 5 modulo 8, and inert in $\mathbb{Q}(\sqrt{-7})$. We then have*

$$ord_2(L^{(alg)}(A^{(M)},1))=r-1.$$

In particular, we have $L(A^{(M)}, 1) \neq 0$.

Proof. According to Theorem 6.1, when $q_i \equiv 3, 5 \bmod 8$ and q_i is inert in $\mathbb{Q}(\sqrt{-7})$, we have $ord_2(N_{q_i}) = 1$ for $1 \leq i \leq r$. The theorem then follows immediately by Theorem 4.2. □

We next prove the 2-part of the Birch and Swinnerton-Dyer conjecture for all the twists $E^{(M)}$ in Theorem 1.5. Note that $A^{(M)}$ has bad additive reduction at all primes dividing M. Write $c_q(A^{(M)})$ for the Tamagawa factor of $A^{(M)}$ at a finite odd prime $q \mid M$. We then have that

$$ord_2(c_q(A^{(M)})) = ord_2(\#A(\mathbb{Q}_q)[2]). \tag{6.1}$$

We apply the results in [4, §7] on the Tamagawa factors of $A^{(M)}$, we then get the following result.

Proposition 6.3. *For all odd square-free integers* M *with* $(M, 14) = 1$, *we have (i)* $A^{(M)}(\mathbb{R})$ *has one connected component, (ii)* $ord_2(c_2(A^{(M)})) = 1$, $ord_2(c_7(A^{(M)})) = 0$, *(iii)* $ord_2(c_q(A^{(M)})) = 1$ *if* q *does not split in* $\mathbb{Q}(\sqrt{-7})$, *and (iv)* $ord_2(c_q(A^{(M)})) = 2$ *if* q *splits in* $\mathbb{Q}(\sqrt{-7})$.

Proof. Assertion (i) follows immediately from the fact that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{-7})$. Assertion (ii) follows easily from Tate's algorithm. The remaining assertions involving odd primes q of bad reduction follow immediately from (6.1), on noting that $A(\mathbb{Q}_q)[2]$ is of order 2 or 4, according as q does not or does split in $\mathbb{Q}(\sqrt{-7})$, respectively. □

To obtain the 2-part of the Birch–Swinnerton-Dyer formula, we also have to investigate the 2-part of $Ш(A^{(M)})$. If we just apply Theorem 1.5, of course we will get that the 2-part of the Birch–Swinnerton-Dyer formula holds for a family of quadratic twists, provided both 2 and 7 split in $\mathbb{Q}(\sqrt{M})$, whence M has to have an even number of prime factors. However, a classical 2-descent of quadratic twists of $X_0(14)$ has been carried out earlier by Junhwa Choi, which yields that $Ш(A^{(M)})[2]$ is trivial, provided that all the prime factors of M are distinct primes congruent to $3, 5$ modulo 8 and inert in $\mathbb{Q}(\sqrt{-7})$. We then can get the following theorem.

Theorem 6.4. *Let* M *be any integer of the form* $M = q_1 q_2 \cdots q_r$, $r \geq 1$, *with* $q_1, \ldots, q_r$ *arbitrary distinct odd primes all congruent to* 5 *modulo* 8, *and inert in* $\mathbb{Q}(\sqrt{-7})$. *Then the* 2*-part of Birch and Swinnerton-Dyer conjecture is valid for* $A^{(M)}$.

Proof. Under the assumptions of the theorem, $Ш(A^{(M)})[2]$ is trivial. Then combining the results of Proposition 6.3, we have that $ord_2(\prod_{q|M} c_q(A^{(M)})) = r$. Note also that $\#(A(\mathbb{Q})[2]) = 2$. So we have

$$ord_2(\#(Ш(A^{(M)}))) + ord_2(\prod_p c_p(A^{(M)})) + ord_2(c_\infty(A^{(M)})) - 2ord_2(\#(A^{(M)}(\mathbb{Q}))) = r - 1.$$

Hence, the 2-part of Birch and Swinnerton-Dyer conjecture holds for $A^{(M)}$. □

Here is the beginning of an infinite set of primes q satisfying the conditions in the above theorem:-

$$\mathcal{S} = \{5, 13, 61, 101, 157, 173, 181, 229, 269, 293, 349, 397, \ldots\}.$$

6.2. **More numerical examples.** For the following three examples, the analogous methods of quadratic twists of $X_0(14)$ would apply, so we will not give the detailed proofs here.

6.2.1. *Quadratic twists of "*$34A1$*".* Let A be the elliptic curve "$34A1$" with the minimal Weierstrass equation given by

$$A : y^2 + xy = x^3 - 3x + 1,$$

which has split multiplicative reduction at 2 and $a_2 = 1$. Moreover, $A(\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$ and $L^{(alg)}(A, 1) = 1/6$. The discriminant of A is $2^6 \cdot 17$. Also, a simple computation shows that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{17})$ and $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{2})$. Here is the beginning of an infinite set of primes q which are congruent to 1 modulo 4 and inert in both the fields $\mathbb{Q}(\sqrt{17})$ and $\mathbb{Q}(\sqrt{2})$:-

$$\mathcal{S} = \{5, 29, 37, 61, 109, 173, 181, 197, 269, 277, 317, 397, \ldots\}.$$

Let $M = q_1 q_2 \cdots q_r$, be a product of r distinct primes in $\mathcal{S}$. We then have

$$ord_2(L^{(alg)}(A^{(M)}, 1)) = r - 1,$$

and the 2-part of Birch and Swinnerton-Dyer conjecture is valid for all these twists.

6.2.2. *Quadratic twists of "*$56B1$*".* Let A be the elliptic curve "$56B1$" with the minimal Weierstrass equation given by

$$A : y^2 = x^3 - x^2 - 4,$$

which has potentially supersingular reduction at 2 and $a_2 = 0$. Moreover, $A(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and $L^{(alg)}(A, 1) = 1/6$. The discriminant of A is $-2^{10} \cdot 7$. Also, a simple computation shows that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{2})$. Here is the beginning of an infinite set of primes q which are congruent to 1 modulo 4 and inert in both the fields $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{2})$:-

$$\mathcal{S} = \{5, 13, 61, 101, 157, 173, 181, 229, 269, 293, 349, 397, \ldots\}.$$

Let $M = q_1 q_2 \cdots q_r$, be a product of r distinct primes in $\mathcal{S}$. We then have

$$ord_2(L^{(alg)}(A^{(M)}, 1)) = r - 1,$$

and the 2-part of Birch and Swinnerton-Dyer conjecture is valid for all these twists.

6.2.3. *Quadratic twists of "*$99C1$*".* Let A be the elliptic curve "$99C1$" with the minimal Weierstrass equation given by

$$A : y^2 + xy = x^3 - x^2 - 15x + 8,$$

which has good reduction at 2 and $a_2 = 1$. Moreover, $A(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and $L^{(alg)}(A, 1) = 1/2$. The discriminant of A is $3^9 \cdot 11$. Also, a simple computation shows that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{33})$ and $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{3})$. Here is the beginning of an infinite set of primes q which are congruent to 1 modulo 4 and inert in both the fields $\mathbb{Q}(\sqrt{33})$ and $\mathbb{Q}(\sqrt{3})$:-

$$\mathcal{S} = \{5, 53, 89, 113, 137, 257, 269, 317, 353, 389, \ldots\}.$$

Let $M = q_1 q_2 \cdots q_r$, be a product of r distinct primes in $\mathcal{S}$. We then have

$$ord_2(L^{(alg)}(A^{(M)}, 1)) = r - 1,$$

and the 2-part of Birch and Swinnerton-Dyer conjecture is valid for all these twists.

6.3. **Examples satisfying the full Birch–Swinnerton-Dyer conjecture.** Let A be the elliptic curve "$46A1$" with the minimal Weierstrass equation given by

$$A : y^2 + xy = x^3 - x^2 - 10x - 12,$$

which has non-split multiplicative reduction at 2 and $a_2 = -1$, $a_3 = 0$. Moreover, $A(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and $L^{(alg)}(A, 1) = 1/2$. The discriminant of A is $-2^{10} \cdot 23$. The Tamagawa factors $c_2 = 2$, $c_{23} = 1$. Also, a simple computation shows that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{2})$. Here is the beginning of an infinite set of primes q which are congruent to 1 modulo 4 and inert in both the fields $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{2})$, and satisfy $a_q \neq 0$:-

$$\mathcal{S} = \{5, 37, 53, 61, 149, 157, 181, 229, 293, 373, \ldots\}.$$

Let $M = q_1 q_2 \cdots q_r$ be a product of r distinct primes in $\mathcal{S}$. By Theorem 1.1, we have $L(A^{(M)}, 1) \neq 0$, and

$$ord_2(L^{(alg)}(A^{(M)}, 1)) = r - 1.$$

If we carry out a classical 2-descent on $A^{(M)}$, one shows easily that the 2-primary component of $Ш(A^{(M)})$ is zero and $ord_2(c_{q_i}) = 1$ for $1 \leq i \leq r$, and therefore the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$. Alternatively, we can just apply Theorem 1.5, and take the number of prime factors of M, say $r(M)$, to be even, and take $M \equiv 1 \bmod 8$, then the assumption that both 2 and 23 split in $\mathbb{Q}(\sqrt{M})$ will hold, whence we can also verify the 2-part of the Birch and Swinnerton-Dyer conjecture. Then combining with the result in [19, Theorem 9.3], the full Birch and Swinnerton-Dyer conjecture is valid for $A^{(M)}$. Hence the full Birch and Swinnerton-Dyer conjecture is verified for infinitely many elliptic curves.

References

[1] L. Cai, Y. Chen, Y. Liu, *Heegner points on modular curves*, Trans. Amer. Math. Soc. 370 (2018), no. 5, 3721–3743.

[2] L. Cai, J. Shu, Y. Tian, *Explicit Gross-Zagier and Waldspurger formulae*, Algebra Number Theory 8 (2014), no. 10, 2523–2572.

[3] K. Česnavičius, *The Manin constant in the semistable case*, Compos. Math. 154 (2018), no. 9, 1889–1920.

[4] J. Coates, *Lectures on the Birch–Swinnerton-Dyer conjecture*, Notices of the ICCM, 2013.

[5] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. (3) 110 (2015), no. 2, 357–394.

[6] J. Coates, *The conjecture of Birch and Swinnerton-Dyer*, Open problems in mathematics, 207–223, Springer, [Cham], 2016.

[7] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997.

[8] J. Cremona, *Manin constants and optimal curves: conductors* 60000–400000, (2016).

[9] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), no. 2, 225–320.

[10] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[11] Z. Klagsbrun, *Selmer ranks of quadratic twists of elliptic curves with partial rational two-torsion*, Trans. Amer. Math. Soc. 369 (2017), no. 5, 3355–3385.

[12] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves*, Math. USSR-Izv. 32 (1989), 523–541.

[13] D. Kriz, C. Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum of Mathematics, Sigma (2019), Vol. 7, e15, 80 pages.

[14] D. Kriz, C. Li, *Prime twists of elliptic curves*, to appear in Mathematical Research Letters.

[15] Ju. I. Manin, *Parabolic points and zeta-functions of modular curves*, Math. USSR-Izv. 6 (1972), 19–64.

[16] E. F. Schaefer, M. Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. 356 (2004), no. 3, 1209–1231.
[17] A. Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325v2 (2017).
[18] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. 23 (1974), 179–206.
[19] X. Wan, *Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture*, arXiv:1411.6352v6 (2019).
[20] S. Zhai, *Non-vanishing theorems for quadratic twists of elliptic curves*, Asian J. Math. 20 (2016), no. 3, 475–502.

Li Cai
Yau Mathematical Sciences Center
Tsinghua University
Beijing 100084
China
lcai@mail.tsinghua.edu.cn

Chao Li
Department of Mathematics
Columbia University
2990 Broadway, New York, NY 10027
U.S.A.
chaoli@math.columbia.edu

Shuai Zhai
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge
Cambridge CB3 0WB
UK
&
Institute for Advanced Research
Shandong University
Jinan, Shandong 250100
China
S.Zhai@dpmms.cam.ac.uk