SELMER GROUPS OF QUADRATIC TWISTS OF ELLIPTIC CURVES

Kevin James and Ken Ono

1. Introduction and Statement of Results

Let $E/\mathbb{Q}$ be an elliptic curve given by:

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. Let $N(E)$ denote the conductor of E, $j(E)$ the j-invariant of E, and $L(E,s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ the Hasse-Weil L-function of E. If E is modular, then let $F_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n \in S_2(N(E), \chi_1)$ be the associated weight 2 cusp form. Here χ_1 denotes the trivial Dirichlet character.

Throughout, D will denote a square-free integer, and χ_D shall denote the Kronecker character for the field $\mathbb{Q}(\sqrt{D})$. Let $h(D)$ denote the order of $Cl(D)$, the ideal class group of $\mathbb{Q}(\sqrt{D})$. If ℓ is prime, then define $h(D)_\ell$ by

$$h(D)_\ell := |Cl(D)/\ell \cdot Cl(D)| = \ell^{r(D,\ell)},$$

where $r(D,\ell)$ denotes the ℓ-rank of $Cl(D)$.

Moreover, let $E(D)$ denote the elliptic curve over $\mathbb{Q}$ which is the D-quadratic twist of E. This curve is given by the equation:

$$E(D): \quad y^2 = x^3 + b_2Dx + 8b_4D^2x + 16b_6D^3, \tag{1.2}$$

where $b_2 := a_1^2 + 4a_2$, $b_4 := 2a_4 + a_1a_3$, and $b_6 := a_3^2 + 4a_6$. Later, we shall require the standard invariants

$$c_4 := b_2^2 - 24b_4 \quad \text{and} \quad c_6 := b_2^3 + 36b_2b_4 - 216b_6. \tag{1.3}$$

1991 *Mathematics Subject Classification.* Primary 11G05, 11G40; Secondary 11R29.

Key words and phrases. Selmer groups, elliptic curves.

The second author is supported by NSF grant DMS-9508976 and NSA grant MSPR-97Y012.

In an important paper [Gol], Goldfeld conjectured that

$$\sum_{|D|<X} rk(E(D)) \sim \frac{1}{2} \sum_{|D|<X} 1, \tag{1.4}$$

where $rk(E(D))$ denotes the Mordell-Weil rank of $E(D)$. This implies that almost every $E(D)$ has rank zero or one dictated by $\delta(E(D))$, the sign of the functional equation of $L(E(D), s)$. Although there are strong results in the direction of (1.4) for special curves by the works of Heath Brown, James, Vatsal, and Wong (see [HB, HB2, Ja1, V, Wo]), this conjecture remains open. For a general modular elliptic curve E (see [O-S2]), it is only known that there is a positive integer r_E for which

$$\#\{|D| < X \ : \ rk(E(D)) = 0\} \gg_E \frac{X}{\log X} \cdot (\log\log X)^{r_E - 1}.$$

Throughout, the notation $F(X) \gg G(X)$ shall mean that there is a positive constant c such that for sufficiently large X we have $F(X) \geq c \cdot G(X)$. Subscripts under the symbol $\gg$ shall indicate the parameters which determine the choice of the constant c.

While the aforementioned papers study the frequency of the finiteness of the Mordell-Weil groups of $E(D)$, here we focus on the frequency of the triviality of Selmer groups over $\mathbb{Q}$. Let ℓ be an odd prime, and for each curve $E(D)$ we have the usual Kummer exact sequence

$$1 \to E(D)/\ell E(D) \to S(E(D))_\ell \to Ш(E(D))[\ell] \to 1, \tag{1.5}$$

where $S(E(D))_\ell$ is the ℓ-Selmer group of $E(D)$, and $Ш(E(D))[\ell]$ denotes the elements of the Tate-Shafarevich group $Ш(E(D))$ with order dividing ℓ. Given an elliptic curve E, we shall estimate how often $S(E(D))_\ell$ is trivial.

Numerical evidence suggests that if ℓ is an odd prime, then

$$\#\{|D| < X \ : \ D \text{ square-free and } S(E(D))_\ell = \{1\}\} \gg_{E,\ell} X. \tag{1.6}$$

To illustrate this expectation, consider the congruent number elliptic curves

$$E(D): \quad y^2 = x^3 - D^2 x.$$

Assuming the Birch and Swinnerton-Dyer Conjecture, let $\delta(\ell, X)$ denote the proportion of square-free integers $1 \leq D \leq X$ with the property that $S(E(D))_\ell$ is trivial. Using Tunnell's important paper [T], the first author has compiled the following table.

X	$\delta(3,X)$	$\delta(5,X)$	$\delta(7,X)$	$\delta(11,X)$
1,000,000	0.32530	0.39535	0.42117	0.44022
5,000,000	0.32397	0.39543	0.42317	0.44420
10,000,000	0.32286	0.39556	0.42353	0.44542
15,000,000	0.32212	0.39567	0.42377	0.44617
20,000,000	0.32193	0.39564	0.42401	0.44672
25,000,000	0.32183	0.39565	0.42415	0.44710
30,000,000	0.32178	0.39573	0.42426	0.44740

Although it is unreasonable to formulate a precise conjecture based on this data, one has little difficulty accepting the widely held belief that (1.6) is indeed true.

Using theorems of Coates and Wiles, and Rubin, Kohnen and the second author recently obtained a result in the direction of (1.6) for elliptic curves with complex multiplication. If E is such a curve [Th. 2, K-O], then for every sufficiently large prime ℓ we have

$$\#\{|D| < X \ : \ S(E(D))_\ell = \{1\}\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}. \tag{1.7}$$

Less was known for generic modular elliptic curves E. Works by Bruinier, Jochnowitz, and Skinner and the second author (see [B, J, O-S]) shed some light on (1.6) for modular elliptic curves. From these works, subject to the truth of the Birch and Swinnerton-Dyer Conjecture, if E is modular, then for every sufficiently large prime ℓ

$$\#\{D \ : \ S(E(D))_\ell = \{1\}\} = +\infty. \tag{1.8}$$

In this paper we improve on (1.8) by obtaining a quantitative estimate , and by noticing that Kolyvagin's method leads to an unconditonal result.

Theorem 1. *If $E/\mathbb{Q}$ is a modular elliptic curve, then for every prime $\ell \gg_E 1$*

$$\#\{|D| < X \ : \ D \text{ square-free and } S(E(D))_\ell = \{1\}\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}.$$

Theorem 1 is a corollary of Theorem 9, which is a much more precise result.

Theorem 1 does not cover any odd primes ℓ for which E has rational ℓ-torsion. By a theorem of Mazur, the only such primes are $\ell = 3, 5$, and 7. However, in these cases, by invoking a theorem of Frey [A-Bu-Fr, Fr], we obtain the following result.

Theorem 2. *Let $E/\mathbb{Q}$ be an elliptic curve with a rational point of order $\ell \in \{3, 5, 7\}$. Suppose that every odd prime factor v of $N(E)$ has the property that $v \not\equiv 0, -1 \pmod{\ell}$.*

(i) If $\ell = 3$, then

$$\#\{-X < D < 0 \ : \ D \text{ square-free and } S(E(D))_\ell = \{1\}\} \gg_{E,\ell} X.$$

(ii) If $\ell = 5$ or 7, and E is good at ℓ (see §3 for the definition), then

$$\#\{-X < D < 0 \ : \ D \text{ square-free and } S(E(D))_\ell = \{1\}\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}.$$

In §2 we shall prove Theorem 1, and in §3 we prove Theorem 2. To prove Theorem 1, we shall study the behavior of the U_p and V_p operators on the "Waldspurger cusp forms" of weight 3/2 associated to E. Using standard results about Galois representations, the Chebotarev density theorem, and results of Kolyvagin, we obtain Theorem 1. To prove Theorem 2, we combine a similar argument involving the U_p and V_p operators with a theorem of Frey which characterizes the structure of Selmer groups of quadratic twists of elliptic curves with rational ℓ-torsion.

2. Proof of Theorem 1

In this section we prove Theorem 1 by studying the behavior of the U_p and V_p operators on half-integral weight modular forms. For $k \in \frac{1}{2}\mathbb{Z}$ and $N \in \mathbb{N}$ (with $4|N$ if $k \notin \mathbb{Z}$) let $M_k(N,\chi)$ (resp. $S_k(N,\chi)$) denote the space of modular forms (resp. cusp forms) of weight k on $\Gamma_0(N)$ with Nebentypus character χ (see [Sh] for definitions).

Suppose that k is a non-negative integer and p is prime. If $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ ($q := e^{2\pi iz}$ throughout) is a modular form in $M_{k+\frac{1}{2}}(N,\chi)$, then define $(U_pf)(z)$ and $(V_pf)(z)$ by

$$(U_pf)(z) := \sum_{n=0}^{\infty} a(pn)q^n \tag{2.1}$$

$$(V_pf)(z) := \sum_{n=0}^{\infty} a(n)q^{pn}. \tag{2.2}$$

The following proposition is well known.

Proposition 3. ([§1, Sh]) *Suppose that k is a non-negative integer and $f(z)$ is a modular form in $M_{k+\frac{1}{2}}(N,\chi)$ (resp. $S_{k+\frac{1}{2}}(N,\chi)$). If p is prime, then both $(U_pf)(z)$ and $(V_pf)(z)$ are modular forms in $M_{k+\frac{1}{2}}(Np, \left(\frac{4p}{\bullet}\right)\cdot\chi)$ (resp.$S_{k+\frac{1}{2}}(Np, \left(\frac{4p}{\bullet}\right)\cdot\chi)$).*

We shall be interested in the behavior of half-integral weight modular forms mod ℓ and mod $\mathfrak{l}$ under these operators. To make this precise, we recall the following definition.

Definition 4. *Suppose that K is a number field and $f = \sum_{n=0}^{\infty} a(n)q^n$ is a formal power series whose coefficients are in O_K, the ring of algebraic integers of K. If $\mathfrak{l}$ is a prime ideal in O_K, then define* $\mathrm{ord}_{\mathfrak{l}}(f)$ *by*

$$\mathrm{ord}_{\mathfrak{l}}(f) := \begin{cases} \min\{n \ : \ a(n) \notin \mathfrak{l}\} & \text{if } a(n) \notin \mathfrak{l} \text{ for some } n, \\ +\infty & \text{otherwise.} \end{cases}$$

Sturm proved the following important result.

Proposition 5. ([Th. 1, St]) *Suppose that $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ is a modular form in $M_k(N,\chi)$ whose coefficients are algebraic integers in some number field K. If $\mathfrak{l}$ is a prime ideal in O_K and*

$$\mathrm{ord}_{\mathfrak{l}}(f) > \frac{k}{12}\cdot[\Gamma_0(1) : \Gamma_0(N)],$$

then $\mathrm{ord}_{\mathfrak{l}}(f) = +\infty$.

He proved this for integral k and trivial χ, but the general case obviously follows by taking an appropriate power of f.

Let $\delta \in \{\pm 1\}$, and let $\Omega_{E,\delta}$ denote the real period of $E(\delta)$. For each square-free integer D, let $\Omega(E(D))$ denote the real period of $E(D)$. In this discussion, we shall assume that D is an odd square-free integer for which $\delta D > 0$ and $\gcd(D, N(E)) = 1$. For such D, we have that

$$\Omega(E(D)) = \frac{\Omega_{E,\delta}}{\sqrt{|D|}} \cdot \alpha(E, D, \delta), \tag{2.3}$$

where $\alpha(E, D, \delta) \in \mathbb{Q}$. If ℓ is an odd prime, then $\mathrm{ord}_\ell(\alpha(E, D, \delta)) = 0$.

Since E is modular, there is a non-zero integer $c_{E,\delta}$ such that

$$c_{E,\delta} \cdot \frac{L(E(D), 1)}{\Omega(E(D))} \in \mathbb{Z} \tag{2.4}$$

(see [M-T-T] and [Th. 3.5.4, G-S]).

However, more is conjectured to be true. If $L^{alg}(E(D), 1) := L(E(D), 1)/\Omega(E(D))$ and $L(E(D), 1) \neq 0$, then the Birch and Swinnerton-Dyer Conjecture states that

$$L^{alg}(E(D), 1) = \frac{\#Ш(E(D))}{\#E(D)^2_{tor}} \cdot Tam(E(D)), \tag{2.5}$$

where $E(D)_{tor}$ is the torsion subgroup of $E(D)$ and $Tam(E(D))$ is the Tamagawa integer.

Waldspurger proved a fundamental theorem [Th. 1, Wal] relating $L(E(D), 1)$ to the Fourier coefficients of certain weight 3/2 cusp forms. We shall require the following special case of his result.

Theorem 6. ([§2, O-S2], [Th. 4, K-O]) *If $E/\mathbb{Q}$ is a modular elliptic curve and $\delta(E) \in \{\pm 1\}$ is the sign of the functional equation of $L(E, s)$, then there is a non-zero complex number Ω_F, an integer N_W where $4N(E) \mid N_W$, a Dirichlet character χ modulo N_W, and a non-zero eigenform*

$$g(z) = \sum_{n=1}^{\infty} b(n) q^n \in S_{3/2}(N_W, \chi)$$

such that for each square-free integer D with $\delta(E)D > 0$

$$b(|D|)^2 = \begin{cases} \epsilon(D) \cdot \frac{L(E(D),1)\sqrt{|D|}}{\Omega_F} & \text{if } \gcd(D, N_W) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, the $\epsilon(D)$ and $b(n)$ are algebraic integers in some fixed number field.

Using the notation in Theorem 6, if D is a square-free integer coprime to N_W for which $\delta(E)D > 0$, then define $L^{alg}_W(E(D), 1)$ by

$$L^{alg}_W(E(D), 1) := b(|D|)^2. \tag{2.6}$$

For such D, by Theorem 6, (2.3) and (2.5) we find that

$$L_W^{alg}(E(D),1) = \epsilon(D)\cdot\alpha(E,D,\delta)\cdot\frac{\Omega_{E,\delta(E)}}{\Omega_F}\cdot L^{alg}(E(D),1). \tag{2.7}$$

If ℓ is prime, then let $|\bullet|_\ell$ denote an extension of the usual multiplicative ℓ-adic valuation to an algebraic closure of $\mathbb{Q}$. In view of Theorem 6, (2.4), and (2.7) we obtain the following corollary.

Corollary 7. *Assuming the notation from Theorem 6, suppose that ℓ is an odd prime for which $|\Omega_{E,\delta(E)}/\Omega_F|_\ell = |c_{E,\delta(E)}|_\ell = 1$. If D is a square-free integer for which*

(i) $\delta(E)D > 0$,
(ii) $gcd(D, N_W) = 1$,
(iii) $|L_W^{alg}(E(D),1)|_\ell = 1$,

then $|L^{alg}(E(D),1)|_\ell = 1$.

In view of the famous Gross-Zagier formula [Gr-Z], we recall an important result which follows from the work of Kolyvagin.

Theorem 8. ([Cor. E, Ko2]) *Suppose that $E/\mathbb{Q}$ is modular, and let $\mathrm{Sha}(E(D))$ denote the order of $Ш(E(D))$ as predicted by the Birch and Swinnerton-Dyer Conjecture. If D is a negative square-free integer for which*

(i) $gcd(D, 2N(E)) = 1$ *and* $D \equiv \square \pmod{4N(E)}$,
(ii) $L'(E, \mathbb{Q}(\sqrt{D}), 1) \neq 0$,

where $L(E, \mathbb{Q}(\sqrt{D}), s) = L(E,s)\cdot L(E(D),s)$, then for every prime $\ell \gg_E 1$ we have

$$\mathrm{ord}_\ell(\#Ш(E(D))) \leq \mathrm{ord}_\ell(\mathrm{Sha}(E(D))).$$

Now we prove the main theorem which yields Theorem 1 as an easy corollary.

Theorem 9. *Assume the notation from Theorem 6. Suppose $\ell \geq 5$ is a prime for which the Galois representation*

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

defined by the action of Galois on the ℓ-torsion points of E is surjective. In addition, suppose that $\delta(E) = -1$, $|\Omega_{E,\delta(E)}/\Omega_F|_\ell = |c_{E,\delta(E)}|_\ell = 1$, and that there is a negative square-free integer D_0 for which

(i) $gcd(D_0, N_W) = 1$,
(ii) $D_0 \equiv \square \pmod{4N(E)}$,
(iii) $|L_W^{alg}(E(D_0),1)|_\ell = 1$.

Then there is a positive constant $\kappa(E)$ and a set of primes p of positive density with the property that there is an odd integer $1 \le |n_p| \le \kappa(E)(p+1)$ for which

(*i*) $n_p < 0$ *and* $gcd(n_p, pN_W) = 1$,
(*ii*) $n_p p \equiv \square \pmod{4N(E)}$,
(*iii*) $|L^{alg}(E(n_p p), 1)|_\ell = 1$,
(*iv*) $E(n_p p)$ *has rank zero.*

Proof of Theorem 9. Using the form $g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{3/2}(N_W, \chi)$ from Theorem 6, define the auxilary modular form $g_0(z) = \sum_{n=1}^{\infty} b_0(n)q^n \in S_{3/2}(16N_W N(E)^2, \chi)$ so (see [Sh]) that

$$b_0(n) = \begin{cases} b(n) & \text{if } -n \equiv \square \pmod{4N(E)}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.8}$$

This form is easily obtained by taking an obvious linear combination of quadratic twists of $g(z)$ using (if necessary) the nontrivial real character with conductor 8, and the Legendre symbols $\left(\frac{\bullet}{v}\right)$ for the odd primes $v \mid N(E)$. Since $b(|D_0|) \neq 0$, it follows immediately that $g_0(z)$ is nonzero.

By (2.1), (2.2), and Proposition 3, if p is prime, then the forms $(U_p g_0)(z) = \sum_{n=1}^{\infty} u_p(n)q^n$ and $(V_p g_0)(z) = \sum_{n=1}^{\infty} v_p(n)q^n$ are cusp forms in $S_{3/2}\left(16N_W N(E)^2 p, \left(\frac{4p}{\bullet}\right) \cdot \chi\right)$. Hence by (2.8), for every positive integer n

$$u_p(n) = \begin{cases} b(pn) & \text{if } -pn \equiv \square \pmod{4N(E)}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.9}$$

$$v_p(n) = \begin{cases} b(n/p) & \text{if } p \mid n \text{ and } -\frac{n}{p} \equiv \square \pmod{4N(E)}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.10}$$

By the proof of Theorem 6 (see [§2,O-S2], [Th. 4, K-O]), the eigenform $g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{3/2}(N_W, \chi)$ maps to a twist (possibly trivial) of $F_E(z)$ under the Shimura correspondence. Therefore, the eigenvalues $\lambda(p)$ of $g(z)$ with respect to the half-integral weight Hecke operators $T(p^2)$ will be twists of $a_E(p)$, the eigenvalues of $F_E(z)$ with respect to the weight 2 Hecke operators $T(p)$. Specifically, if $\ell \mid a_E(p)$, then $\lambda(p) \equiv 0 \pmod{\ell}$ as well.

Arguing as in [Lemma 7, Sw-D], one finds that the surjectivity of $\rho_{E,\ell}$ together with the Chebotarev density theorem implies that in any arithmetic progression $r \pmod{t}$ with $\gcd(r,t) = 1$ the set of primes

$$T(\ell, r, t) := \{p \text{ prime } : \ p \equiv r \pmod{t} \text{ and } a_E(p) \equiv 0 \pmod{\ell}\} \tag{2.11}$$

has the property that

$$\#\{p \le X \ : \ p \in T(\ell, r, t)\} \gg_{\ell, r, t} \frac{X}{\log X}. \tag{2.12}$$

By the definition of the Hecke operators on the space $M_{3/2}(N_W, \chi)$, we find that if $p \nmid N_W$ and $p \in T(\ell, r, t)$, then for every integer n

$$b(p^2 n) \equiv -\chi(p)\left(\frac{-n}{p}\right) b(n) - \chi(p^2) p b(n/p^2) \pmod{\ell}. \tag{2.13}$$

The crux of the proof is the careful selection of an arithmetic progression $r_0 \pmod{t_0}$ which enjoys the following important properties:

(2.14) $N_W \mid t_0$,
(2.15) $\gcd(r_0, t_0) = 1$ and $\chi(r_0) = 1$,
(2.16) Define the constant $\kappa(E)$ by

$$\kappa(E) := \frac{[\Gamma_0(1) : \Gamma_0(16 N_W N(E)^2)]}{8} + 1.$$

If $p \equiv r_0 \pmod{t_0}$ is prime, then $\left(\frac{-n}{p}\right) = -1$ for each $1 \le n \le \kappa(E)$ with $\gcd(n, N_W) = 1$.
(2.17) For each prime $p \equiv r_0 \pmod{t_0}$ we have $\left(\frac{D_0}{p}\right) = -1$ (Recall that $D_0 < 0$ and $\gcd(D_0, N_W) = 1$).
(2.18) Each prime $p \equiv r_0 \pmod{t_0}$ has the property that $p \not\equiv -1 \pmod{\ell}$.

To see that such a progression exists, notice first that condition (2.16) depends only on those odd primes (Recall that $4 \mid N_W$) up to $\kappa(E)$ which are coprime to N_W. Then notice that (2.17) depends on the prime divisors of D_0 which are also coprime to N_W. Since (2.16) and (2.17) are independent of the conditions imposed by (2.14) and (2.15), we easily obtain progressions which satisfy conditions (2.14-2.17). Condition (2.18) is easily satisfied since $\ell \ge 5$.

Now consider the action of the U_p and V_p operators on $g_0(z)$ for those primes $p \in T(\ell, r_0, t_0)$. By (2.13), (2.15), and (2.16), if $p \in T(\ell, r_0, t_0)$ is sufficiently large, then

$$u_p(pn) = b_0(p^2 n) \equiv b_0(n) = v_p(pn) \pmod{\ell} \tag{2.19}$$

for every $1 \le n \le \kappa(E)$. Recall that $b(n) = 0$ for those n with $\gcd(n, N_W) \neq 1$. By (2.13) again, we find that for every sufficiently large prime $p \in T(\ell, r_0, t_0)$ that

$$v_p(|D_0| p^3) = b_0(|D_0| p^2) \equiv b_0(|D_0|) \pmod{\ell}, \tag{2.20}$$

$$u_p(|D_0| p^3) = b_0(|D_0| p^4) \equiv -p b_0(|D_0|) \pmod{\ell}. \tag{2.21}$$

Hence, for every sufficiently large prime $p \in T(\ell, r_0, t_0)$ we find by (2.20), (2.21), and (2.18) that

$$\mathrm{ord}_\ell(U_p g_0 - V_p g_0) < +\infty. \tag{2.22}$$

The form $(U_p g_0)(z) - (V_p g_0)(z)$ is in the space $S_{3/2}\left(16N_W N(E)^2 p, \left(\frac{4p}{\bullet}\right)\right)$ by Proposition 3. Therefore, by Proposition 5, (2.9), (2.10), (2.19) and (2.22), if $p \in T(\ell, r_0, t_0)$ is sufficiently large, then there is at least one integer $1 \leq n_0 < \kappa(E)(p+1)$ with $\gcd(n_0, p) = 1$ with the property that

$$b_0(pn_0) = u_p(n_0) \not\equiv 0 = v_p(n_0) \pmod{\ell}.$$

To see this, notice that the "Sturm bound" in Proposition 5 for $(U_p g_0)(z) - (V_p g_0)(z)$ is

$$\frac{1}{8} \cdot [\Gamma_0(1) : \Gamma_0(16N_W N(E)^2 p)] < \kappa(E) \cdot [\Gamma_0(16N_W N(E)^2) : \Gamma_0(16N_W N(E)^2 p)].$$

The conclusion above now follows easily by recalling that

$$[\Gamma_0(M) : \Gamma_0(Mp)] = \begin{cases} p+1 & \text{if } \gcd(p, M) = 1, \\ p & \text{if } p \mid M. \end{cases}$$

By Corollary 7 and (2.8), there is an odd square-free integer $n_p < 0$ with $1 \leq |n_p| < \kappa(E)(p+1)$ (clearly $n_0 = -n_p$) so that $\gcd(n_p, N_W p) = 1$, $n_p p \equiv \square \pmod{4N(E)}$, and $|L^{alg}(E(n_p p), 1)|_\ell = 1$.

To complete the proof, it suffices to show that $E(n_p p)$ has rank zero. This follows immediately by a theorem of Kolyvagin [Ko] since $L(E(n_p p), 1) \neq 0$.

□

Proof of Theorem 1. By [Th. 2, K-O], we may without loss of generality assume that E does not have complex multiplication. Moreover, we may without loss of generality assume, by replacing E by a suitable quadratic twist of E if necessary, that $\delta(E) = -1$ and $L'(E, 1) \neq 0$. That we may do so is a corollary of important works by Bump, Friedberg, and Hoffstein, Iwaniec, and M. R. Murty and V. K. Murty (see [B-F-Ho, I, Mu-Mu]).

It is well known that if D is a square-free integer such that $\gcd(D, 2N(E)) = 1$, then $\delta(E(D)) = \chi_D(-N(E))\delta(E)$. Therefore, we see that a candidate for the square-free integer D_0 in Theorem 9 has the property that $\delta(E(D_0)) = +1$. In this case, an important theorem of Friedberg and Hoffstein [Th. B (i), F-H] indeed guarantees that there are such negative D_0 satisfying conditions (i) and (ii) of Theorem 9 for which $L(E(D_0), 1) \neq 0$. Therefore, for any such D_0 we find that $|L_W^{alg}(E(D_0), 1)|_\ell = 1$ for almost every prime ℓ. Since a theorem of Serre [Se] guarantees that $\rho_{E,\ell}$ is surjective for all but finitely many primes ℓ, it then follows that the conclusion of Theorem 9 is valid for all but finitely many primes ℓ.

If ℓ is such a prime, then let $T(\ell, r_0, t_0)$ be as in the proof of Theorem 9. By Theorem 9 and (2.5), it is easy to see that if $p \in T(\ell, r_0, t_0)$ is sufficiently large, then the Birch and Swinnerton-Dyer Conjecture predicts that $\ell \nmid \mathrm{Sha}(E(n_p p))$. For if ℓ is an odd prime, then there are at most finitely many D for which $\ell \mid \#E(D)_{tor}$ (see [Prop.1, Go-M]). Since $L'(E, 1) \neq 0$, by hypothesis, and $L(E(n_p p), 1) \neq 0$ (which implies that $L'(E, \mathbb{Q}(\sqrt{n_p p}), 1) \neq 0$), by Theorem 8, we see that $S(E(n_p p))_\ell = \{1\}$.

For convenience, let p_i denote the primes in $T(\ell, r_0, t_0)$ in increasing order, and let D_i denote the square-free part of $p_i n_{p_i}$. If $j < k < l$ and $D_j = D_k = D_l$, then $p_j p_k p_l \mid D_j$. However this can only occur for finitely many j, k, and l since $|D_i| < k(E)p_i(p_i+1)$. Therefore, the number of distinct $|D_i| < X$ is at least half the number of $p \in T(\ell, r_0, t_0)$ with $p \leq \sqrt{X/\kappa(E)}$. Theorem 1 then follows easily from (2.12).

□

Remarks. 1. The conditions in Theorem 9 are quite mild. Although Serre's theorem guarantees, for E without complex multiplication, that all but finitely many primes ℓ have surjective $\rho_{E,\ell}$, more is known. For example, Mazur [M] has proved that if E is semistable, then every $\ell \geq 11$ has surjective $\rho_{E,\ell}$. Masser and Wüstholz [Ma-W] have shown that every prime $\ell \gg \log^A H(E)$ has surjective $\rho_{E,\ell}$, where the constants are absolute and $H(E)$ is the naive height of E. More recently, Duke [Du] has shown that almost every E without complex multiplication has the property that $\rho_{E,\ell}$ is surjective for every odd prime ℓ.

2. The primes ℓ which are sufficiently large for the conclusion in Theorem 1 are effectively computable for any given E. Apart from the hypotheses on ℓ which appear in Corollary 7 and Theorem 9, there are further hypotheses required by [Cor. E, Ko2]. These hypotheses are described completely in [pp. 440-442, Ko2].

3. Proof of Theorem 2

In this section, we use an argument similar to the one in the proof of Theorem 9 and a theorem of Frey [A-Bu-Fr,Fr] to prove a strong form of Theorem 2 (see Theorem 14). Before stating Frey's theorem, we recall the definition and some basic facts about *Tate curves* (see [V.3-V.5, Si] for a more detailed account). Let v be a rational prime. An elliptic curve $E/\mathbb{Q}_v$ is said to be a *Tate curve* if there is a $\mathfrak{q} \in \mathbb{Q}_v^*$ with $|\mathfrak{q}|_v < 1$ such that $E(\bar{\mathbb{Q}}_v) \cong \bar{\mathbb{Q}}_v^*/\mathfrak{q}^{\mathbb{Z}}$. Suppose that $E/\mathbb{Q}$ is as in (1.1). The following proposition [Th. V.5.3, Si] determines whether E is a Tate curve over $\mathbb{Q}_v$.

Proposition 10. (Tate) *If $E/\mathbb{Q}$ has integer coefficients, and v is a prime for which $\mathrm{ord}_v(j(E)) < 0$, then there is a unique $\mathfrak{q} \in \mathbb{Q}_v^*$ and a Tate curve $E_{\mathfrak{q}}$ with $E_{\mathfrak{q}}(\bar{\mathbb{Q}}_v) \cong \bar{\mathbb{Q}}_v^*/\mathfrak{q}^{\mathbb{Z}}$ such that E is isomorphic to $E_{\mathfrak{q}}$ over $\bar{\mathbb{Q}}_v$. Furthermore, E is isomorphic to $E_{\mathfrak{q}}$ over $\mathbb{Q}_v$ if and only if $\left(\frac{-c_4 c_6^{-1}}{v}\right) = 1$.*

To ease the notation, we make the following definitions.

Definition 11. (I). *If ℓ is prime and E is an elliptic curve, then we say that a negative square-free integer D is <u>good for E at ℓ</u> if*

(*i*) *$gcd(D, \ell N(E)) = 1$,*
(*ii*) *If $N(E)$ is even, then $D \equiv 3 \pmod 4$.*
(*iii*) *For every odd prime $v \mid N(E)$ we have*

$$\left(\frac{D}{v}\right) = \begin{cases} -1 & \text{if } \mathrm{ord}_v(j(E)) \geq 0, \\ -\left(\frac{-c_4 c_6^{-1}}{v}\right) & \text{otherwise.} \end{cases}$$

(II). *We say that an elliptic curve E is good at ℓ if there is a negative square-free integer D_0 which is good for E at ℓ for which*

(*i*) $h(D_0) \not\equiv 0 \pmod{\ell}$,
(*ii*) *At least one prime factor of D_0 exceeds $\kappa(N(E), \ell)$ where*

$$\kappa(N, \ell) := \frac{[\Gamma_0(1) : \Gamma_0(4\ell^2 N^4)]}{8} + 1.$$

Using Proposition 10 we obtain the following convenient form of a theorem of Frey [Prop. 1.5, A-Bu-Fr; Fr].

Proposition 12. (Frey) *Let $\ell \in \{3, 5, 7\}$ and let $E/\mathbb{Q}$ be an elliptic curve with a rational point of order ℓ and good reduction at ℓ. Furthermore, suppose for each odd prime $v \mid N(E)$ with $v \equiv -1 \pmod{\ell}$ that $\mathrm{ord}_v(j(E)) \equiv 0 \pmod{\ell}$. If D is a negative square-free integer which is good for E at ℓ, then*

$$h(D)_\ell \mid \#S(E(D))_\ell \mid h(D)_\ell^2.$$

To obtain Theorem 14, we shall employ Proposition 12 along with the following result regarding the indivisibility of class numbers of imaginary quadratic fields.

Theorem 13. *If $v_1, v_2, \ldots, v_j$ are distinct odd primes, $\epsilon_{v_1}, \epsilon_{v_2}, \ldots, \epsilon_{v_j} \in \{\pm 1\}$, then let*

$$N := 4v_1 v_2 \cdots v_j.$$

If $\ell \geq 5$ is prime, $a \in (Z/4\mathbb{Z})^*$, and there is a square-free positive integer D_0 for which:

(*i*) *gcd*$(D_0, N\ell) = 1$,
(*ii*) $D_0 \equiv a \pmod{4}$,
(*iii*) $\left(\frac{-D_0}{v_i}\right) = \epsilon_{v_i}$ *for each* $1 \leq i \leq j$,
(*iv*) $h(-D_0) \not\equiv 0 \pmod{\ell}$,
(*v*) D_0 *has at least one prime factor larger than* $\kappa(N, \ell)$,

then

$$\#\{0 < D < X \ : D \text{ is square-free and satisfies } (i) - (iv)\} \gg_\ell \frac{\sqrt{X}}{\log X}.$$

Proof of Theorem 13. Define the modular form $g(z) \in M_{3/2}(4, \chi_1)$ by

$$g(z) = \sum_{n=1}^{\infty} r(n) q^n := \theta^3(z) = \left(\sum_{n \in \mathbb{Z}} q^{n^2} \right)^3 = 1 + 6q + 12q^2 + 8q^3 + 6q^4 + \cdots . \tag{3.1}$$

It is easy to obtain a modular form $f(z) = \sum_{n=1}^{\infty} b(n)q^n$ as an appropriate linear combination of twists of $g(z)$ (including a twist by $\chi_1 \pmod{N\ell}$) for which

$$b(n) = \begin{cases} r(n) & \text{if } n \equiv a \pmod 4,\ \left(\frac{-n}{v_i}\right) = \epsilon_{v_i} \text{ for } 1 \le i \le j, \text{ and } \gcd(n, N\ell) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

Moreover, by well known facts (see [Sh]), it turns out that $f(z) \in M_{3/2}(4\ell^2N^4, \chi_1)$.

By a theorem of Gauss (see [K-O]), if $n = mf^2$ where m is a positive square-free integer, then

$$r(n) = \begin{cases} 12\frac{h(-m)}{\omega(-m)} \sum_{d|f} \mu(d) \left(\frac{-m}{d}\right) \sigma_1(f/d) & \text{if } n \equiv 1, 2 \pmod 4, \\ 24\frac{h(-m)}{\omega(-m)} \sum_{d|f} \mu(d) \left(\frac{-m}{d}\right) \sigma_1(f/d) & \text{if } n \equiv 3 \pmod 8, \\ r(n/4) & \text{if } n \equiv 0 \pmod 4, \\ 0 & \text{if } n \equiv 7 \pmod 8, \end{cases} \tag{3.3}$$

where $\omega(-m)$ is half the number of units in the ring of integers of $\mathbb{Q}(\sqrt{-m})$ and $\sigma_1(n)$ denotes the sum of the positive divisors of n.

As in the last section, if p is prime, then using Proposition 3 recall that the modular forms $(U_pf)(z)$ and $(V_pf)(z)$ in the space $M_{3/2}\left(4\ell^2N^4p, \left(\frac{4p}{\bullet}\right)\right)$ are given by

$$(U_pf)(z) = \sum_{n\ge 1} u_p(n)q^n := \sum_{n=1}^{\infty} b(pn)q^n, \tag{3.4}$$

$$(V_pf)(z) = \sum_{n\ge 1} v_p(n)q^n := \sum_{n=1}^{\infty} b(n)q^{pn}. \tag{3.5}$$

As in the proof of Theorem 9, we select an appropriate arithmetic progression $r \pmod t$ which enjoys the following important properties (3.6-3.9):

$$gcd(r, t) = 1 \text{ and } 4\ell \mid t, \tag{3.6}$$

$$r \equiv 1 \pmod{4\ell}, \tag{3.7}$$

For every prime $p \equiv r \pmod t$ we insist that

$$\left(\frac{-D_0}{p}\right) = -1, \tag{3.8}$$

$$\left(\frac{-m}{p}\right) = 1 \ \text{ for } \ 1 \le m \le \kappa(N, \ell) \ \text{ with } \ gcd(m, N\ell) = 1. \tag{3.9}$$

It is straight forward to select arithmetic progressions satisfying (3.7) and (3.9). Moreover, assumption (v) in the statement of Theorem 13 ensures us the freedom to impose condition (3.8).

Using (3.3), (3.8) and (i) – (iv) in the statement of the theorem, it is easy to verify that if $p \equiv r \pmod{t}$ is a sufficiently large prime, then $u_p(pD_0) \not\equiv v_p(pD_0) \pmod{\ell}$, and so $U_p f \not\equiv V_p f \pmod{\ell}$. Hence, by Proposition 5 there is a natural number $n < \kappa(N,\ell)(p+1)$ so that $u_p(n) \not\equiv v_p(n) \pmod{\ell}$. However, (3.3), (3.7) and (3.9) guarantee that for such p we have $u_p(pn) \equiv v_p(pn) \pmod{\ell}$ for $1 \le n \le \kappa(N,\ell)$ (Recall that $b(n) = 0$ if $\gcd(n, N\ell) \neq 1$). Hence, for every sufficiently large prime $p \equiv r \pmod{t}$ there is a natural number n_p such that

$$n_p < \kappa(N,\ell)(p+1), \tag{3.10}$$

$$p \nmid n_p, \tag{3.11}$$

$$u_p(n_p) = b(n_p p) \not\equiv 0 = v_p(n_p) \pmod{\ell}. \tag{3.12}$$

By (3.2), (3.3) and (3.12), we find that pn_p satisfies the assumptions (i) – (iv) listed in the statement of the theorem.

The theorem now follows if we make use of the bound (3.10) in an argument analogous to the one given in the proof of Theorem 1.

□

Now we state the strong version of Theorem 2.

Theorem 14. *Let $E/\mathbb{Q}$ be an elliptic curve having a rational torsion point of odd prime order ℓ and good reduction at ℓ. Furthermore, suppose for each odd prime $v \mid N(E)$ with $v \equiv -1 \pmod{\ell}$ that $\mathrm{ord}_v(j(E)) \equiv 0 \pmod{\ell}$.*

(i) If $\ell = 3$, then

$$\#\{-X < D < 0 \ : \ D \text{ square-free and } S(E(D))_\ell = \{1\}\} \gg_{E,\ell} X.$$

(ii) If $\ell = 5$ or 7 and E is good at ℓ, then

$$\#\{-X < D < 0 \ : \ D \text{ square-free and } S(E(D))_\ell = \{1\}\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}.$$

Proof of Theorem 14. Part (i) is an immediate consequence of the Davenport-Heilbronn Theorem as improved by Horie and Nakagawa [H-N] combined with Proposition 12.

For the proof of (ii), we use Proposition 12 along with Theorem 13. We simply choose $v_1, \dots, v_j$ to be the odd prime factors of $N(E)$ and choose $a = 1$. We pick the ϵ_{v_i}'s so that for any square-free negative integer $D \equiv 3 \pmod{4}$ that is coprime to $N(E)\ell$ we have $\left(\frac{D}{v_i}\right) = \epsilon_{v_i}$ for $(1 \le i \le j)$ if and only if D is good for E at ℓ. The theorem now follows easily from Theorem 13 by our assumption on the existence of a suitable D_0.

□

Example. Due to the strength of the theorem of Davenport and Heilbronn, many elliptic curves with rational 3-torsion have the property that the proportion of D for which $S(E(D))_3 = \{1\}$ is quite large. For example, if $E/\mathbb{Q}$ is the conductor 14 curve

$$E: \quad y^2 = x^3 + x^2 + 72x - 368,$$

then

$$\lim_{X\to\infty}\left[\frac{\#\{-X < D < 0 \ : \ D \text{ square-free and } S(E(D))_3 = \{1\}\}}{\#\{-X < D < 0 \ : \ D \text{ square-free}\}}\right] \geq \frac{7}{128}.$$

For further details and examples, the reader may consult [Ja2].

References

[A-Bu-Fr] J. A. Antoniadis, M. Bungert, and G. Frey, *Properties of twists of elliptic curves*, J. reine ange. math. **405** (1990), 1-28.

[B] J. H. Bruinier, *Non-vanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. (accepted for publication).

[Bu–F–Ho] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), 543-618.

[D–H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. Lond. A **322** (1971), 405-420.

[Du] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris **325** (1997), 813-818.

[Fr] G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. **15** (1988), 649-665.

[F-H] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on $GL(2)$*, Ann. Math. **142** (1995), 385-423.

[Gol] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes **751** (1979), 108-118.

[Go-M] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1-23.

[G-S] R. Greenberg and G. Stevens, *On the conjecture of Mazur, Tate, and Teitelbaum*, p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, Ma. 1991), Contemp. Math. 165 (B. Mazur and G. Stevens, ed.), 1994, pp. 183-211.

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

[HB] D. R. Heath Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), 171-195.

[HB2] D. R. Heath Brown, *The size of Selmer groups for the congruent number problem, II*, Invent. Math. **118** (1994), 331-370.

[H-N] K. Horie and J. Nakagawa, *Elliptic curves with no torsion points*, Proc. Amer. Math. Soc. **104** (1988), 20-25.

[I] H. Iwaniec, *On the order of vanishing of modular L-functions at the critical point*, Sém. Thér. Nombres Bordeaux **2** (1990), 365-376.

[Ja1] K. James, *L-series with non-zero central critical value*, J. Amer. Math. Soc. **11** (1998), 635-641.

[Ja2] K. James, *Elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture mod 3.*, J. Number Theory (to appear).

[J] N. Jochnowitz, *Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves,* (preprint).

[K-O] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math., (accepted for publication).

[Ko] V.A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and the Tate-Shafarevich group of $E(\mathbb{Q})$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk, USSR, ser. Matem. **52** (1988).

[Ko2] V. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Progress in Math. 87, ed. P. Cartier et. al. (1990), 435-483.

[Ma-W] D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), 247-254.

[M] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129-162.

[M-T-T] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1-48.

[Mu–Mu] M. R. Murty and V.K. Murty, *Mean values of derivatives of modular L-series*, Ann. Math. **133** (1991), 447-475.

[O-S] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo ℓ*, Ann. Math. **147** (1998), 453-470.

[O-S2] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math., (accepted for publication).

[Se] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[Sh] G. Shimura, *On modular forms of half-integral weight*, Ann. Math. **97** (1973), 440-481.

[Si] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[St] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), 275-280.

[Sw-D] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Springer Lect. Notes **350** (1973), 1-55.

[T] J.B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983), 323-334.

[V] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. (accepted for publication).

[Wal] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

[Wo] S. Wong, *Rank zero twists of elliptic curves* (preprint).

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail address: ono@math.psu.edu

Department of Mathematics, Penn State University, University Park, Pa. 16802
E-mail address: klj@math.psu.edu