INDIVISIBILITY OF CLASS NUMBERS OF IMAGINARY QUADRATIC FIELDS AND ORDERS OF TATE-SHAFAREVICH GROUPS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

Winfried Kohnen and Ken Ono

1. Introduction and Statement of Results

Since Gauss, ideal class groups of imaginary quadratic fields have been the focus of many investigations, and recently there have been many investigations regarding Tate-Shafarevich groups of elliptic curves. In both cases the literature is quite extensive, but little is known.

Throughout D will denote a fundamental discriminant of a quadratic field. Let $CL(D)$ denote the class group of $\mathbb{Q}(\sqrt{D})$, and let $h(D)$ denote its order, i.e. the usual class number of primitive positive binary quadratic forms with discriminant D.

One of the main problems deals with the structure of $CL(D)$, and so one naturally studies the divisibility of $h(D)$ by primes. Here we consider imaginary quadratic fields. Gauss' genus theory precisely determines the parity of $h(D)$, but the divisibility of $h(D)$ by odd primes ℓ is much less well understood. In view of these difficulties, Cohen and Lenstra [C-L] gave heuristics describing the "expected" behavior of $CL(D)$, and in particular they predicted that the probability that $\ell \nmid h(D)$ is

$$\prod_{k=1}^{\infty}(1-\ell^{-k}) = 1 - \frac{1}{\ell} - \frac{1}{\ell^2} + \frac{1}{\ell^5} + \cdots .$$

1991 *Mathematics Subject Classification.* Primary 11E41, 11F33; Secondary 11E25, 11G40.

Key words and phrases. class numbers and Tate-Shafarevich groups of elliptic curves.

The second author is supported by NSF grant DMS-9508976 and NSA grant MSPR-97Y012, and the first author thanks the Department of Mathematics at Penn State where his research was supported by the Shapiro fund.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Although extensive numerical evidence lends credence to these heuristics, little has been proved apart from the works of Davenport and Heilbronn [D-H] when $\ell = 3$. They proved that if $\epsilon > 0$, then for sufficiently large $X > 0$

$$\frac{\#\{-X < D < 0 \mid h(D) \not\equiv 0 \pmod 3\}}{\#\{-X < D < 0\}} \geq \frac{1}{2} - \epsilon.$$

Ankeny and Chowla, Humbert, and Nagell proved that if ℓ is an odd prime, then there are infinitely many $D < 0$ for which $h(D) \equiv 0 \pmod{\ell}$, and recently M. R. Murty [M] extended these arguments and obtained the first nontrivial estimate for the number of such D. These results employ the useful fact that one can construct binary quadratic forms with prescribed order.

For the complementary question, Hartung [Ha] proved that there are infinitely many D for which $h(D) \not\equiv 0 \pmod 3$, and he noticed that his method works for every prime ℓ. More recent works by Bruinier [B], Horie and Onishi [Ho1, Ho2, Ho-On], Jochnowitz [J], and Ono and Skinner [O-S] address various refinements and generalizations.

We go a step further by obtaining an estimate. This estimate is obtained from a more general result which is proved in §2 (see Theorem 3).

Theorem 1. *If $\ell > 3$ is prime and $\epsilon > 0$, then for all sufficiently large $X > 0$*

$$\#\{-X < D < 0 \mid h(D) \not\equiv 0 \pmod{\ell}\} \;\geq\; \left(\frac{2(\ell-2)}{\sqrt{3}(\ell-1)} - \epsilon\right)\frac{\sqrt{X}}{\log X}.$$

Similar questions are of interest for Tate-Shafarevich groups $Ш(E)$ of elliptic curves $E/\mathbb{Q}$. Let E be an elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation

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

where a, b and c are integers. Moreover, let $N(E)$ denote the conductor of E, and let $rk(E)$ denote its rank. If d is a non-zero integer, then let $E(d)$ denote the d-quadratic twist of E

$$E(d): \quad y^2 = x^3 + adx^2 + bd^2x + cd^3.$$

Let $Ш(E(d))$ denote the Tate-Shafarevich group of $E(d)$, and let $rk(E(d))$ denote the rank of its Mordell-Weil group. If ℓ is an odd prime, then it is widely believed that a positive proportion of square-free d have the property that $\ell \nmid \#Ш(E(d))$. By works of Bruinier [B], Jochnowitz [J], and Ono and Skinner [O-S], for modular E it is known that for almost every prime ℓ there are indeed infinitely many square-free d for which $\#Ш(E(d)) \not\equiv 0 \pmod{\ell}$. These results have important implications for rank 1 elliptic curves (see [O-S], [K2]).

In §3 we prove a general result (see Theorem 6 and Corollary 7) that implies the following result.

Theorem 2. *If $E/\mathbb{Q}$ has complex multiplication, then for every prime $\ell \gg_E 0$*

$$\#\{0<|D|<X \mid rk(E(D))=0 \;\; and \;\; \ell \nmid \#\text{Ш}(E(D))\} \gg_{E,\ell} \frac{\sqrt{X}}{\log X}.$$

All of these results are obtained by combining a theorem of Sturm on modular forms 'mod p' and classical facts regarding the behavior of the operators U_p and V_p on spaces of half-integral weight modular forms.

2. The Class number case.

We prove Theorem 1 by bounding the largest fundamental discriminant D that is a multiple of p for which $\ell \nmid h(D)$. This is the content of the following theorem.

Theorem 3. *Let $\ell > 3$ be prime, and p any prime for which $p \not\equiv \left(\frac{-4}{p}\right) \pmod{\ell}$. Then there exists an integer $1 \leq d_p \leq \frac{3}{4}(p+1)$ for which $D := -pd_p$ or $-4pd_p$ is a fundamental discriminant and $h(D) \not\equiv 0 \pmod{\ell}$.*

Proof of Theorem 3. Without loss of generality we may assume that $p > 3$. Let $\theta(z) := \sum_{n\in\mathbb{Z}} q^{n^2}$ (throughout $q := e^{2\pi i z}$) be the classical theta function, and define $r(n)$ by

$$\sum_{n=0}^{\infty} r(n)q^n := \theta^3(z) = 1 + 6q + 12q^2 + 8q^3 + 6q^4 + 24q^5 + \dots.$$

Gauss proved that

$$r(n) = \begin{cases} 12H(4n) & \text{if } n \equiv 1,2 \pmod{4}, \\ 24H(n) & \text{if } n \equiv 3 \pmod{8}, \\ r(n/4) & \text{if } n \equiv 0 \pmod{4}, \\ 0 & \text{if } n \equiv 7 \pmod{8}. \end{cases} \tag{1}$$

Here if $N \equiv 0,3 \pmod{4}$, then $H(N)$ denotes the Hurwitz-Kronecker class number, i.e. the class number of quadratic forms of discriminant $-N$ where each class C is counted with multiplicity $1/\text{Aut}(C)$. If $-N = Df^2$ where D is a negative fundamental discriminant, then $H(N)$ is related to usual class numbers by the formula [p. 273, C]:

$$H(N) = \frac{h(D)}{w(D)} \sum_{d|f} \mu(d) \left(\frac{D}{d}\right) \sigma_1(f/d). \tag{2}$$

Here $w(D)$ is half the number of units in $\mathbb{Q}(\sqrt{D})$, and $\sigma_s(n)$ denotes the sum of the s^{th} powers of the positive divisors of n.

Define $(U_p\theta^3)(z)$ and $(V_p\theta^3)(z)$ in the usual way, i.e.

$$(U_p\theta^3)(z) := \sum_{n\geq 0} r(pn)q^n = 1 + \sum_{n\geq 1} r(pn)q^n, \tag{3a}$$

$$(V_p\theta^3)(z) := \theta^3(pz) = \sum_{n\geq 0} r(n)q^{pn} = 1 + \sum_{n\geq 1} r(n)q^{pn}. \tag{3b}$$

Both $U_p\theta^3$ and $V_p\theta^3$ are forms of weight 3/2 on $\Gamma_0(4p)$ with character $\left(\frac{4p}{\bullet}\right)$ [Prop. 1.3, Sh].

For $k \in \frac{1}{2}\mathbb{Z}$ and $N \in \mathbb{N}$ (with $4|N$ if $k \notin \mathbb{Z}$) let $M_k(N,\chi)$ denote the space of modular forms of weight k on $\Gamma_0(N)$ with Nebentypus character χ (see [Sh] for definitions). If $g = \sum_{n=0}^{\infty} a(n)q^n$ is a formal power series with integer coefficients, then define $\mathrm{ord}_\ell(g)$ by

$$\mathrm{ord}_\ell(g) := \min\{n \mid a(n) \not\equiv 0 \pmod{\ell}\}.$$

By a theorem of Sturm [Th. 1, St], if $g \in M_k(N,\chi)$ has integer coefficients and

$$\mathrm{ord}_\ell(g) > \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)],$$

then $g \equiv 0 \pmod{\ell}$, i.e. $a(n) \equiv 0 \pmod{\ell}$ for all n. He proved this for integral k and trivial χ, but the general case obviously follows by taking an appropriate power of g.

It is well known that $[\Gamma_0(1) : \Gamma_0(4p)] = 6(p+1)$, hence $\kappa(p) := \frac{3}{4}(p+1)$ is the relevant Sturm bound for forms in $M_{3/2}\left(4p, \left(\frac{4p}{\bullet}\right)\right)$. If $p > 3$, then $\kappa(p) < p$. Moreover, the reduction of $V_p\theta^3$ is

$$V_p\theta^3 \equiv 1 + 6q^p + \dots \pmod{\ell}.$$

Now we claim that $U_p\theta^3 \not\equiv V_p\theta^3$ when $p \not\equiv \left(\frac{-4}{p}\right) \pmod{\ell}$. To see this, it is sufficient to show that the coefficients of q^p in $U_p\theta^3$ and $V_p\theta^3$ are not congruent modulo ℓ, i.e. $r(p^2) \not\equiv 6 \pmod{\ell}$. By (1) and (2) we know that

$$r(p^2) = 12H(4p^2) = 6\left(p + 1 - \left(\frac{-4}{p}\right)\right),$$

and the claim follows. Therefore there exists some $1 \leq n_p \leq \kappa(p)$ for which $\ell \nmid r(pn_p)$. By (1) and (2) again, the result follows.

Q.E.D.

Deduction of Theorem 1 from Theorem 3. Let $p_1 < p_2 < \ldots$ be the primes in increasing order. If p_i and p_j are distinct primes for which $p_i \not\equiv \left(\frac{-4}{p_i}\right) \pmod{\ell}$ and $p_j \not\equiv \left(\frac{-4}{p_j}\right)$, then in the notation from the proof of the theorem

$$p_i n_{p_i} \neq p_j n_{p_j}.$$

If D_i and D_j are the negative fundamental discriminants associated by (1) and (2), then $D_i \neq D_j$ since $n_{p_i} \leq \frac{3}{4}(p_i + 1) < p_i$ and $n_{p_j} \leq \frac{3}{4}(p_j + 1) < p_j$. Moreover, it is obvious that $D_i \geq -3p_i(p_i + 1)$. Since there are only two arithmetic progressions of primes $\pmod{4\ell}$ that do not satisfy the given condition, the result now follows by Dirichlet's theorem on primes in arithmetic progressions.

Q.E.D.

3. The Tate-Shafarevich case

In this section we shall prove Theorem 2. As in Theorem 3, we will depend heavily on Sturm's theorem. First we give a few preliminaries and fix notation. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by K whose conductor is $N(E)$, and let $L(E,s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be its Hasse-Weil L-function. Let $F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_2(N(E))$ be the cusp form associated to E. If $D \neq 0$ is a fundamental discriminant, then let χ_D denote the Kronecker character for the field $\mathbb{Q}(\sqrt{D})$, and let $E(D)$ denote the D-quadratic twist of E.

For notational convenience, if D is a fundamental discriminant of a quadratic number field, then define D_0 by

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

Let $\delta \in \{\pm 1\}$, and let Ω_E denote the real period of $E(\delta)$. Since E is a modular elliptic curve, it follows from the theory of modular symbols that

$$L^{alg}(E(D),1) := \frac{L(E(D),1)\sqrt{D_0}}{\Omega_E} \in \mathbb{Q} \tag{4}$$

for each fundamental discriminant D with $\delta D > 0$ and $(D_0, N(E(\delta))) = 1$. However since F is a cusp form associated to a Hecke Grössencharacter by K (see [§2.8, Cr], [M-T-T], [Theorem 3.5.4, G-S]), there is a non-zero complex period Ω_F for which

$$\frac{L(E(D),1)\sqrt{D_0}}{\Omega_F} \in \begin{cases} \frac{1}{2}\mathbb{Z} & \text{if } K \neq \mathbb{Q}(i) \text{ or } \mathbb{Q}(\sqrt{-3}), \\ \frac{1}{2\Delta_K}\mathbb{Z} & \text{otherwise} \end{cases} \tag{5}$$

for every discriminant D with $\delta D > 0$ and $(D_0, N(E(\delta))) = 1$. Here Δ_K denotes the discriminant of K.

Much more is conjectured to be true. The Birch and Swinnerton-Dyer Conjecture states that if $L(E(D),1) \neq 0$, then

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

where $\Omega_{E(D)}$ is the real period of $E(D)$, $Tam(E(D))$ is the Tamagawa factor, and $E(D)_{tor}$ is the torsion subgroup of $E(D)$. Since E has complex multiplication, there are no primes larger than 3 that can divide $\#E(D)_{tor}$. Moreover, if ℓ is an odd prime, then $\left|\frac{\Omega_{E(D)}\sqrt{D_0}}{\Omega_E}\right|_\ell = 1$. Here $|\cdot|_\ell$ denotes the usual multiplicative ℓ-adic valuation.

Waldspurger proved a fundamental theorem [Th. 1, Wal] relating $L(E(D),1)$ to the Fourier coefficients of weight $3/2$ cusp forms g. For our purposes we require the following result which follows from his work.

Theorem 4. *If $E/\mathbb{Q}$ is an elliptic curve with complex multiplication, then there is a $\delta(E) \in \{\pm 1\}$, 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 fundamental discriminant D with $\delta(E)D > 0$

$$b(D_0)^2 = \begin{cases} \epsilon_D \frac{L(E(D),1)\sqrt{D_0}}{\Omega_F} & \text{if } (D_0, N_W) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Here the ϵ_D and the coefficients $b(D_0)$ are algebraic integers in some fixed number field.

Proof of Theorem 4. Waldspurger's theorem [Th. 1, Wal] is quite general, but at first glance two technical hypotheses intervene. Let $G \in S_2(M)$ be a newform and let ρ_0 be the associated automorphic representation, and let S denote the set of primes for which $\rho_{0,p}$, the local component of ρ_0, does not belong to the principal irreducible series. Moreover if $p \notin S$, then let $\mu_{1,p}$ and $\mu_{2,p}$ denote the two characters of $\mathbb{Q}_p^\times$ such that $\rho_{0,p} \sim \pi(\mu_{1,p}, \mu_{2,p})$. For definitions see [§III, Wal]. In his notation, these two hypotheses are

H1. For every prime $p \notin S$ we have the equality $\mu_{1,p}(-1) = \mu_{2,p}(-1)$.

H2. One of the following holds:

- *(i)* $\rho_{0,2}$ is not supercuspidal,
- *(ii)* The conductor of χ is a multiple of 16.
- *(iii)* M is a multiple of 16.

His formulae hold for every G that satisfies H1 and H2.

To complete the proof of this theorem it suffices to show that there is a twist F_ψ satisfying H1 and H2. One can construct such a character ψ as follows. Choose ψ to be a product of an even character of conductor a large power of 2 and odd characters of conductor either ℓ or ℓ^2 for each prime ℓ for which $\epsilon_\ell(F) = -1$ (ℓ can equal 2). Here $\epsilon_\ell(F)$ is the local root number at ℓ. That F_ψ satisfies H1 is a consequence of the characterization of local root numbers. The large power of 2 dividing the conductor of ψ ensures that F_ψ satisfies H2. Now put

$$\delta(E) := -\psi(-1) \quad \text{and} \quad \chi := \begin{cases} \psi\left(\frac{-1}{\cdot}\right) & \text{if } \psi(-1) = -1, \\ \psi & \text{otherwise,} \end{cases}$$

and apply [Th. 1, Wal] to the form F_ψ and character χ (which is even by construction and satisfies $\chi^2 = \psi^2$). The existence of an N_W and g can be seen by inspecting the explicit formulae given for the functions $c_p(n)$ (notation as in [I, 4, Wal]). Moreover, N_W can be chosen so that it is divisible by f_χ, the conductor of χ. This is just a straight-forward case-by-case analysis.

Now we can verify indeed that there exists a normalization of g such that the coefficients $b(D_0)$ are algebraic integers, and that there are algebraic integers ϵ_D for which the claimed identity is true. We will choose the ϵ_D's to be an appropriate fixed multiple of the root number $W := W(\chi^{-1}\chi_{-4}\chi_D)$ if $\delta(E) = 1$ or $W := W(\chi^{-1}\chi_D)$ if $\delta(E) = -1$. It is a simple consequence of the definition of the root numbers and the assumption that $(D_0, N_W) = 1$ that $W \cdot \sqrt{f_\chi}$ is an algebraic integer lying in a fixed finite extension of $\mathbb{Q}$. Hence by (5) there is a positive integer α dividing $2\Delta_K$ for which $\epsilon_D := \alpha \cdot W \cdot \sqrt{f_\chi}$ and $b(D_0)$ are always algebraic integers. Notice that ϵ_D does not depend on the coefficients of g.

Q.E.D.

Using the notation in Theorem 4, if D is a fundamental discriminant coprime to N_W for which $\delta(E)D > 0$, then define $L_W^{alg}(E(D), 1)$ by

$$L_W^{alg}(E(D), 1) := b(D_0)^2. \tag{6}$$

For such D it is easy to see that

$$L_W^{alg}(E(D), 1) = \epsilon_D \cdot \frac{\Omega_E}{\Omega_F} \cdot L^{alg}(E(D), 1).$$

By Theorem 4 and the discussion immediately following (5), we obtain the following.

Corollary 5. *Suppose that ℓ is an odd prime for which $|\Omega_E/\Omega_F|_\ell = 1$. If D is a fundamental discriminant for which $\delta(E)D > 0, (D_0, N_W) = 1$, and*

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

then

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

Using the notation above we obtain the following theorem.

Theorem 6. *Suppose that $E/\mathbb{Q}$ has complex multiplication, and let $\ell \geq 5$ be any prime for which $|\Omega_E/\Omega_F|_\ell = 1$ and $\ell \nmid N_W$. If there is a fundamental discriminant D for which*

$$(i)\ \delta(E)D > 0,$$
$$(ii)\ (D_0, N_W) = 1,$$
$$(iii)\ |L_W^{alg}(E(D), 1)|_\ell = 1,$$

then there is an arithmetic progression $r \pmod t$ with $(r, t) = 1$, and a constant $k(E) > 0$ such that for every prime $p \equiv r \pmod t$ there is a square-free integer $1 \leq |n_p| \leq k(E)p$ satisfying

$$(i)\ \delta(E)n_p > 0 \text{ and } (n_p, p) = 1,$$
$$(ii)\ rk(E(pn_p)) = 0,$$
$$(iii)\ \#\text{Ш}(E(pn_p)) \not\equiv 0 \pmod{\ell}.$$

Corollary 7. *Suppose that $E/\mathbb{Q}$ has complex multiplication, and let $\ell \geq 5$ be a prime for which $|\Omega_E/\Omega_F|_\ell = 1$ and $\ell \nmid N_W$. If there is a fundamental discriminant D with $\delta(E)D > 0, (D_0, N_W) = 1$, and $|L_W^{alg}(E(D), 1)|_\ell = 1$, then the number of square-free $|d| < X$ for which*

$$(i)\ \delta(E)d > 0 \text{ and } (d, N_W) = 1,$$
$$(ii)\ rk(E(d)) = 0,$$
$$(iii)\ \#\text{Ш}(E(d)) \not\equiv 0 \pmod{\ell}$$

is $\gg \sqrt{X}/\log X$.

Proof of Theorem 6. Let $g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{3/2}(N_W, \chi)$ be the eigenform given in Theorem 4. Under the Shimura correspondence, this form maps to a twist (possibly trivial) of $F(z)$.

If p is prime, then define $(U_p g)(z), (V_p g)(z) \in S_{3/2}\left(N_W p, \left(\frac{4p}{\bullet}\right) \cdot \chi\right)$ by

$$(U_p g)(z) = \sum_{n=1}^{\infty} u_p(n) q^n := \sum_{n=1}^{\infty} b(pn) q^n,$$
$$(V_p g)(z) = \sum_{n=1}^{\infty} v_p(n) q^n := \sum_{n=1}^{\infty} b(n) q^{pn}.$$

Thus for every positive integer n

(7a) $$u_p(n) = b(pn),$$

(7b) $$v_p(n) = \begin{cases} 0 & \text{if } n \not\equiv 0 \pmod{p}, \\ b(n/p) & \text{otherwise.} \end{cases}$$

If $p \equiv 3 \pmod 4$ is a prime for which $\left(\frac{\Delta_K}{p}\right) = -1$ and $(p, N_W) = 1$, then the eigenvalue of $g(z)$ with respect to $T(p^2)$ is zero. Therefore for such p we find that

(8) $$b(p^2 n) = \chi(p) \left(\frac{n}{p}\right) b(n) - p\chi(p^2) b(n/p^2).$$

Therefore by (7a-b), and (8) it is easy to see that if $p \equiv 3 \pmod 4$ is a prime for which $\left(\frac{\Delta_K}{p}\right) = -1$, $(p, N_W) = 1$, and $p^2 \nmid n$, then

(9) $$u_p(pn) = \chi(p) \left(\frac{n}{p}\right) v_p(pn).$$

Let $p \equiv 3 \pmod 4$ be a sufficiently large prime for which

(10a) $$(p, N_W) = 1,$$

(10b) $$\left(\frac{\Delta_K}{p}\right) = -1,$$

(10c) $$\left(\frac{n}{p}\right) = 1 \quad \text{for all } 1 \leq n \leq \kappa(E) := \frac{N_W[\Gamma_0(1) : \Gamma_0(N_W)]}{8} + 1.$$

By (9), every sufficiently large prime p satisfying (10a-c) has the property that

(11) $$u_p(pn) = \chi(p) v_p(pn) \quad \text{for every } 1 \leq n \leq \kappa(E).$$

Now let d be a square-free integer for which $|b(d)|_\ell = 1$. By (7a-b) and (8), one finds that if p is a sufficiently large prime satisfying (10a-c), then

$$v_p(dp^3) = \chi(p)\left(\frac{d}{p}\right)b(d) \quad \text{and} \quad u_p(dp^3) = -p\chi(p^2)b(d).$$

Therefore if $\left|\chi(p^2)p - \chi(p)\left(\frac{d}{p}\right)\right|_\ell = 1$, then $\mathrm{ord}_\ell(U_p g - \chi(p)V_p g) < \infty$.

However by Sturm's theorem, if $g_1(z), g_2(z) \in S_{3/2}\left(Np, \left(\frac{4p}{\bullet}\right)\cdot\chi\right)$ are two forms with algebraic integer coefficients and $p \gg 0$ prime, then $\mathrm{ord}_\ell(g_1 - g_2) = \infty$ if

$$\mathrm{ord}_\ell(g_1 - g_2) > p\kappa(E). \tag{12}$$

If $\ell \geq 5$ and $\ell \nmid N_W$, then there is an arithmetic progression $r \pmod t$ with $(r,t) = 1$ and $f_\chi \mid t$ for which every prime $p \equiv r \pmod t$ satisfies (10a-c) and has the property that $\left|\chi(p^2)p - \chi(p)\left(\frac{d}{p}\right)\right|_\ell = 1$. If $p \equiv r \pmod t$ is a sufficiently large prime, then by (11) we see that

$$u_p(pn) = \chi(r)v_p(pn) \quad \text{for every} \;\; pn \leq p\kappa(E).$$

However it is also true that $\mathrm{ord}_\ell(U_p g - \chi(r)V_p g) < \infty$. Hence by Sturm's theorem there exists an integer $m \leq \kappa(E)$ coprime to p for which $|b(mp)|_\ell = 1$.

Therefore by Corollary 5 and the multiplicative properties of the coefficients of half-integral weight eigenforms, there is a fundamental discriminant D that is a multiple of p with $\delta(E)D > 0$, $D_0 \leq \kappa(E)p$, and $|L^{alg}(E(D),1)|_\ell = 1$. By a theorem of Rubin [Th. A, R], since $\ell \nmid O_K^\times$ we find that $\#Ш(E(D)) \not\equiv 0 \pmod \ell$. In addition, it is clear that $L(E(D),1) \neq 0$, and so by a theorem of Coates and Wiles [Th. 1, Co-W] we find that $rk(E(D)) = 0$.

Q.E.D.

Proof of Corollary 7. In the notation from Theorem 6, if $p \equiv r \pmod t$ is prime, then there exists an integer $1 \leq |n_p| \leq k(E)p$ with $\delta(E)n_p > 0$ for which $E(pn_p)$ has the desired properties. Let p_i denote these primes in increasing order, and D_i 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 k, j, and l since $|D_i| < k(E)p_i^2$. The result now follows from Dirichlet's theorem on primes in arithmetic progressions.

Q.E.D.

Example. Using Tunnell's work [T], we consider the congruent number elliptic curve

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

Let $p \equiv 3 \pmod 4$ be a prime greater than 3 for which

$$\left(\frac{3}{p}\right) = \left(\frac{11}{p}\right) = \left(\frac{17}{p}\right) = \left(\frac{19}{p}\right) = 1.$$

If ℓ is an odd prime for which $p \not\equiv -1 \pmod{\ell}$, then there exists a square-free integer $1 \leq n_p \leq 24(p+1)$ for which

$$\begin{aligned} &(i)\ (n_p, 2p) = 1,\\ &(ii)\ rk(E(pn_p)) = 0,\\ &(iii)\ \#\text{Ш}(E(pn_p)) \not\equiv 0 \pmod{\ell}. \end{aligned}$$

If $\ell \neq 3, 11, 17, 19$ is an odd prime and $\epsilon > 0$, then for $X \gg 0$

$$\#\left\{0 < D < X \mid rk(E(D)) = 0 \text{ and } \ell \nmid \#\text{Ш}(E(D))\right\} \geq \left(\frac{\ell - 2}{64\sqrt{6}(\ell - 1)} - \epsilon\right)\frac{\sqrt{X}}{\log X}.$$

References

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

[Co-W] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223-251.

[C] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. **217** (1975), 271-285.

[C–L] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983, Springer Lect. Notes **1068** (1984), 33-62.

[Cr] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992.

[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.

[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.

[Ho1] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. **88** (1987), 31-38.

[Ho2] K. Horie, *Trace formulae and imaginary quadratic fields*, Math. Ann. **288** (1990), 605-612.

[Ho–On] K. Horie and Y. Onishi, *The existence of certain infinite families of imaginary quadratic fields*, J. Reine und ange. Math. **390** (1988), 97-133.

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

[K] 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).

[K2] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Progress in Math. 87, ed. P. Cartier et. al. (1990), 435-483.

[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.

[Ha] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Th. **6** (1974), 276-278.

[M] M. R. Murty, *in preparation.*

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

[R] K. Rubin, *Tate-Shafarevich groups and* $L-$*functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560.

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

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

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

[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.

Mathematisches Institut, Universität Heidelberg, INF 288, D-69120 Heidelberg, Germany
E-mail address: winfried@mathi.uni-heidelberg.de

Dept. of Math., Penn State University, University Park, Pennsylvania 16802, USA.
E-mail address: ono@math.psu.edu