NONVANISHING OF QUADRATIC TWISTS OF MODULAR L-FUNCTIONS AND APPLICATIONS TO ELLIPTIC CURVES

Ken Ono

J. reine angew. math., 533, 2001, pages 81-97

1. Introduction and Statement of Results

If $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(\Gamma_0(M), \chi_0)$ (note: $q := e^{2\pi iz}$ throughout) is a newform of even integer weight $2k$ with trivial character χ_0, then let $L(F, s)$ be its L-function

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

If d is square-free or is a fundamental discriminant, then let $\chi_d = \chi_D$ denote the Kronecker character for the quadratic field $\mathbb{Q}(\sqrt{d})$ whose fundamental discriminant is D. Throughout D shall denote a fundamental discriminant. The D-quadratic twist of F, denoted $F \otimes \chi_D$, is the newform corresponding to the twist of F by the character χ_D. In particular, if $\gcd(M, D) = 1$, then $(F \otimes \chi_D)(z) = \sum_{n=1}^{\infty} \chi_D(n)a(n)q^n$ and

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

We establish, for those newforms satisfying a mild hypothesis, a curious multiplicative property for many D for which $L(F \otimes \chi_D, k) \neq 0$.

Before we state our result we recall that a set of primes S is said to have Frobenius density if there is a Galois extension $K/\mathbb{Q}$ with the property that those primes $p \in S$, up to finitely many exceptions, are distinguished as those primes for which the $Frob(p)$ constitute a fixed conjugacy class c or a union of conjugacy classes in $\mathrm{Gal}(K/\mathbb{Q})$. By the Chebotarev Density Theorem, a set S corresponding to a conjugacy class c has density $\alpha = \#c/\#\mathrm{Gal}(K/\mathbb{Q})$. The density for general S are defined in the obvious way.

1991 *Mathematics Subject Classification.* Primary 11F37; Secondary 11G05.

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

Theorem 1. *Let $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(\Gamma_0(M), \chi_0)$ 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*

$$\text{ord}_v(a(p)) = 0, \tag{1.1}$$

then there is a fundamental discriminant D_F and a set of primes S_F with positive Frobenius 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.

It is easy to see that the choice of D_F is not unique.

In an important paper [G], Goldfeld conjectured that

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

(note: The original form of this conjecture was for weight 2 newforms $F(z)$ associated to modular elliptic curves). Obviously, this conjecture implies the weaker conjecture that

$$\#\{|D| \leq X \ : \ L(F \otimes \chi_D, k) \neq 0 \text{ and } \gcd(D, M) = 1\} \gg_F X. \tag{1.2}$$

Recent important work by Katz and Sarnak [Ka-Sa] yields, among many other results, conditional proofs of (1.2). Although there has been some recent success in proving (1.2) unconditionally for exceptional $F(z)$ (those with exceptional mod 3 Galois representations) by the works of James, Kohnen, and Vatsal [J, Ko, V], the best unconditional lower bound for general F is due to the author and Skinner. They established [Cor. 3, O-Sk] that

$$\#\{|D| \leq X \ : \ L(F \otimes \chi_D, k) \neq 0 \text{ and } \gcd(D, M) = 1\} \gg_F \frac{X}{\log X}. \tag{1.3}$$

For most $F(z)$ we obtain the following modest improvement to (1.3).

Corollary 2. *If $F(z) \in S_{2k}(\Gamma_0(M), \chi_0)$ is a newform satisfying (1.1), then*

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

where $0 < \alpha < 1$ is the density of S_F.

Hypothesis (1.1) in Theorem 1.1 is a mild condition which is satisfied by most newforms (there are exceptions like $\Delta(z)$). For example, almost every weight 2 newform associated to an elliptic curve $E/\mathbb{Q}$ satisfies (1.1) (for example, see [Du]).

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 $E(K)$.

Suppose that $E/\mathbb{Q}$ is an elliptic curve. Then (1.2) together with a celebrated theorem of Kolyvagin and the modularity of E implies that

$$\#\{|D| \ : \ rk(E(D),\mathbb{Q}) = 0\} \gg_E X. \tag{1.4}$$

Heath-Brown confirmed (1.4) for the congruent number elliptic curve in [HB], and subsequent works by James, Vatsal and Wong [Ko, V, Wo] confirm this assertion for a variety of elliptic curves with rational torsion points of order 3. However, (1.4) remains open for most elliptic curves.

Corollary 3. *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*

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

The most interesting consequence of Theorem 1 may be the following result concerning the triviality of the rank of the Mordell-Weil group of most elliptic curves E over arbitrarily large prescribed elementary abelian 2-extensions of $\mathbb{Q}$.

Theorem 4. *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 Frobenius density $0 < \alpha(E) < 1$ with the property that for every positive integer j we have*

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

whenever the integers $m_1, m_2, \dots, m_j > 1$ 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.*

As in Theorem 1, the choice of D_E is not unique.

The last consequence of Theorem 1 that we would like to point out involves Tate-Shafarevich groups of quadratic twists. By the works of Bölling, Cassels, Kramer, and

Rohrlich [Bö, Ca, Kr, R], quite a bit is known about the non-triviality of the 2 and 3-parts of Tate-Shafarevich groups. However, much less is known about the non-triviality of p-parts of $Ш(E)$ for primes $p \geq 5$. In this direction, Wong [Wo] has proved that infinitely many quadratic twists of $X_0(11)$ have elements of order 5 in their Tate-Shafarevich groups. We know of no other similar results when $p = 5$ for any other elliptic curve or any results for $p \geq 7$.

Wong obtained his result by combining an old observation of the author and Frey with his own results regarding the prime factorization of the discriminants of certain quadratic fields whose class groups have elements of fixed order ℓ (e.g. in this case $\ell = 5$). Using Theorem 1, a theorem of Frey, and a simple refinement of Wong's strategy for $X_0(11)$ we obtain a general result which probably holds for almost all curves E whose Mordell-Weil group over $\mathbb{Q}$ has torsion subgroup $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$. The hypotheses which need to be verified for any given E are cumbersome and unmotivating. For aesthetics, here we simply refer to an E which satisfies these hypotheses for a given prime $\ell \in \{3, 5, 7\}$ as an *excellent elliptic curve at* ℓ. We shall defer the explicit definition to §5.

Theorem 5. *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 excellent at ℓ, then there are infinitely many negative square-free integers d for which*

$$rk(E(d), \mathbb{Q}) = 0 \qquad \text{and} \qquad \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \subseteq Ш(E(d), \mathbb{Q}).$$

Here is a special case of Theorem 5.

Corollary 6. *Suppose that $E/\mathbb{Q}$ is an elliptic curve whose torsion subgroup over $\mathbb{Q}$ is $Z/\ell\mathbb{Z}$ with $\ell \in \{3, 5, 7\}$. If E has good reduction at ℓ and 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

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

Example. Let E be the elliptic curve of conductor 26 given by

$$E: \quad y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Its torsion subgroup is $\mathbb{Z}/7\mathbb{Z}$ and we have $\Delta(E) = -2^7 \cdot 13$. By Corollary 6, there are infinitely many negative fundamental discriminants D for which

$$rk(E(D), \mathbb{Q}) = 0 \quad \text{and} \quad \#Ш(E(D), \mathbb{Q}) \equiv 0 \pmod{7}.$$

Acknowledgements

The author thanks M. Papanikolas, D. Penniston and S. Wong for their helpful comments during preparation of this paper.

2. Preliminaries

The arguments in this paper depend heavily on the combinatorics of the half-integer weight and integer weight Hecke operators combined with the intrinsic properties of Galois representations associated to newforms (see [K, Mi] for essential facts concerning modular forms). We briefly recall the definition of Hecke operators. If k is a positive integer and χ is a Dirichlet character modulo M, then for every prime $p \nmid M$ the Hecke operator $T_p^{k,\chi}$ on $S_k(\Gamma_0(M), \chi)$ acts by sending the cusp form $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ to

$$f(z) \mid T_p^{k,\chi} := \sum_{n=1}^{\infty} (a_f(np) + \chi(p)p^{k-1}a_f(n/p))q^n. \tag{2.1}$$

Similarly, recall that if $p \nmid 4N$ is prime and χ is a Dirichlet character modulo $4N$, then the half-integer weight Hecke operator $T_k^{\chi}(p^2)$ on $S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$ is defined by sending a cusp form $h(z) = \sum_{n=1}^{\infty} a_h(n)q^n$ to

$$h(z) \mid T_k^{\chi}(p^2) := \sum_{n=1}^{\infty} \left(a_h(np^2) + \chi^{\star}(p)p^{k-1}\left(\frac{n}{p}\right)a_h(n) + \chi^{\star}(p^2)p^{2k-1}a_h(n/p^2) \right) q^n, \tag{2.2}$$

where $\chi^{\star}(p) := \chi(p)\left(\frac{-1}{p}\right)^k$.

We also require the following classical result on Galois representations associated to modular forms due to Deligne and Serre [D, D-S].

Theorem 2.1. *Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k(\Gamma_0(M), \chi)$ 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 χ. 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

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

Using this theorem we prove the following crucial theorem.

Theorem 2.2. *Let $f_1(z), f_2(z), \dots, f_y(z)$ be integer weight cusp forms where*

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

Suppose that the coefficients of all the $f_i(z)$ and the values of all the χ_i are in O_K, the ring of integers of some number field K. 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 there is a set of primes p with positive Frobenius density such that for every $1 \le i \le y$ we have

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

Proof. By the theory of newforms (a.k.a. primitive forms), each $f_i(z)$ may be expressed as

$$f_i(z) = \sum_{\delta \mid M_i} \sum_{s} \beta(i,s,\delta) h_{i,s}(\delta z) \tag{2.3}$$

where each $\beta(i,s,\delta)$ is algebraic and the inner sum above is over the newforms $h_{i,s}(z)$ with level dividing M_i/δ. For convenience, we denote the q-expansions of the $h_{i,s}(z)$ by

$$h_{i,s}(z) = \sum_{n=1}^{\infty} a_{i,s}(n)q^n. \tag{2.4}$$

Let K_1 be a finite extension of K which contains all the $\beta(i,s,\delta)$ and all the Fourier coefficients $a_{i,s}(n)$ of all the newforms $h_{i,s}(z)$. Let w be a place of K_1 over v and let e be its ramification index. Moreover, let O_w be the completion of O_{K_1} at w and let λ be its uniformizer.

For each $h_{i,s}(z)$ let $\rho_{i,s,w}$ be the representation described in Theorem 2.1. If E is defined by

$$E := \max_{\substack{i,s,\delta \\ \beta(i,s,\delta) \neq 0}} |\mathrm{ord}_w(\beta(i,s,\delta))|, \tag{2.5}$$

then consider the representation

$$\rho := \oplus_{i,s} \ \rho_{i,s,w} \pmod{\lambda^{E+je+1}}.$$

Since the image of ρ is finite, the Chebotarev Density Theorem implies that there is a set of primes p with positive Frobenius density which have the property that

$$\mathrm{Tr}(\rho_{i,s,w}(Frob(p))) \equiv a_{i,s}(p_0) \pmod{\lambda^{E+je+1}}$$

for all i and s. Since $a_{i,s}(p)$ is the eigenvalue of $h_{i,s}(z)$ for the Hecke operator $T_p^{k_i,\chi_i}$ for a prime $p \nmid \ell M_1 M_2 \cdots M_y$, it follows by (2.3-5) that

$$f_i(z) \mid T_p^{k_i,\chi_i} \equiv f_i(z) \mid T_{p_0}^{k_i,\chi_i} \pmod{\lambda^{je+1}}$$

for all i.

Q.E.D.

3. Fourier coefficients of half-integer weight cusp forms

In this section we prove a general nonvanishing theorem for the Fourier coefficients of most half-integer weight cusp forms. We begin with the following simple proposition.

Proposition 3.1. *Suppose that k is a positive integer and that $g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$ is an eigenform of the Hecke operators $T_k^{\chi}(p^2)$. If $p \nmid 4N$ is a prime and $\lambda(p)$ is the eigenvalue of $g(z)$ with respect to $T_k^{\chi}(p^2)$, then*

$$b(np^2) = \left(\lambda(p) - \chi^{\star}(p)p^{k-1}\left(\frac{n}{p}\right)\right) b(n) - \chi^{\star}(p^2)p^{2k-1}b(n/p^2).$$

Lemma 3.2. *Suppose that $g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$ is an eigenform of the Hecke operators $T_k^{\chi}(p^2)$ with eigenvalues $\lambda(p)$ where k is a positive integer. If $k = 1$, then make the further assumption that the image of $g(z)$ under the Shimura correspondence is a cusp form. Let $G(z) \in S_{k+1}(\Gamma_0(4N), \chi\chi_{-1}^{k+1})$ be the cusp form defined by*

$$G(z) = \sum_{n=1}^{\infty} b_g(n)q^n := g(z) \cdot \left(1 + 2\sum_{n=1}^{\infty} q^{n^2}\right).$$

Let K be a number field with the property that all the coefficients $b(n)$ and the values of χ are in O_K, the ring of integers of K. Let v be a place in O_K above 2. If there is a prime $p_0 \nmid 4N$ for which

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

then for every positive integer j there is a set of primes $S_{p_0,j}$ with positive Frobenius density which satisfies the following conditions.

(1) *If $p \in S_{p_0,j}$, then*
$$\mathrm{ord}_v(\lambda(p)) = \mathrm{ord}_v(\lambda(p_0)) = 0.$$

(2) *If $p \in S_{p_0,j}$ then*
$$\mathrm{ord}_v\left(G(z) \mid T_p^{k+1,\chi\chi_{-1}^{k+1}} - G(z) \mid T_{p_0}^{k+1,\chi\chi_{-1}^{k+1}}\right) > j.$$

Proof. If $k > 1$, then the image of $g(z)$ under the Shimura correspondence is a newform $f_g(z)$ of integer weight $2k$ and level dividing $4N$ with Nebentypus character χ^2 [Sh]. Moreover, the eigenvalues of this newform with respect to T_p^{2k,χ^2} are the eigenvalues $\lambda(p)$ for every prime $p \nmid 4N$. The same is true for those $g(z)$ with $k = 1$ whose image under the correspondence is a cusp form [Sh]. Therefore we may apply Theorem 2.1 to the eigenvalues $\lambda(p)$ for primes $p \nmid 4N$ viewed as the Fourier coefficients $a_{f_g}(p)$ of the newform $f_g(z)$. The conclusion now follows immediately from Theorem 2.2 for the forms $G(z)$ and $f_g(z)$.

Q.E.D.

We shall require the following Lemma.

Lemma 3.3. *Assume the notation and hypotheses from Lemma 3.2, and define s_0 by*

$$s_0 := \min\{\mathrm{ord}_v(b(n))\}.$$

Then the following are true.

(1) *An integer n has the property that $\mathrm{ord}_v(b_g(n)) = s_0$ if and only if $\mathrm{ord}_v(b(n)) = s_0$.*
(2) *Let n_0 be an integer for which $\mathrm{ord}_v(b(n_0)) = s_0$. If j is a positive integer and $p_1, p_2, \dots, p_{2j-1}, p_{2j} \in S_{p_0,s_0}$ are distinct primes not dividing n_0, then*

$$\mathrm{ord}_v(b(n_0 p_1 p_2 \cdots p_{2j-1} p_{2j})) = s_0.$$

Proof. By the definition of $G(z)$, it is easy to see that if n is a positive integer, then

$$b_g(n) = b(n) + 2\sum_{t=1}^{\infty} b(n - t^2).$$

Conclusion (1) follows easily from the definition of s_0 and v.

Suppose that m is a positive integer for which

$$\mathrm{ord}_v(b(m)) = s_0.$$

Let $q_1, q_2 \in S_{p_0,s_0}$ be distinct primes which are coprime to m. The coefficient of q^{mq_1}, by (2.1), in $G(z) \mid T_{q_1}^{k+1,\chi\chi_{-1}^{k+1}}$ is

$$\begin{aligned}
&= b_g(mq_1^2) + \chi(q_1)\chi_{-1}^{k+1}(q_1)q_1^k b_g(m) \\
&= \left(\lambda(q_1) - \chi^\star(q_1)q_1^{k-1}\left(\frac{m}{q_1}\right)\right) b_g(m) + \chi(q_1)\chi_{-1}^{k+1}(q_1)q_1^k b_g(m) \\
&= \lambda(q_1) b_g(m) + b_g(m)\chi^\star(q_1)q_1^{k-1}\left(\chi_{-1}(q_1)q_1 - \left(\frac{m}{q_1}\right)\right)
\end{aligned}$$

Since $\chi_{-1}(q_1)q_1 - \left(\frac{m}{q_1}\right) \equiv 0 \pmod 2$, by Lemma 3.2 we find that the coefficient of q^{mq_1} in $G(z) \mid T_{q_1}^{k+1,\chi\chi_{-1}^{k+1}}$ has ord_v equal to s_0.

By Lemma 3.2 (2), the coefficient of q^{mq_1} in $G(z) \mid T_{q_2}^{k,\chi\chi_{-1}^{k+1}}$ also has $\mathrm{ord}_v = s_0$ if $q_2 \in S_{p_0,s_0}$. This then implies that

$$\begin{aligned}
&b_g(mq_1q_2) + \chi(q_2)\chi_{-1}^{k+1}(q_2)q_2^k b_g(mq_1/q_2) \\
&= b_g(mq_1q_2)
\end{aligned}$$

has ord_v equal to s_0.

This shows, by (1), that if $\mathrm{ord}_v(b(m)) = s_0$ and $q_1, q_2 \in S_{p_0,s_0}$ are distinct odd primes which do not divide m, then

$$\mathrm{ord}_v(b(mq_1q_2)) = s_0. \tag{3.1}$$

Iterating (3.1) yields (2).

Q.E.D.

Now we briefly recall Waldspurger's theorem, which gives a formula for many of the central values $L(F \otimes \chi_D, k)$ in terms of the squares of the Fourier coefficients of cusp forms with half integer weight $k + \frac{1}{2}$ which are related to $F(z)$, or a twist of $F(z)$, by Shimura's correspondence [Sh]. For every D define D_0 by

$$D_0 := \begin{cases} |D| & \text{if } D \text{ is odd,} \\ |D|/4 & \text{if } D \text{ if even.} \end{cases} \tag{3.2}$$

The following is a convenient reformulation of Waldspurger's theorem.

Theorem 3.4. ([Th. 1, W1, §2 O-Sk]) *If $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(\Gamma_0(M), \chi_0)$ is an even weight newform and $\delta \in \{\pm 1\}$ 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 modulo $4N$, a non-zero complex number Ω_F and a non-zero 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

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

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

$$\lambda(p) = \chi^2(p)a(p),$$

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

We now prove the following technical theorem which immediately implies Theorem 1.

Theorem 3.5. *Assume the notation from Theorem 3.4. Let v be a place of K over 2 and let s_0 be the non-negative integer*

$$s_0 := \min\{\mathrm{ord}_v(b(n))\}.$$

Suppose there is a prime $p \nmid M$ for which $\mathrm{ord}_v(a(p)) = 0$. Then there is a set of primes S_F with positive Frobenius density with the property that for every positive integer j we have

$$L(F \otimes \chi_{\delta n_0 p_1 p_2 \cdots p_{2j}}, k) \neq 0$$

whenever n_0 is a square-free integer with $\mathrm{ord}_v(b_F(n_0)) = s_0$ and $p_1, p_2, \ldots, p_{2j} \in S_F$ are distinct primes not dividing n_0.

Proof of Theorem 3.5. We apply Lemma 3.3 to the eigenform $g_F(z)$ given in Theorem 3.4. Since $g_F(z)$ is an eigenform, by (2.2) there is a square-free integer n_0 coprime to $4N$ for which $\mathrm{ord}_v(b(n_0)) = s_0$. Theorem 1 now follows from Lemma 3.3 and Theorem 3.4.

Q.E.D.

Lemma 3.6. *Let T be a set of primes with Frobenius density $0 < \alpha < 1$. If $\mathbb{N}_T$ denotes the set*

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

then

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

Here μ denotes the usual Möbius function.

Proof. Generalizing an argument of Landau, Serre proved [Th. 2.8, S] that if $N_T(X)$ is defined by

$$N_T(X) := \{n \leq X \ : \ n = \prod_i p_i \text{ with } p_i \in T\},$$

then

$$\#N_T(X) = c_T \cdot \frac{X}{\log^{1-\alpha} X} + O\left(\frac{X}{\log^{2-\alpha} X}\right) \tag{3.3}$$

for some positive constant c_T. Therefore, we need to consider those n counted in (3.3) which are square-free and have an even number of prime factors. Now let $M_T(X)$ denote the set

$$M_T(X) := \{n \leq X \ : \ n \in N_T(X) \text{ square-free}\}.$$

It is easy to see that

$$\begin{aligned} \#M_T(X) &\geq \#N_T(X) - \sum_{\substack{p_i \leq \sqrt{X} \\ p_i \in T}} \#N_T(X/p_i^2) \\ &\geq \#N_T(X) - \sum_{\substack{p_i \leq \sqrt{X} \\ p_i \in T}} \frac{1}{p_i^2} \#N_T(X) \gg \#N_T(X). \end{aligned} \tag{3.4}$$

Define $\mathbb{N}_T^o(X)$ by

$$\mathbb{N}_T^o(X) := \#\{n \leq X \ : \ n \in M_T(X) \text{ with } \mu(n) = -1\}.$$

Obviously, we have that

$$\#M_T(X) = \#\mathbb{N}_T(X) + \#\mathbb{N}_T^o(X). \tag{3.5}$$

If $p_0 \in T$ is prime, then by multiplying elements in $\mathbb{N}_T^o(X/p_0)$ by p_0 we find that

$$\begin{aligned} \#\mathbb{N}_T(X) &\geq \#\mathbb{N}_T^o(X/p_0) - \#\{n \leq X \ : \ n \in \mathbb{N}_T^o(X/p_0) \text{ and } \gcd(n, p_0) = p_0\} \\ &\gg \#\mathbb{N}_T^o(X/p_0). \end{aligned} \tag{3.6}$$

So, if $\mathbb{N}_T(X) = o\left(\frac{X}{\log^{1-\alpha} X}\right)$, then by (3.5) and (3.6) we have that

$$M_T(X/p_0) = o\left(\frac{X}{\log^{1-\alpha} X}\right).$$

However, this contradicts (3.4), which asserts that

$$M_T(X/p_0) \gg \frac{X}{(\log X - \log p_0)^{1-\alpha}}.$$

Q.E.D.

Proof of Corollary 2. This result follows immediately by letting the set T in Lemma 3.6 be the set S_F in Theorem 1.

Q.E.D.

4. Applications to ranks of elliptic curves

We recall a celebrated result due to Kolyvagin [Kol] which depends on a nonvanishing theorem for modular L-functions which can be attributed to Bump, Friedberg and Hoffstein, Iwaniec, and Murty and Murty [B-F-H, I, M-M].

Theorem 4.1. *If $E/\mathbb{Q}$ is a modular elliptic curve for which $L(E,1) \neq 0$, then $rk(E,\mathbb{Q}) = 0$.*

Proof of Corollary 3. By the works of Wiles and Taylor, Diamond, Conrad, Diamond and Taylor, and Breuil, Conrad, Diamond and Taylor [W, T-W, Di, C-D-T, B-C-D-T], it is now known that every elliptic curve $E/\mathbb{Q}$ is modular. If E is an elliptic curve with conductor $N(E)$ and D is coprime to $N(E)$, then $L(E(D), s)$ is the D-quadratic twist of $L(E, s)$. These are simply quadratic twists of modular L-functions. The conclusion of Corollary 3 now follows immediately by Theorem 4.1, Theorem 1, and Corollary 2. We use the fact that $a_E(p)$ is even for all but finitely many primes p if and only if E has a rational point of order 2.

Q.E.D.

We recall the following well known proposition.

Proposition 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose that $S := \{m_1, m_2, \dots, m_t\}$ is a set of square-free pairwise coprime integers > 1 such that for each $1 \leq s \leq t$ and any $d_1, d_2, \dots, d_s \in S$ distinct we have*

$$rk(E(d_1 d_2 \cdots d_s), \mathbb{Q}) = 0.$$

Then for every integer $1 \leq s \leq t$ we have

$$rk(E, \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \dots, \sqrt{m_s})) = rk(E, \mathbb{Q}).$$

Proof of Theorem 4. This result follows from Theorem 1, Theorem 4.1 and Proposition 4.2.

Q.E.D.

5. Applications to Tate-Shafarevich groups of elliptic curves

In this section we prove Theorem 5 and give one numerical example. If E is an elliptic curve over $\mathbb{Q}$, then let $N(E)$ denote its conductor, $j(E)$ its j-invariant, and $\Delta(E)$ its discriminant. If p is prime, then let $S(E,\mathbb{Q})_p$ be its pth-Selmer group and let $Ш(E,\mathbb{Q})$ denote the Tate-Shafarevich group of E. We begin by recalling an important Theorem due to Frey [Fr] regarding the Selmer groups of quadratic twists of elliptic curves with a rational point of odd prime order ℓ (note: By a theorem of Mazur this forces $\ell = 3, 5$, or 7).

Theorem 5.1. *Let ℓ be an odd prime such that $E/\mathbb{Q}$ is an elliptic curve with good reduction at ℓ with a point of order ℓ. Define the set of primes $S(E,\ell)$ by*

$$S(E,\ell) := \{q \mid N(E) \ : \ q \neq 2, q \equiv -1 \pmod{\ell} \text{ and } \mathrm{ord}_q(\Delta(E)) \not\equiv 0 \pmod{\ell}\}.$$

Suppose that d is a negative square-free integer satisfying the following conditions:

(1) *We have $\gcd(d, \ell N(E)) = 1$ and $d \equiv 3 \pmod 4$.*

(2) *If* $\mathrm{ord}_\ell(j(E)) < 0$, *then* $\left(\frac{d}{\ell}\right) = -1$.
(3) *If* $q \mid N(E)$ *is prime but* $q \notin \{2, \ell\} \cup S(E, \ell)$ *then*

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

If $Cl(d)_\ell$ *denotes the* ℓ*-part of the ideal class group of* $\mathbb{Q}(\sqrt{d})$, *then*

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

Now we give the precise definition of an *excellent* elliptic curve.

Definition 5.2. *Let* $E/\mathbb{Q}$ *be an elliptic curve with a rational point of odd prime order* ℓ *that has good reduction at* ℓ. *Moreover, suppose that*

$$g_E(z) = \sum_{n=1}^{\infty} b_E(n) q^n \in S_{3/2}(\Gamma_0(4N), \chi)$$

is an eigenform, for some N, *satisfying the conclusion of Theorem 3.4 for the weight 2 newform*

$$F_E(z) = \sum_{n=1}^{\infty} a_E(n) q^n \in S_2(\Gamma_0(N(E)), \chi_0)$$

associated to E *with* $\delta = -1$. *Moreover, suppose that* v *is a place of* K *over 2 and that*

$$s_0 := \min\{\mathrm{ord}_v(b_E(n))\}.$$

We say that E *is excellent at* ℓ *if there is a negative square-free integer* d_E *which satisfies all of the following conditions:*

(1) *This integer* d_E *is coprime to* $\ell N(E)$ *and satisfies the congruence*

$$d_E \equiv 3 \pmod 4.$$

(2) *If* $\mathrm{ord}_\ell(j(E)) < 0$, *then* $\left(\frac{d_E}{\ell}\right) = -1$.
(3) *If* $q \mid N(E)$ *is prime but* $q \notin \{2, \ell\} \cup S(E, \ell)$, *then*

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

(4) *We have that*

$$\mathrm{ord}_v(b_E(|d_E|)) = s_0.$$

Remark. Condition (4) above is not as restrictive as it may appear. It is typical that a suitable modification of $g_E(z)$ satisfies it. Specifically, suppose that d_E has the property that $b_E(|d_E|) \neq 0$. By using combinations of twists and possibly twists of twists of $g_E(z)$, one may replace $g_E(z)$ by the cusp form

$$\tilde{g}_E(z) = \sum b_E(n)q^n$$

where the sum ranges over those positive integers $n \equiv |d_E| \pmod{(\mathbb{Q}_q^\times)^2}$ for each prime $q \mid N(E)$. It is now easy to see that $\tilde{g}_E(z)$ is non-zero and has a $\tilde{d}_E$ which satisfies (4).

Wong [Wo] has proved a nice theorem regarding the existence of quadratic fields whose ideal class groups contain elements of order ℓ with the additional property that all of the prime factors p of the discriminant of these fields have $Frob(p)$ lying in some prescribed conjugacy class in the Galois group of any fixed Galois extension $K/\mathbb{Q}$. A straightforward modification of Wong's arguments yields the following theorem.

Theorem 5.3. *Let $K/\mathbb{Q}$ be a finite Galois extension, and let c be a conjugacy class in* $\mathrm{Gal}(K/\mathbb{Q})$. *Moreover, let $S(K,c)$ denote the set of negative square-free integers which are divisible by only primes p which are unramified in $K/\mathbb{Q}$ and whose $Frob(p)$ lies in c. Let M_0 and M_1 be positive odd square-free coprime integers. For every odd prime ℓ there are infinitely many numbers $-d \in S(K,c)$ for which*

$$\begin{aligned}
&(i) \quad -dM_1 \equiv 3 \pmod 4,\\
&(ii) \quad \gcd(d, M_0) = 1,\\
&(iii) \quad \#Cl(-dM_1)_\ell \equiv 0 \pmod \ell,\\
&(iv) \quad \mu(d) = 1.
\end{aligned}$$

Before we sketch the proof of Theorem 5.3, we use it to prove Theorem 5.

Proof of Theorem 5. Since E is excellent at ℓ, we may apply Theorem 5.1 by hypothesis to $E(d_E)$. However, much more is true. Let S_E be the set of primes with positive density given in Theorem 3.5. By considering a sufficiently large Galois extension, one which contains the $\ell N(E)$'th roots of unity, we may assume that every prime $p \in S_E$ enjoys the following properties:

$$\left(\frac{p}{q}\right) = \left(\frac{p_0}{q}\right) \quad \text{for every prime } q \mid N(E), \tag{5.1}$$

$$\left(\frac{p}{\ell}\right) = \left(\frac{p_0}{\ell}\right). \tag{5.2}$$

By (5.1-2) and Theorem 5.1 we find that if j is a positive integer and $p_1, p_2, \dots, p_{2j} \in S_E$ are distinct primes not dividing d_E, then

$$L(E(d_E p_1 p_2 \cdots p_{2j}), 1) \neq 0, \tag{5.3}$$

$$\#Cl(d_E p_1 p_2 \cdots p_{2j})_\ell \mid \#S(E(d_E p_1 p_2 \cdots p_{2j})). \tag{5.4}$$

This follows from the fact that the conditions in Frey's theorem are quadratic residue conditions which d_E satisfies.

However, by Kolyvagin's theorem, (5.3) implies that $E(d_E p_1 p_2 \cdots p_{2j})$ has rank zero. Therefore, we find that if $p_1, p_2, \ldots, p_{2j} \in S_E$ are distinct primes which do not divide d_E, then

$$\#Cl(d_E p_1 p_2 \cdots p_{2j})_\ell \equiv 0 \pmod{\ell} \;\Rightarrow\; \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \subseteq Ш(E(d_E p_1 p_2 \cdots p_{2j})). \tag{5.5}$$

This follows from the fact that $\#Ш(E(d_E p_1 p_2 \cdots p_{2j}))$ is a square when finite, and the fact that $E(d_E p_1 p_2 \cdots p_{2j})$ does not have a $\mathbb{Q}$-rational point of order ℓ since a family of quadratic twists has at most one curve with a $\mathbb{Q}$-rational point of order ℓ. The theorem now follows from Theorem 5.3.

Q.E.D.

Now we briefly show how to modify Wong's argument to deduce Theorem 5.3.

Sketch of Proof of Theorem 5.3. Suppose that $p_0 \nmid M_1$ is a prime such that $Frob(p_0)$ lies in c. Now pick a sufficiently large odd prime g for which $\left(\frac{p_0}{g}\right) = -1$ and $\left(\frac{M_1}{g}\right) = \left(\frac{-1}{g}\right)$. Let K' be the extension of K defined by adjoining the gth roots of unity. Moreover, let c' be the conjugacy class of p_0 in $\mathrm{Gal}(K'/\mathbb{Q})$. It is easy to see that every prime p whose $Frob(p)$ is in c' has the property that its $Frob(p)$ in $\mathrm{Gal}(K/\mathbb{Q})$ is in c and has the additional property that

$$\left(\frac{p}{g}\right) = -1. \tag{5.6}$$

If $\Delta_{K'}$ is the discriminant of K', then define the positive integer C by

$$C := \prod_{\substack{q \mid M_0 \cdot \Delta_{K'} \text{ odd prime,} \\ q \nmid M_1}} q. \tag{5.7}$$

For positive integers G, define the set of integers $S(G)$ by

$$S(G) := \left\{ 0 < x \leq \frac{G}{g} \;:\; x \in 2\mathbb{Z},\ \gcd(x, g) = 1,\ x \not\equiv \pm 1 \pmod{q} \text{ for every prime } q \mid C \right\}. \tag{5.8}$$

Let δ be any fixed positive multiple of $\ell \prod_{q|C}(q-1)$. If λ is sufficiently large and $x \in S(g^{\delta\lambda})$ and satisfies the property that

$$d := g^{2\delta\lambda} - x^2 \tag{5.9}$$

is square-free, then we easily see that $d \equiv 1 \pmod 4$ and is a positive integer with no prime factors in common with C. By [Lemma 1, Wo], it follows that $\#Cl(-d)_\ell \equiv 0 \pmod{\ell}$.

Suppose that d is such a number which is a multiple of M_1 with the property that all the prime factors p of d/M_1 have $Frob(p)$ in c'. Since $\left(\frac{d/M_1}{g}\right) = 1$, by (5.9), the choice of g, and (5.6), there must be an even number of p. This yields (iv). Hence, any such d satisfies the conclusion of the theorem.

Therefore it suffices to show that one can construct infinitely many such d. If λ is sufficiently large, then there always is such a d, and the proof of this assertion follows virtually mutatis mutandis the proof of [Lemma 2, Wo]. Since selecting larger and larger $\lambda's$ uncovers quadratic fields whose class groups contains elements with orders that are larger and larger multiples of ℓ, the infinitude of the number of d is obvious.

Q.E.D.

Proof of Corollary 6. If E is excellent at ℓ, then the proof is complete. In view of the remark preceding Theorem 5.3, it remains to consider the case where δ, the sign of the functional equation of $L(E, s)$, is $+1$.

We recall a simple fact regarding the signs of functional equations of twists. If D is odd and coprime to $N(E)$, then the sign of the functional equation of $L(E(D), s)$ is $\delta\chi_D(-N(E))$. Let $d_+ \equiv 1 \pmod 4$ be a positive square-free integer for which the sign of the functional equation of $L(E(d_+), s)$ is -1 which also satisfies conditions (2) and (3) for d_E in Definition 5.2. This can be done since conditions (2) and (3) impose no restriction on $\left(\frac{d_+}{p_0}\right)$. It is now simple to modify the proof of Theorem 5 by using the weight 3/2 cusp form associated to $E(d_+)$ by Theorem 3.4.

Q.E.D.

References

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

[B-C-D-T] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$, preprint.

[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.

[C-D-T] B. Conrad, F. Diamond and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), 521-567.

[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.

[Di] F. Diamond, *On deformation rings and Hecke rings*, Annals of Math. **144** (1996), 137-166.

[Du] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris, sér. I **t. 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. **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.

[K] N. Koblitz, *Introduction to elliptic curves and modular forms*, vol. GTM 97, Springer-Verlag, New York, 1984.

[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.

[Mi] T. Miyake, *Modular forms*, Springer-Verlag, New York, 1989.

[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-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.

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, vol. GTM 106, Springer Verlag, New York, 1986.

[T-W] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553-572.

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

[W1] J.-L.Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141** (1995), 443-551.

[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