QUADRATIC TWISTS OF MODULAR FORMS AND ELLIPTIC CURVES

Ken Ono and Matthew A. Papanikolas

1. Introduction

Here we summarize the results presented in the first author's lecture at the Millenial Conference on Number Theory. Some of these results appear in [O] in full detail. In addition, we present a new result regarding the growth of Tate-Shafarevich groups of certain elliptic curves over elementary abelian simple 2-extensions.

We begin by fixing notation. Suppose that $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(\Gamma_0(M))$ ($q := e^{2\pi iz}$ throughout) is an even weight newform on $\Gamma_0(M)$ with trivial Nebentypus character. As usual, let $L(F, s)$ denote its L-function which is defined by analytically continuing

$$L(F, s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

If D is a fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, then let $\chi_D = \left(\frac{D}{\bullet}\right)$ denote its usual Kronecker character. Let $F \otimes \chi_D$ denote the newform that is the D-quadratic twist of F, and let $L(F \otimes \chi_D, s)$ denote the associated L-function. In particular, if $\gcd(D, M) = 1$, then

$$(F \otimes \chi_D)(z) = \sum_{n=1}^{\infty} \chi_D(n)a(n)q^n.$$

Given a fixed F, we consider the behavior of the central critical values $L(F \otimes \chi_D, k)$ as D varies. In an important paper, Goldfeld [G] conjectured that

$$\sum_{\substack{|D| \le X \\ \gcd(D,M)=1}} \operatorname{ord}_{s=k} \left(L(F \otimes \chi_D, s)\right) \sim \frac{1}{2} \sum_{\substack{|D| \le X \\ \gcd(D,M)=1}} 1. \tag{1}$$

(note. This conjecture was originally formulated for weight 2 newforms associated to modular elliptic curves). Obviously, this conjecture implies the weaker statement

$$\#\{|D| \le X \ : \ L(F \otimes \chi_D, k) \neq 0\} \gg_F X. \tag{2}$$

The first author thanks the National Science Foundation, the Alfred P. Sloan Foundation and the David and Lucile Packard Foundation for their generous research support.

Using a variety of methods, early works by Bump, Friedberg, Hoffstein, Iwaniec, Murty, Murty and Waldspurger (see [B-F-H], [I], [M-M], [W]) produced a number of important nonvanishing theorems in the direction of (2). More recently, Katz and Sarnak [Ka-Sa] provided (among many other results) conditional proofs of (2). However, this claim has only been proven for certain special newforms by the works of James, Kohnen and Vatsal [J, Ko, V]. These cases require that the modular forms possess exceptional mod 3 Galois representations. The best unconditional general result in the direction of (2) is due to the first author and Skinner. They proved that

$$\#\{|D| \leq X \ : \ L(F \otimes \chi_D, k) \neq 0\} \gg_F X/\log X. \tag{3}$$

We obtain, for almost every F, the following minor improvement of (3).

Theorem 1. *Let $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(\Gamma_0(M))$ be an even weight newform and let K be a number field containing the coefficients $a(n)$. If v is a place of K over 2 and there is a prime $p \nmid 2M$ for which*

$$\mathrm{ord}_v(a(p)) = 0, \tag{4}$$

then there is a rational number $0 < \alpha < 1$ for which

$$\#\{|D| \leq X \ : \ L(F \otimes \chi_D, k) \neq 0\} \gg_F \frac{X}{\log^{1-\alpha} X}.$$

This result has immediate implications for elliptic curves. We begin by fixing notation. Suppose that $E/\mathbb{Q}$ is an elliptic curve

$$E: \quad y^2 = x^3 + ax + b,$$

and let $L(E, s) = \sum_{n=1}^{\infty} a_E(n)n^{-s}$ be its Hasse-Weil L-function. For integers d which are not perfect squares, let $E(d)$ denote the d-quadratic twist of E

$$E(d): \quad dy^2 = x^3 + ax + b.$$

Moreover, if E is an elliptic curve defined over a number field K, then let $rk(E, K)$ denote the rank of the Mordell-Weil group $E(K)$. Similarly, let $Ш(E, K)$ denote the Tate-Shafarevich group of E/K.

By a celebrated theorem of Kolyvagin [Kol] and the modularity of E, (2) implies the widely held speculation that

$$\#\{|D| \leq X \ : \ rk(E(D), \mathbb{Q}) = 0\} \gg_E X. \tag{5}$$

Heath-Brown confirmed (5) for the congruent number elliptic curves in [HB], and subsequent works by James and Vatsal [Ko, V] confirm this assertion for a variety of families of quadratic twists which contain an elliptic curve with a rational torsion point of order 3. However, (5) remains open for most elliptic curves. In this direction, Theorem 1 implies the following result.

Corollary 2. *If $E/\mathbb{Q}$ is an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2, then there is a number $0 < \alpha(E) < 1$ for which*

$$\#\{|D| \le X \ : \ rk(E(D), \mathbb{Q}) = 0\} \gg_E \frac{X}{\log^{1-\alpha(E)} X}.$$

Theorem 1 and Corollary 2 depend on a nonvanishing theorem (see Theorem 2.1) which guarantees the existence of a fat set of discriminants D, which is closed under multiplication, for which $L(F \otimes \chi_D, k) \neq 0$. The most interesting consequence of Theorem 2.1 may be the following result concerning the triviality of the rank of the Mordell-Weil group of most elliptic curves E over prescribed elementary abelian 2-extensions of $\mathbb{Q}$ of arbitrarily large degree.

Theorem 3. *Let $E/\mathbb{Q}$ be an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. Then there is a fundamental discriminant D_E and a set of primes S_E with positive density with the property that for every positive integer j we have*

$$rk(E(D_E), \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_j})) = rk(E(D_E), \mathbb{Q}) = 0$$

whenever the integers $m_1, m_2, \ldots, m_j > 1$ satisfy the following conditions:

1. *Each m_i is square-free with an even number of prime factors.*
2. *All of the prime factors of each m_i are in S_E.*

Theorem 2.1 may also be used to prove the existence of non-trivial elements of Tate-Shafarevich groups of elliptic curves. Regarding Tate-Shafarevich groups, works by Bölling, Cassels, Kramer, and Rohrlich [Bö, Ca, Kr, R] yield a variety of results concerning the non-triviality of the 2 and 3-parts of Tate-Shafarevich groups for families of elliptic curves. Less is known about the non-triviality of p-parts of $Ш(E)$ for primes $p \ge 5$.

Under a natural hypothesis, Theorem 2.1 and a theorem of Frey yield a general result which holds for many (if not all) curves E whose Mordell-Weil group over $\mathbb{Q}$ has torsion subgroup $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$. For simplicity we present the following special case of this result.

Theorem 4. *Suppose that $E/\mathbb{Q}$ is an elliptic curve whose torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/\ell\mathbb{Z}$ with $\ell \in \{3, 5, 7\}$. If E is good at ℓ (see §3), has good reduction at ℓ and has the property that there is an odd prime $p_0 \equiv -1 \pmod{\ell}$ of bad reduction with*

$$\mathrm{ord}_{p_0}(\Delta(E)) \not\equiv 0 \pmod{\ell},$$

where $\Delta(E)$ is the discriminant of E, then there are infinitely many negative square-free integers d for which

$$rk(E(d), \mathbb{Q}) = 0 \quad \text{and} \quad \#Ш(E(d), \mathbb{Q}) \equiv 0 \pmod{\ell}.$$

Remark. Earlier work of Wong [Wo] implied that every elliptic curve without a $\mathbb{Q}$-rational point of order 2 is good at ℓ. We employed his result in a crucial way to obtain [Th. 5, O] and [Cor. 6, O]. Unfortunately, we have been informed that there is a mistake in Wong's argument. Therefore, readers should be aware that [Th. 5, O] and [Cor. 6, O] are true for elliptic curves that are good at ℓ (see §3).

Using Theorems 3 and 4, we obtain the next theorem which shows, for certain elliptic curves $E/\mathbb{Q}$, that there are infinitely many number fields K for which both

$$rk(E,K) \gg_E \log([K:\mathbb{Q}]),$$
$$rk_p(Ш(E,K)) \gg_E \log([K:\mathbb{Q}]).$$

Theorem 5. *Let $E/\mathbb{Q}$ be an elliptic curve whose torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/p\mathbb{Z}$ with $p \in \{3,5,7\}$. If E is good at p (see §3), has good reduction at p, and has the property that there is an odd prime $p_0 \equiv -1 \pmod{p}$ of bad reduction with*

$$\mathrm{ord}_{p_0}(\Delta(E)) \not\equiv 0 \pmod{p},$$

where $\Delta(E)$ is the discriminant of E, then for every pair of non-negative integers r_m and r_s there are $r_m + r_s$ square-free integers $d_1, d_2, \dots, d_{r_m+r_s}$ with

$$rk(E, \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_{r_m+r_s}})) \geq 2r_m,$$
$$rk_p(Ш(E, \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_{r_m+r_s}})) \geq 2r_s.$$

In §2 we describe Theorem 2.1 and give a brief sketch of its proof, and in §3 we sketch the proofs of Theorem 1, 3, 4 and 5.

2. The crucial nonvanishing theorem

The next theorem is the main result which is vital for all of the results described in §1.

Theorem 2.1. *Let $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(\Gamma_0(M))$ be an even weight newform and let K be a number field containing the coefficients $a(n)$. If v is a place of K over 2 and there is a prime $p \nmid 2M$ for which*

$$\mathrm{ord}_v(a(p)) = 0, \tag{2.1}$$

then there is a fundamental discriminant D_F and a set of primes S_F with positive density such that for every positive integer j we have

$$L(F \otimes \chi_{p_1 p_2 \cdots p_{2j} D_F}, k) \neq 0$$

whenever $p_1, p_2, \dots, p_{2j} \in S_F$ are distinct primes not dividing D_F.

Sketch of the Proof. We begin by recalling a theorem due to Waldspurger [Th. 1, W] on the Shimura correspondence [Sh]. This result expresses many of the central critical values $L(F \otimes \chi_D, k)$ in terms of the Fourier coefficients of certain half integral weight cusp forms.

For every fundamental discriminant D, define D_0 by

$$D_0 := \begin{cases} |D| & \text{if } D \text{ is odd,} \\ |D|/4 & \text{if } D \text{ if even.} \end{cases} \tag{2.2}$$

If $\delta \in \{\pm 1\}$ is the sign of the functional equation of $L(F, s)$, then there is a positive integer N with $M \mid N$, a Dirichlet character χ modulo $4N$, a non-zero complex number Ω_F and a non-zero half integral weight eigenform

$$g_F(z) = \sum_{n=1}^{\infty} b_F(n) q^n \in S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$$

with the property that if $\delta D > 0$, then

$$b_F(D_0)^2 = \begin{cases} \epsilon_D \cdot \frac{L(F \otimes \chi_D, k) D_0^{k-\frac{1}{2}}}{\Omega_F} & \text{if } \gcd(D_0, 4N) = 1, \\ 0 & \text{otherwise,} \end{cases} \tag{2.3}$$

where ϵ_D is algebraic. Moreover, the coefficients $a(n), b_F(n)$ and the values of χ are in O_K, the ring of integers of some fixed number field K. In addition, if $p \nmid 4N$ is prime, then

$$\lambda(p) = \chi^2(p) a(p), \tag{2.4}$$

where $\lambda(p)$ is the eigenvalue of $g_F(z)$ for the half integer weight Hecke operator $T_k^{\chi}(p^2)$ on $S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$.

Define the integer s_0 by

$$s_0 := \min\{\mathrm{ord}_v(b_F(n))\}. \tag{2.5}$$

In addition, let $G_F(z)$ be the integer weight cusp form defined by

$$G_F(z) = \sum_{n=1}^{\infty} b_g(n) q^n := g_F(z) \cdot \left(1 + 2 \sum_{n=1}^{\infty} q^{n^2}\right). \tag{2.6}$$

It is easy to see that if n is a positive integer, then

$$b_g(n) = b_F(n) + 2 \sum_{t=1}^{\infty} b_F(n - t^2) \equiv b_F(n) \pmod 2. \tag{2.7}$$

It is our goal to determine conditions under which $b_g(n)$ is non-zero modulo 2. To achieve this, we employ classical results regarding modular Galois representations due to Deligne and Serre [D, D-S].

Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(M), \psi)$ is an integer weight newform and suppose that K is a number field whose ring of integers O_K contains the Fourier coefficients $a(n)$ and the values of ψ. If O_v is the completion of O_K at any finite place v of K, say with residue characteristic ℓ, then there is a continuous representation

$$\rho_{f,v} : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(O_v)$$

with the property that if $p \nmid \ell M$ is prime, then

$$\mathrm{Tr}(\rho_{f,v}(Frob(p))) = a_f(p).$$

Using these representations, we are able to study the arithmetic of the Fourier expansions of a collection of integer weight cusp forms with coefficients that are algebraic integers. Suppose that $f_1(z), f_2(z), \dots, f_y(z)$ are integer weight cusp forms with

$$f_i(z) = \sum_{n=1}^{\infty} a_i(n)q^n \in S_{k_i}(\Gamma_0(M_i), \chi_i).$$

Suppose that the coefficients of all the $f_i(z)$ and the values of all the χ_i are in O_K, (for some sufficiently large number field K), and let v be a finite place of K with residue characteristic ℓ. If $p_0 \nmid \ell M_1 M_2 \cdots M_y$ is prime and j is a positive integer, then the Chebotarev Density theorem implies that there is a set of primes p, of positive density, such that for every $1 \le i \le y$ we have

$$\mathrm{ord}_v \left(f_i(z) \mid T_{p_0}^{k_i,\chi_i} - f_i(z) \mid T_p^{k_i,\chi_i} \right) > j. \tag{2.8}$$

In view of (2.4), there is a prime $p_0 \nmid 4N$ for which $\mathrm{ord}_v(\lambda(p_0)) = 0$. Applying (2.8) to $G_F(z)$ and $F(z)$, there is a set of primes S_{p_0} with positive density with the property that every prime $p \in S_{p_0}$ satisfies

$$\mathrm{ord}_v(\lambda(p)) = \mathrm{ord}_v(\lambda(p_0)) = 0, \tag{2.9}$$

and

$$\mathrm{ord}_v \left(G_F(z) \mid T_p^{k+1,\chi\chi_{-1}^{k+1}} - G_F(z) \mid T_{p_0}^{k+1,\chi\chi_{-1}^{k+1}} \right) > s_0. \tag{2.10}$$

Suppose that m is a positive integer for which $\mathrm{ord}_v(b_F(m)) = s_0$, and suppose that $q_1, q_2 \in S_{p_0}$ are distinct odd primes which are coprime to m. Using the definition of the integer and half integral weight Hecke operators, one easily checks that the coefficient of q^{mq_1}, in $G_F(z) \mid T_{q_1}^{k+1,\chi\chi_{-1}^{k+1}}$ is

$$\lambda(q_1)b_g(m) + b_g(m)\chi^\star(q_1)q_1^{k-1}\left(\chi_{-1}(q_1)q_1 - \left(\frac{m}{q_1}\right)\right),$$

where $\chi^\star(p) := \chi(p)\left(\frac{-1}{p}\right)^k$. Since $\chi_{-1}(q_1)q_1 - \left(\frac{m}{q_1}\right) \equiv 0 \pmod 2$, by (2.9), we find that the coefficient of q^{mq_1} in $G_F(z) \mid T_{q_1}^{k+1,\chi\chi_{-1}^{k+1}}$ has ord_v equal to s_0. By (2.10), the coefficient of q^{mq_1} in $G_F(z) \mid T_{q_2}^{k,\chi\chi_{-1}^{k+1}}$ also has $\mathrm{ord}_v = s_0$, and this equals

$$b_g(mq_1q_2) + \chi(q_2)\chi_{-1}^{k+1}(q_2)q_2^k b_g(mq_1/q_2) = b_g(mq_1q_2).$$

This shows that if $\mathrm{ord}_v(b_F(m)) = s_0$ and $q_1, q_2 \in S_{p_0}$ are distinct odd primes which do not divide m, then $\mathrm{ord}_v(b_F(mq_1q_2)) = s_0$. In view of (2.3), the theorem follows by iterating this observation.

□

3. The loose ends

In this section we sketch the proofs of Theorem 1, 3 and 4.

Sketch of the proof of Theorem 1. Let T be a set of primes with density $0 < \alpha < 1$, and let $\mathbb{N}_T$ denote the set

$$\mathbb{N}_T := \{n \in \mathbb{N} \ : \ n = \prod_i p_i, \ p_i \in T, \text{ and } \mu(n) = 1\}. \tag{3.1}$$

Here μ denotes the usual Möbius function.

Generalizing an argument of Landau, Serre proved [Th. 2.8, S] that

$$\#\{n \le X \ : \ n = \prod_i p_i \ \text{ with } \ p_i \in T\} = c_T \cdot \frac{X}{\log^{1-\alpha} X} + O\left(\frac{X}{\log^{2-\alpha} X}\right)$$

for some positive constant c_T. A simple sieve argument yields

$$\#\{n \in \mathbb{N}_T \ : \ n \le X\} \gg \frac{X}{\log^{1-\alpha} X}.$$

Theorem 1 follows immediately from this estimate and Theorem 2.1.

□

Sketch of the proof of Theorem 3. Since $a_E(p)$ is even for all but finitely many primes p if and only if E has a rational point of order 2, we may freely apply Theorem 2.1. By the modularity of E and Kolyvagin's theorem, if $L(E(D), 1) \neq 0$, then $rk(E(D), \mathbb{Q}) = 0$. Suppose that $S := \{m_1, m_2, \ldots, m_t\}$ is a set of square-free pairwise coprime integers > 1 where all the prime factors of each m_i are in the prescribed set of primes. If each m_i has an even number of prime factors, then for each $1 \le s \le t$ and any distinct $d_1, d_2, \ldots, d_s \in S$ we have

$$rk(E(d_1d_2\cdots d_s), \mathbb{Q}) = 0.$$

Theorem 3 now follows from the fact that

$$rk(E, K(\sqrt{d})) = rk(E, K) + rk(E(D), K)$$

whenever $[K(\sqrt{d}) : K] = 2$.

□

Let $E/\mathbb{Q}$ be an elliptic curve whose torsion subgroup over $\mathbb{Q}$ is $\mathbb{Z}/\ell\mathbb{Z}$ where $\ell \in \{3, 5, 7\}$. By Theorem 2.1, there is a discriminant d_E and a subset of primes of primes S_E such that for every set of distinct odd primes $p_1, \dots, p_{2j} \in S_E$ coprime to d_E we have

$$L(E(d_E p_1 \cdots p_{2j}), 1) \neq 0.$$

We say that E is *good at* ℓ if there are infinitely many such negative fundamental discriminants $D = d_E p_1 \cdots p_{2j}$ for which the following hold:

(*i*) We have $\ell \mid \#Cl(D)$, the ideal class group of the quadratic field $\mathbb{Q}(\sqrt{D})$.
(*ii*) We have $\gcd(D, \ell N(E)) = 1$, where $N(E)$ is the conductor of E.
(*iii*) We have $D \equiv 0 \pmod 4$ and $D/4 \equiv 3 \pmod 4$.
(*iv*) If $\mathrm{ord}_\ell(j(E)) < 0$, then $\left(\frac{D}{\ell}\right) = -1$.
(*v*) Every prime $p \mid N(E)$ with $p \notin \{2, \ell\} \cup S_E$ and with the additional property that $p \not\equiv -1 \pmod \ell$ or $\mathrm{ord}_p(\Delta(E)) \not\equiv 0 \pmod \ell$ satisfies:

$$\left(\frac{D}{p}\right) = \begin{cases} -1 & \text{if } \mathrm{ord}_p(j(E)) \geq 0, \\ -1 & \text{if } \mathrm{ord}_p(j(E)) < 0 \text{ and } E/\mathbb{Q}_p \text{ is a Tate curve}, \\ 1 & \text{otherwise.} \end{cases}$$

Sketch of the proof of Theorem 4. Let ℓ be an odd prime such that $E/\mathbb{Q}$ is an elliptic curve with good reduction at ℓ with a $\mathbb{Q}$-rational point of order ℓ. If D is a negative fundamental discriminant satisfying the conditions appearing in the definition above, then Frey [F] proved that

$$\#Cl(D)_\ell \mid \#S_\ell(E(D), \mathbb{Q}).$$

Here $Cl(D)_\ell$ denotes the ℓ-part of the ideal class group of $\mathbb{Q}(\sqrt{D})$, and $S_\ell(E(D), \mathbb{Q})$ is the ℓ-Selmer group of $E(D)$ over $\mathbb{Q}$.

Let S_E be the set of primes with positive density given in Theorem 2.1. Then there is a discriminant d_E, and a subset $\tilde{S}_E$ of S_E, such that for every set of distinct odd primes $p_1, p_2, \dots, p_{2j} \in \tilde{S}_E$ which are coprime to d_E we have

$$L(E(d_E p_1 p_2 \cdots p_{2j}), 1) \neq 0, \tag{3.2}$$

$$\#Cl(d_E p_1 p_2 \cdots p_{2j})_\ell \mid \#S_\ell(E(d_E p_1 p_2 \cdots p_{2j}), \mathbb{Q}). \tag{3.3}$$

By Kolyvagin's theorem, (3.2) implies that $E(d_E p_1 p_2 \cdots p_{2j})$ has rank zero. Therefore, we find that if $p_1, p_2, \dots, p_{2j} \in \tilde{S}_E$ are distinct primes which do not divide d_E, then

$$\#Cl(d_E p_1 p_2 \cdots p_{2j})_\ell \equiv 0 \pmod \ell \;\Rightarrow\; \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \subseteq Ш(E(d_E p_1 p_2 \cdots p_{2j})).$$

Therefore, it suffices to prove that there are infinitely many suitable discriminants satisfying (3.2) and (3.3) with the additional property that $\ell \mid \#Cl(d_E p_1 p_2 \cdots p_{2j})_\ell$. This is guaranteed since E is good at ℓ.

□

Now we prove Theorem 5. We begin by fixing notation. For an abelian group A and a positive integer m, we let $A[m]$ denote the m-torsion of A, and for a prime p, we let $rk_p(A)$ denote the p-rank of $A[p]$. If A is finitely generated, we let $rk(A)$ denote its rank. For a Galois extension of fields L/K, we let $G_{L/K}$ denote the Galois group. We let $G_K = G_{\overline{K}/K}$. For $d \in K$, we let $K_d = K(\sqrt{d})$ and $G_d = G_{K_d/K}$.

Our results depend on the following relations between p-ranks of Tate-Shafarevich and Mordell-Weil groups of elliptic curves upon a quadratic extension. Here $S_p(E, K)$ denotes the p-Selmer group of an elliptic curve E/K.

Lemma 3.1. *Let E be an elliptic curve defined over a number field K. Let p be an odd prime, and let d be a non-square in K. Let $r(E, K)$ denote either $rk(E, K)$, $rk_p(S_p(E, K))$, or $rk_p(Ш(E, K))$. Then*

$$r(E, K_d) = r(E, K) + r(E(d), K).$$

Proof. The result for the rank of $E(K_d)$ is well-known. Let G_d be represented by $\{1, \rho\} \subset G_K$. Fix an isomorphism $\phi : E \to E(d)$ defined over K_d so that $\rho\phi(Q) = -\phi(\rho Q)$ for all $Q \in E(\overline{K})$. As p is odd, we note that

$$E(K_d)[p] \cong E(K)[p] \oplus E(d)(K)[p]$$

via the map $Q \mapsto \frac{1}{2}(\rho Q + Q, \phi(\rho Q - Q))$. Therefore the result also holds for $r(E, K_d) = rk_p(E(K_d)/pE(K_d))$.

By the exact sequence

$$0 \to E(K_d)/pE(K_d) \to S_p(E, K_d) \to Ш(E, K_d)[p] \to 0,$$

it now suffices to prove the result for Selmer groups. The Selmer group decomposes as

$$S_p(E, K_d) = S_p(E, K_d)^{G_d, +} \oplus S_p(E, K_d)^{G_d, -},$$

where the first group is the G_d-invariants of $S_p(E, K_d)$ and the second comprises those elements on which ρ acts by -1. Since p is odd, the Galois cohomology groups $H^i(G_d, E(K_d)[p])$ are trivial for $i \geq 1$; therefore, by the Hochschild-Serre spectral sequence, the restriction map $H^1(G_K, E[p]) \to H^1(G_{K_d}, E[p])^{G_d}$ is an isomorphism. Thus it follows that

$$\text{res} : S_p(E, K) \to S_p(E, K_d)^{G_d}$$

is an isomorphism. Likewise, $S_p(E(d),K) \cong S_p(E(d),K_d)^{G_d}$. If $\tilde{\phi}$ is the map induced by ϕ on cohomology, then one can check that

$$\tilde{\phi} : H^1(G_{K_d}, E[p])^{G_{d,-}} \to H^1(G_{K_d}, E(d)[p])^{G_d}$$

is well-defined and an isomorphism. For each place v of K_d the map

$$\tilde{\phi} : H^1(G_{K_{d,v}}, E(\overline{K}_{d,v})) \to H^1(G_{K_{d,v}}, E(d)(\overline{K}_{d,v}))$$

is necessarily an isomorphism, so it follows from the definition of the Selmer group that

$$\tilde{\phi} : S_p(E,K_d)^{G_{d,-}} \to S_p(E(d),K_d)^{G_d}$$

is also an isomorphism. Therefore $S_p(E,K_d)^{G_{d,-}} \cong S_p(E(d),K)$, and we are done.

□

The following theorem is a weak version of one of the main results in [St-T].

Theorem 3.2. *If $E/\mathbb{Q}$ is an elliptic curve, then for every positive integer r_m there are distinct square-free integers $D_1, D_2, \dots, D_{r_m}$ for which*

$$rk(E(D_i),\mathbb{Q}) \geq 2.$$

Proof of Theorem 5. Using Theorem 3.2, let $D_1, D_2, \dots D_{r_m}$ be distinct square-free integers for which $rk(E(D_i),\mathbb{Q}) \geq 2$. Hence, Lemma 3.1 implies that

$$rk(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\dots,\sqrt{D_{r_m}})) \geq \sum_{j=1}^{r_m} rk(E(D_j),\mathbb{Q}) = 2r_m. \tag{3.4}$$

Similarly, by Theorem 4 there are r_s many distinct square-free integers $d_1, d_2, \dots, d_{r_s}$ for which

$$rk(E(d_i),\mathbb{Q}) = 0 \ \text{ and } \ \#Ш(E(d_i),\mathbb{Q}) \equiv 0 \pmod{p}.$$

By the proof of Theorem 4 and Kolyvagin's theorem on the Birch and Swinnerton-Dyer Conjecture (i.e. finiteness of $Ш(E,\mathbb{Q})$ and the existence of the Cassels-Tate pairing implies that $rk_p(Ш(E,\mathbb{Q}))$ is even), it follows that for each such d_i that

$$rk_p(Ш(E(d_i),\mathbb{Q})) \geq 2.$$

Therefore, by Lemma 3.1 we get

$$rk_p(Ш(E,\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\dots,\sqrt{d_{r_s}}))) \geq \sum_{j=1}^{r_s} rk_p(Ш(E(d_i),\mathbb{Q})) \geq 2r_s. \tag{3.5}$$

Consequently, (3.4), (3.5) and Lemma 3.1 imply that

$$rk(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\dots,\sqrt{D_{r_m}},\sqrt{d_1},\sqrt{d_2},\dots,\sqrt{d_{r_s}}) \geq 2r_m,$$
$$rk_p(E,\mathbb{Q}(\sqrt{D_1},\sqrt{D_2},\dots,\sqrt{D_{r_m}},\sqrt{d_1},\sqrt{d_2},\dots,\sqrt{d_{r_s}}) \geq 2r_s.$$

This completes the proof.

□

References

[Bö] R. Bölling, *Die Ordung der Schafarewitsch-Tate Gruppe kann beliebeg gross werden*, Math. Nachr. **67** (1975), 157-179.

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

[Ca] J. W. S. Cassels, *Arithmetic on curves of genus 1 (VI). The Tate-Shafarevich group can be arbitrarily large*, J. reine. angew. math. **214/215** (1964), 65-70.

[D] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sem. Bourbaki 1968/1969, Exposé 355, Springer Lect. Notes 179 (1971), 139-172.

[D-S] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Scient. Ec. Norm. Sup., Sér. 4 **7** (1974), 507-530.

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

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

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

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

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

[Ka-Sa] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy, Amer. Math. Soc. Colloq. Publ.*, vol. 45, Amer. Math. Soc., Providence, 1999.

[Ko] W. Kohnen, *On the proportion of quadratic twists of L-functions attached to cusp forms not vanishing at the central point*, J. reine. angew. math. **508** (1999), 179-187.

[Kol] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk., USSR, ser. Matem. **52** (1988), 522-540.

[Kr] K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevich groups*, Proc. Amer. Math. Soc. **89** (1983), 473-499.

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

[O] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. reine angew. math **533** (2001), 81-97.

[O-Sk] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651-660.

[R] D. Rohrlich, *Unboundedness of the Tate-Shafarevich group in families of quadratic twists, Appendix to J. Hoffstein and W. Luo, Nonvanishing of L-series and the combinatorial sieve*, Math. Res. Lett. **4** (1997), 435-444.

[S] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Enseign. Math. **22** (1976), 227-260.

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

[S] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[St-T] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc, **8 no. 4** (1995), 947-974.

[V] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), 397-419.

[W] 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, *Elliptic curves and class number divisibility*, Int. Math. Res. Not. **12** (1999), 661-672.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: ono@math.wisc.edu

Department of Mathematics, Brown University, Providence, Rhode Island 02912

E-mail address: map@math.brown.edu