Journal of the London Mathematical Society Advance Access published June 7, 2012

J. London Math. Soc. Page 1 of 19
doi:10.1112/jlms/jds018

Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves

Jack Fearnley, Hershy Kisilevsky and Masato Kuwata

Abstract

Let $L(E/\mathbb{Q}, s)$ be the L-function of an elliptic curve E defined over the rational field $\mathbb{Q}$. We examine the vanishing and non-vanishing of the central values $L(E, 1, \chi)$ of the twisted L-function as χ ranges over Dirichlet characters of a given order.

1. *Introduction*

Let E be an elliptic curve defined over the field $\mathbb{Q}$. Denote by

$$L(E/\mathbb{Q}, s) = L(E, s) = \sum_{n\geqslant 1} a_n n^{-s}$$

its L-function.

By the proof [4, 35] of the modularity of elliptic curves over $\mathbb{Q}$, we know that $L(E, s)$ has an analytic continuation for all $s \in \mathbb{C}$, and satisfies the functional equation

$$\Lambda(E, s) = w_E \Lambda(E, 2 - s),$$

where $\Lambda(E, s) = (\sqrt{N_E}/2\pi)^s \Gamma(s) L(E, s)$, N_E is the conductor of $E/\mathbb{Q}$, and $w_E = \pm 1$.

For a primitive Dirichlet character χ of conductor $\mathfrak{f}_\chi$, the *twist* of $L(E, s)$ by χ is

$$L(E, s, \chi) = \sum_{n\geqslant 1} \chi(n) a_n n^{-s}.$$

Then we also know that the L-function, $L(E, s, \chi)$, has an analytic continuation and, if $\mathfrak{f}_\chi$ is coprime to N_E, satisfies the functional equation

$$\Lambda(E, s, \chi) = w_E \chi(N_E) \tau(\chi)^2 \mathfrak{f}_\chi^{-1} \Lambda(E, 2 - s, \bar{\chi}),$$

where $\Lambda(E, s, \chi) = (\mathfrak{f}_\chi \sqrt{N_E}/2\pi)^s \Gamma(s) L(E, s, \chi)$ and $\tau(\chi)$ is the Gauss sum

$$\tau(\chi) = \sum_{c=0}^{\mathfrak{f}_\chi - 1} \chi(c) \exp(2\pi i c/\mathfrak{f}_\chi).$$

We consider the question of the vanishing or non-vanishing of $L(E, s, \chi)$ at $s = 1$ as χ ranges over sets of Dirichlet characters of fixed order. For integers $n \geqslant 1$, let $\mathcal{X}(n)$ denote the set of primitive Dirichlet characters of order exactly equal to n, that is,

$$\mathcal{X}(n) = \{\chi | \chi^n = \chi_0 \text{ and } \chi^d \neq \chi_0 \text{ for } d < n\},$$

where χ_0 is the trivial character.

Given n a positive integer and $X > 0$, we consider

$$\mathfrak{F}_E(n, X) = \mathfrak{F}_E^1(n, X) = \#\{\chi \in \mathcal{X}(n) \mid \mathfrak{f}_\chi \leqslant X \text{ and } L(E, 1, \chi) = 0\},$$

Received 6 November 2007; revised 2 February 2012.

2010 *Mathematics Subject Classification* 11G05, 14G05 (primary), 11G40, 14G10, 14G25, 14J28 (secondary).

This work was supported in part by grants from NSERC and FCAR.

or more generally

$$\mathfrak{F}_E^r(n,X) = \#\{\chi \in \mathcal{X}(n) \mid \mathfrak{f}_\chi \leqslant X \text{ and } \mathrm{ord}_{s=1} L(E,s,\chi) \geqslant r\}.$$

These functions have been extensively studied in the case that $n = 2$, and there are many results and conjectures that describe $\mathfrak{F}_E^r(2,X)$ as $X \to \infty$. Some of these will be reviewed in § 2.

Given a Dirichlet character χ, let K_χ be the cyclic extension of $\mathbb{Q}$ (of conductor $\mathfrak{f}_\chi$) which corresponds to χ. We write $K_\chi = K$ when the character χ is understood.

The Birch & Swinnerton-Dyer conjecture equates the order of vanishing of $L(E,s)$ at $s = 1$ to the $\mathbb{Z}$-rank of the Mordell–Weil group $E(\mathbb{Q})$. More generally (see [**28**]), the order of vanishing of $L(E,s,\chi)$ at $s = 1$ is conjectured to be the rank of the 'χ-component' $E(K)^\chi$ of $E(K)$, where $K = K_\chi$. Here $\mathrm{rank}_{\mathbb{Z}}\, E(K)^\chi = \dim_{\mathbb{C}}(\mathbb{C} \otimes E(K))^\chi$ is the dimension of the χ eigenspace of $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$ as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-space.

The algebro-geometric version of vanishing (resp. non-vanishing) of $L(E,1,\chi)$ is whether the χ-component $E(K)^\chi$ of $E(K)$ has a positive rank (resp. $\mathrm{rank}_{\mathbb{Z}}\, E(K)^\chi = 0$) as K_χ ranges over the corresponding cyclic extensions of $\mathbb{Q}$. This amounts to asking whether or not $\mathrm{rank}_{\mathbb{Z}}\, E(K_\chi) > \mathrm{rank}_{\mathbb{Z}}\, E(F)$ for all proper subfields $F \subset K_\chi$.

We rely on Kato's important result [**15**] generalizing Kolyvagin's theorem [**19**], which asserts that if the χ-component of $E(K_\chi)$ has a positive rank, then $L(E,1,\chi) = 0$ (see Scholl [**30**].)

Suppose that χ is a character of prime order ℓ, $K = K_\chi$ is the field corresponding to χ, and let $V = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then V is a representation space for $G = \mathrm{Gal}(K/\mathbb{Q})$ with $\dim_{\mathbb{Q}} V = \mathrm{rank}_{\mathbb{Z}}\, E(K)$. Since G is a cyclic group of prime order, the $\mathbb{Q}$-irreducible characters of G are the trivial character χ_0 and an irreducible of degree $\ell - 1$ containing all the conjugates of χ. Hence if $\mathrm{rank}_{\mathbb{Z}}\, E(K) > \mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q})$, then the χ^j-component of $E(K)$ has a positive rank for each $j = 1, \ldots, \ell - 1$. It follows from Kato's theorem (Kolyvagin [**19**], if $\ell = 2$) that if $\mathrm{rank}_{\mathbb{Z}}\, E(K)^\chi > 0$ for a non-trivial character of prime order ℓ, then $L(E,1,\chi^j) = 0$ for each $j = 1, \ldots, \ell - 1$. In this context, it will follow from a modular symbol computation in § 3 that if $L(E,1,\chi) = 0$ for a single character of order ℓ, then $L(E,1,\chi^j) = 0$ for all $j = 1, \ldots, \ell - 1$.

In this paper, we consider the case $\ell \geqslant 3$. Our main theorems (proved in § 3, § 5 and § 6) are:

THEOREM A. *If $L(E,1) \neq 0$, then, for all but a finite number of primes ℓ, the number of non-vanishing twists by Dirichlet characters of order ℓ and prime conductor satisfies*

$$\#\{\chi \in \mathcal{X}(\ell) \mid \mathfrak{f}_\chi = p \text{ prime } < X, L(E,1,\chi) \neq 0\} \gg X/\log X.$$

THEOREM B. *If there is at least one character $\chi_1 \in \mathcal{X}(3)$ or $\chi_1 = \chi_0$, such that $E(K_{\chi_1})$ is infinite, then there are infinitely many cubic characters $\chi \in \mathcal{X}(3)$ such that $L(E,1,\chi) = 0$.*

THEOREM C. *Let $E/\mathbb{Q}$ be an elliptic curve with at least six rational points. Then there exist infinitely many $\chi \in \mathcal{X}(3)$ such that $\mathrm{rank}_{\mathbb{Z}}\, E(K_\chi) > \mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q})$. As a consequence, there are infinitely many cubic characters $\chi \in \mathcal{X}(3)$ such that $L(E,1,\chi) = 0$.*

A random matrix model for the distribution of zeros of L-functions in families was introduced by Katz and Sarnak [**17**] and was related to the distribution of eigenvalues of random matrices taken from classical groups. They proved that the model held in the case of L-functions attached to certain families of curves over finite fields. This heuristic was applied by Conrey, Keating, Rubinstein and Snaith [**8**] to give rather precise predictions for the frequency of vanishing of the central values of quadratic twists of elliptic L-functions with sign $+1$. In [**10**, **11**], their work was adapted to predict the frequency of vanishing at $s = 1$ of twists of the L-function by

Dirichlet characters χ of fixed order greater than 2. The predictions for $\mathfrak{F}_E(n, X)$ as $X \to \infty$ become

$$\mathfrak{F}_E(n, X) \sim b_E X^{1/2} \log^{a_E}(X) \quad \text{if } \phi(n) = 2$$
$$\mathfrak{F}_E(n, X) \sim \log^{a'_E}(X) \quad \text{if } \phi(n) = 4$$
$$\mathfrak{F}_E(n, X) \text{ is bounded if } \phi(n) \geqslant 6,$$

where ϕ is Euler's totient function and $b_E, a_E, a'_E \neq 0$. These predictions compare favourably to the numerical computations reported in [**10**, **11**].

In § 7, we work out the case of a curve with rational 3-torsion, and for many such curves $E/\mathbb{Q}$ we obtain the strong lower bound

$$\mathfrak{F}_E(3, X) \gg X^{1/2}.$$

2. *The quadratic case*

If χ is a *real* primitive character, that is, if $\chi^2 = \chi_0$, then $\chi = \chi_0$ or $\chi = \left(\frac{\cdot}{D}\right)$ is the character of a quadratic field $\mathbb{Q}(\sqrt{D})$, and $\mathfrak{f}_\chi = D$, a fundamental discriminant. In the latter case, $L(E, s, \chi)$ is the L-function of the elliptic curve E^D, the twist of E by D. Since χ is real, the functional equation relates $L(E, 1, \chi)$ to itself and necessarily vanishes if the sign of the functional equation $w_{E^D} = -1$. For a primitive quadratic character χ, with $(\mathfrak{f}_\chi, N_E) = 1$, the sign of the functional equation for $L(E, s, \chi)$ is equal to $\chi(-N_E)$ times that of $L(E, s)$. Hence we see that $L(E, 1, \chi) = 0$ for at least one half of such quadratic characters. It follows from the theorem of Waldspurger [**36**] (see also Ono and Skinner [**25**]), that there is an infinite number of quadratic characters χ for which $L(E, 1, \chi) \neq 0$.

Gouvêa and Mazur [**14**] show, assuming the parity conjecture (that $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$ of an elliptic curve, E, has the same parity as $\operatorname{ord}_{s=1} L(E, s)$), that there are infinitely many twists D with Mordell–Weil groups of rank at least 2. They show (under the parity conjecture) that

$$\mathfrak{F}^2_E(2, X) = \#\{\chi \in \mathcal{X}(2) \mid \mathfrak{f}_\chi < X, L(E, 1, \chi) = 0 = L'(E, 1, \chi)\} \gg X^{1/2-\epsilon}.$$

Stewart and Top [**34**] have removed the parity conjecture in the Gouvêa–Mazur result and obtain $X^{1/7-\epsilon}$ ($X^{1/6-\epsilon}$ for some special families of curves). Mai [**21**] proved that the number of cubic twists of $x^3 + y^3 = d$ for which the corresponding L-function has at least a double zero at $s = 1$ is asymptotically greater than $X^{2/3-\epsilon}$, also assuming the parity conjecture. Goldfeld [**13**] conjectured that, for a given elliptic curve E defined over $\mathbb{Q}$, asymptotically one half of the quadratic twists $L(E, s, \chi)$ of $L(E, s)$ will have a *simple* zero at $s = 1$ and asymptotically one half will be non-vanishing.

Murty and Murty [**27**] and Bump, Friedberg and Hoffstein [**5**] have shown that

$$L(E, 1, \chi) = 0 \neq L'(E, 1, \chi)$$

occurs for infinitely many quadratic characters χ.

In the case of twists of $L(E, s)$ by characters of higher order, that is, by characters χ of order $\ell \geqslant 3$, χ assumes complex values and the functional equation relates $L(E, s, \chi)$ to $L(E, s, \bar{\chi})$. Consequently, there is no longer a 'forced' central zero due to the sign of the functional equation. It is an interesting question to determine the number of characters χ in a given set of characters $\mathcal{X}$ for which $L(E, 1, \chi) = 0$.

Rohrlich [**29**] has shown that among all Dirichlet characters χ with conductors supported on a finite set of primes only finitely many can vanish at $s = 1$. Stefanicki [**33**], Akbary [**1**] and Murty [**26**] give various non-vanishing results for twisted central L-values and of particular interest is the result of Chinta [**6**], which states that, for sufficiently large prime q,

$$\#\{\chi \mid \mathfrak{f}_\chi = q, L(E, 1, \chi) = 0\} \ll q^{7/8+\epsilon}.$$

3. *Non-vanishing of twists of prime order*

Let $\ell > 2$ denote an *odd prime* number and suppose that E is an elliptic curve defined over the rational field $\mathbb{Q}$. Let $\chi \in \mathcal{X}(\ell)$ be a Dirichlet character. We will demonstrate a congruence between the algebraic part of $L(E,1)$ and the algebraic part of $L(E,1,\chi)$. In the case that $L(E,1) \neq 0$ this will allow us to prove that, for all but a finite number of primes ℓ, there are infinitely many characters $\chi \in \mathcal{X}(\ell)$ such that $L(E,1,\chi) \neq 0$.

Let f be a weight 2 modular form of level N. We recall the properties of modular symbols following Mazur, Tate and Teitelbaum [**22**].

For α and β in the upper half-plane, define a modular symbol $\{\alpha, \beta\}$ as a linear functional on cuspforms $f \in S_2(N) (= S_2(\Gamma_0(N)))$ by

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

For a fixed cuspform $f \in S_2(N)$, we will write $\{\alpha, \beta\}$ for $\{\alpha, \beta\} f$. The properties of the modular symbol which are important for our purposes are summarized below:

Proposition 3.1 (L-function relation). *The L-series of a cuspform at its critical point can be expressed as a modular symbol*

$$L(f,1) = \{\infty, 0\}.$$

Proposition 3.2 (Birch's theorem). *The value of an L-series twisted by a Dirichlet character can be expressed as a weighted sum of modular symbols*

$$L(f,1,\chi) = \frac{\tau(\chi)}{\mathfrak{f}_\chi} \sum_{a \bmod \mathfrak{f}_\chi} \bar{\chi}(a) \left\{\infty, \frac{a}{\mathfrak{f}_\chi}\right\},$$

where $\tau(\chi)$ is the Gauss sum.

Proposition 3.3 (Hecke action). *For an eigenform f of the Hecke operator T_p with eigenvalue a_p we have an action on the modular symbol as follows*:

$$a_p \left\{\infty, \frac{a}{\mathfrak{f}_\chi}\right\} = \left\{\infty, \frac{a}{\mathfrak{f}_\chi}\right\}^{T_p} = \sum_{u=0}^{p-1} \left\{\infty, \frac{a - u\mathfrak{f}_\chi}{p\mathfrak{f}_\chi}\right\} + \delta(p) \left\{\infty, \frac{ap}{\mathfrak{f}_\chi}\right\},$$

where $\delta(p) = 0$ if $p|N$ and $\delta(p) = 1$ otherwise.

Proposition 3.4 (Integrality). *There are non-zero complex numbers $\Omega^\pm$ depending only upon f such that*

$$\Lambda^\pm(a, \mathfrak{f}_\chi) := \left(\left\{\infty, \frac{a}{\mathfrak{f}_\chi}\right\} \pm \left\{\infty, \frac{-a}{\mathfrak{f}_\chi}\right\}\right) / \Omega^\pm \quad \textit{are integers.}$$

In the case that f is the cuspform associated to an elliptic curve, then the numbers $\Omega^\pm$ are rational multiples of the periods of the elliptic curve. As in [**22**], choose such an $\Omega^\pm$ (up to sign) so that the set of integers $\Lambda^\pm(a, \mathfrak{f}_\chi)$ have greatest common divisor equal to 1.

Note that, for $\gamma \in \Gamma_0(N)$ and $f \in S_2(\Gamma_0(N))$, we have $\{\gamma(\alpha), \gamma(\beta)\} f = \{\alpha, \beta\} f$. It follows that $\Lambda^\pm(a, \mathfrak{f}_\chi)$ depends only on the residue class of $a \mod \mathfrak{f}_\chi$.

Since we consider characters χ of prime order $\ell > 2$, they will be even characters (that is, $\chi(-1) = 1$) and we then take the positive sign. In what follows, we write Λ for Λ^+ and Ω for Ω^+.

Following [22], define the algebraic part of $L(f,1,\chi)$ to be

$$\begin{aligned} L^{\mathrm{alg}}(f,1,\chi) &= \frac{2\mathfrak{f}_\chi L(f,1,\chi)}{\Omega\tau(\chi)} \\ &= \sum_{a \bmod \mathfrak{f}_\chi} \bar{\chi}(a)\Lambda(a,\mathfrak{f}_\chi), \end{aligned}$$

where $\Omega = \Omega^+$, chosen as above, is independent of χ and $\Lambda(a,\mathfrak{f}_\chi) \in \mathbb{Z}$.

Let $\mathfrak{l}$ be a prime dividing ℓ in the cyclotomic field $\mathbb{Q}(\zeta_\ell)$ of ℓth roots of unity and let $\chi \in \mathcal{X}(\ell)$ be a Dirichlet character with conductor $\mathfrak{f}_\chi$. Then

$$\begin{aligned} &\chi(a) \equiv 1 \bmod \mathfrak{l} \quad \text{when } (a,\mathfrak{f}_\chi) = 1, \\ &\chi(a) = 0 \quad \text{when } (a,\mathfrak{f}_\chi) \neq 1. \end{aligned}$$

So

$$\sum_{a \bmod \mathfrak{f}_\chi} \bar{\chi}(a)\Lambda(a,\mathfrak{f}_\chi) \equiv \sum_{\substack{a \bmod \mathfrak{f}_\chi \\ (a,\mathfrak{f}_\chi)=1}} \Lambda(a,\mathfrak{f}_\chi) \bmod \mathfrak{l}.$$

Fix a cuspform $f \in S_2(N)$, and let

$$\Sigma_m(t) := \sum_{\substack{a \bmod t \\ (a,m)=1}} \Lambda(a,t).$$

For a character of order ℓ and conductor $\mathfrak{f}_\chi$, we have

$$L^{\mathrm{alg}}(f,1,\chi) \equiv \Sigma_{\mathfrak{f}_\chi}(\mathfrak{f}_\chi) \bmod \mathfrak{l}.$$

Theorem 3.5. *Let $f \in S_2(N)$ be a simultaneous eigenform for all the Hecke operators. Let χ be a Dirichlet character of order dividing ℓ and conductor $\mathfrak{f}_\chi$, and let $\psi \in \mathcal{X}(\ell)$ and prime conductor $\mathfrak{f}_\psi = p$ with $(\mathfrak{f}_\chi, p) = 1$. Let $\delta(t) = 1$ if $(t,N) = 1$ and zero otherwise. Then*

$$L^{\mathrm{alg}}(f,1,\chi\psi) \equiv (a_p - \delta(p) - 1)L^{\mathrm{alg}}(f,1,\chi) \bmod \mathfrak{l}.$$

If φ is the Dirichlet character of order ℓ and conductor ℓ^2 prime to $\mathfrak{f}_\chi$ we have

$$L^{\mathrm{alg}}(f,1,\chi\varphi) \equiv (a_\ell - 1)(a_\ell - \delta(\ell))L^{\mathrm{alg}}(f,1,\chi) \bmod \mathfrak{l}.$$

Since any character ψ of order ℓ and conductor $\mathfrak{f}_\psi$ can be factored as a product of characters of order ℓ either with prime conductors or with conductor ℓ^2, we can iterate the above result to obtain:

Corollary 3.6. *For $f \in S_2(N)$ as above, χ a character of order dividing ℓ, and $\psi \in \mathcal{X}(\ell)$, if $\mathfrak{f}_\psi$ is not divisible by ℓ, then we have*

$$L^{\mathrm{alg}}(f,1,\chi\psi) \equiv L^{\mathrm{alg}}(f,1,\chi) \prod_{p \mid \mathfrak{f}_\psi} (a_p - \delta(p) - 1) \bmod \mathfrak{l}.$$

and if $\ell \mid \mathfrak{f}_\psi$

$$L^{\mathrm{alg}}(f,1,\chi\psi) \equiv L^{\mathrm{alg}}(f,1,\chi)(a_\ell - 1)(a_\ell - \delta(\ell)) \prod_{\substack{p \mid \mathfrak{f}_\psi \\ p \neq \ell}} (a_p - \delta(p) - 1) \bmod \mathfrak{l}.$$

Proof of Theorem 3.5. We consider the sums $\Sigma_m(m)$, $\Sigma_{pm}(pm)$ and $\Sigma_{p^2m}(p^2m)$. Assume that $(m,p)=1$.

$$\begin{aligned}
\Sigma_m(m) \mid T_p = a_p\Sigma_m(m) &= \sum_{\substack{a \bmod m\\(a,m)=1}} \left[\sum_{u=0}^{p-1} \Lambda(a-um,pm) + \delta(p)\Lambda(ap,m)\right]\\
&= \sum_{\substack{a \bmod m\\(a,m)=1}} \sum_{u=0}^{p-1} \Lambda(a-um,pm) + \delta(p) \sum_{\substack{a \bmod m\\(a,m)=1}} \Lambda(ap,m)\\
&= \Sigma_m(pm) + \delta(p)\Sigma_m(m).
\end{aligned}$$

Now

$$\begin{aligned}
\Sigma_m(pm) &= \sum_{\substack{a \bmod pm\\(a,m)=1}} \Lambda(a,pm)\\
&= \sum_{\substack{a \bmod pm\\(a,pm)=1}} \Lambda(a,pm) + \sum_{\substack{a \bmod pm\\(a,pm)=p}} \Lambda(a,pm)\\
&= \Sigma_{pm}(pm) + \sum_{\substack{b \bmod m\\(b,m)=1}} \Lambda(bp,pm)\\
&= \Sigma_{pm}(pm) + \Sigma_m(m).
\end{aligned}$$

So

$$\begin{aligned}
a_p\Sigma_m(m) &= \Sigma_{pm}(pm) + \Sigma_m(m) + \delta(p)\Sigma_m(m),\\
\Sigma_{pm}(pm) &= (a_p - 1 - \delta(p))\Sigma_m(m).
\end{aligned}$$

Taking $m = \mathfrak{f}_\chi$, and noting that $\mathfrak{f}_\psi = p$, we have

$$\begin{aligned}
L^{\mathrm{alg}}(f,1,\chi\psi) &\equiv \Sigma_{pm}(pm) \bmod \mathfrak{l},\\
L^{\mathrm{alg}}(f,1,\chi) &\equiv \Sigma_m(m) \bmod \mathfrak{l}.
\end{aligned}$$

Therefore the first statement of Theorem 3.5 follows:

$$L^{\mathrm{alg}}(f,1,\chi\psi) \equiv (a_p - \delta(p) - 1)L^{\mathrm{alg}}(f,1,\chi) \bmod \mathfrak{l}.$$

To treat $\Sigma_{p^2m}(p^2m)$, we apply T_p a second time.

$$\begin{aligned}
(\Sigma_m(m) \mid T_p) \mid T_p = a_p^2\Sigma_m(m) &= \sum_{\substack{a \bmod m\\(a,m)=1}} \left[\sum_{u=0}^{p-1} \Lambda(a-um,pm)^{T_p} + \delta(p)\Lambda(ap,m)^{T_p}\right]\\
&= \sum_{\substack{a \bmod m\\(a,m)=1}} \sum_{v=0}^{p-1}\sum_{u=0}^{p-1} \Lambda(a-um-vmp,p^2m)\\
&\quad + \delta(p) \sum_{\substack{a \bmod m\\(a,m)=1}} \sum_{v=0}^{p-1} \Lambda((a-um)p,pm)\\
&\quad + \delta(p) \sum_{\substack{a \bmod m\\(a,m)=1}} \sum_{v=0}^{p-1} \Lambda(ap-vm,pm) + \delta(p)^2 \sum_{\substack{a \bmod m\\(a,m)=1}} \Lambda(ap^2,m)\\
&= \Sigma_m(p^2m) + \delta(p)p\Sigma_m(m) + \delta(p)\Sigma_m(pm) + \delta(p)\Sigma_m(m).
\end{aligned}$$

Now

$$\Sigma_m(pm) = \Sigma_{pm}(pm) + \Sigma_m(m)$$

and

$$\begin{aligned}
\Sigma_m(p^2m) &= \sum_{\substack{a \bmod p^2m \\ (a,m)=1}} \Lambda(a, p^2m) \\
&= \sum_{\substack{a \bmod p^2m \\ (a,mp^2)=1}} \Lambda(a, p^2m) + \sum_{\substack{a \bmod p^2m \\ (a,mp^2)=p}} \Lambda(a, p^2m) + \sum_{\substack{a \bmod p^2m \\ (a,mp^2)=p^2}} \Lambda(a, p^2m) \\
&= \Sigma_{p^2m}(p^2m) + \sum_{\substack{b \bmod pm \\ (b,mp)=1}} \Lambda(bp, p^2m) + \sum_{\substack{c \bmod m \\ (c,m)=1}} \Lambda(cp^2, p^2m) \\
&= \Sigma_{p^2m}(p^2m) + \Sigma_{pm}(pm) + \Sigma_m(m).
\end{aligned}$$

So

$$\begin{aligned}
a_p^2\Sigma_m(m) &= \Sigma_{p^2m}(p^2m) + \Sigma_{pm}(pm) + \Sigma_m(m) + \delta(p)p\Sigma_m(m) + \delta(p)\Sigma_m(m) \\
&\quad + \delta(p)(\Sigma_{pm}(pm) + \Sigma_m(m)) \\
&= \Sigma_{p^2m}(p^2m) + \Sigma_{pm}(pm)(1 + \delta(p)) + \Sigma_m(m)(1 + \delta(p)p + 2\delta(p)) \\
&= \Sigma_{p^2m}(p^2m) + (a_p - 1 - \delta(p))(1 + \delta(p))\Sigma_m(m) + \Sigma_m(m)(1 + \delta(p)p + 2\delta(p)) \\
&= \Sigma_{p^2m}(p^2m) + \Sigma_m(m)(a_p + \delta(p)a_p - \delta(p) + \delta(p)p).
\end{aligned}$$

Simplifying

$$\begin{aligned}
\Sigma_{p^2m}(p^2m) &= [a_p^2 - a_p - \delta(p)a_p - \delta(p)p + \delta(p)]\Sigma_m(m) \\
&= [(a_p - 1)(a_p - \delta(p)) - \delta(p)p]\Sigma_m(m).
\end{aligned}$$

Taking $p = \ell$, we see that the second statement of Theorem 3.5 now follows as above. If φ is the Dirichlet character of order ℓ and conductor $\ell^2 = p^2$ prime to $\mathfrak{f}_\chi$, we have

$$\begin{aligned}
L^{\mathrm{alg}}(f, 1, \chi\varphi) &\equiv \Sigma_{p^2m}(p^2m) \bmod \mathfrak{l} \\
&\equiv [(a_\ell - 1)(a_\ell - \delta(\ell)) - \delta(\ell)\ell]\Sigma_m(m) \bmod \mathfrak{l} \\
&\equiv (a_\ell - 1)(a_\ell - \delta(\ell))L^{\mathrm{alg}}(f, 1, \chi) \bmod \mathfrak{l}.
\end{aligned}$$

□

THEOREM 3.7. *Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime. Suppose that $L^{\mathrm{alg}}(E, 1) \not\equiv 0 \bmod \ell$; then there is a set of primes, S, of positive density such that $L(E, 1, \chi) \neq 0$ for any characters χ of order ℓ with conductor $\mathfrak{f}_\chi$ supported on S.*

Proof. The value of the twist $L^{\mathrm{alg}}(E, 1, \chi)$ can only vanish $\bmod\, \mathfrak{l}$ if either $L^{\mathrm{alg}}(E, 1) \equiv 0 \bmod \mathfrak{l}$ or one of the factors $(a_p - \delta(p) - 1)$ or $(a_\ell - 1)(a_\ell - \delta(\ell))$ vanishes $\bmod\, \mathfrak{l}$.

By Serre's theorem [**31**], we can find a *positive density* of primes $p \equiv 1 \bmod \ell$ for which the factors $(a_p - \delta(p) - 1) \not\equiv 0 \bmod \ell$. □

REMARK 3.8. The following examples show that the condition $L^{\mathrm{alg}}(E, 1) \not\equiv 0 \bmod \ell$ is necessary for the argument proving Theorem 3.7. Consider the elliptic curve $E = 2534\mathrm{f}1$ in Cremona's tables [**9**]. Then $L^{\mathrm{alg}}(E, 1) = 18$ but $L^{\mathrm{alg}}(E, 1, \chi) = 0$ for the character χ of order 3 and conductor $\mathfrak{f}_\chi = 37$. We note that for this curve $a_{37} = 4$ so $a_{37} - \delta(37) - 1 = 2 \not\equiv 0 \bmod 3$. Similar examples are afforded by the elliptic curves 2718d1 twisted by the character of order

3 and conductor 523 and 4229a1 twisted by the character of order 3 and conductor 43. We would like to thank the referee for pointing out the need for such examples.

THEOREM 3.9. *Let $E/\mathbb{Q}$ be an elliptic curve such that $L(E,1) \neq 0$. Then, for all but a finite number of primes ℓ, there is a set of primes S_ℓ of positive density such that $L(E,1,\chi) \neq 0$ for all characters χ of order ℓ with conductor $\mathfrak{f}_\chi$ supported on S_ℓ.*

The statement of Theorem A follows immediately.

4. *Vanishing twists and rational points of an auxiliary variety*

Kato's result [**15**] generalizing Kolyvagin's theorem shows that if the χ-component of $E(K_\chi)$ has a positive rank, then $L(E,1,\chi) = 0$. Thus, the algebro-geometric version of our question is whether the χ-component $E(K_\chi)^\chi$ of $E(K_\chi)$ has a positive rank or not, as K_χ ranges over the corresponding cyclic extensions of $\mathbb{Q}$. In order to find points on E defined over some cyclic extension K_χ, we will define an auxiliary variety of higher dimension whose $\mathbb{Q}$-rational points correspond to points on E defined over some cyclic extensions. As we are interested in cubic extensions, we construct this variety starting from $E^3 = E \times E \times E$.

Let k be a number field, and let $\bar{k}$ be its algebraic closure, which we fix once and for all. We denote by $G_k = \mathrm{Gal}(\bar{k}/k)$, the Galois group of $\bar{k}/k$. Throughout this section, a point means a geometric point, that is, a $\bar{k}$-valued point.

The symmetric group $\mathfrak{S}_3$ acts on E^3 in an obvious way. Its alternating subgroup $\mathfrak{A}_3$ is a cyclic group of order 3 generated by the automorphism ρ given by

$$\begin{aligned} \rho: \quad E \times E \times E &\longrightarrow E \times E \times E, \\ (P,Q,R) &\longmapsto (Q,R,P). \end{aligned}$$

Let $X = E^3/\mathfrak{A}_3$ be the quotient variety (cf. [**24**, Chapter II, § 7 and Chapter III, § 12)]). Since the action of $\mathfrak{A}_3$ commutes with the Galois action of E^3, X is a variety defined over k. We denote by $[P,Q,R]$ the class of (P,Q,R) in X.

Let D be the diagonal subgroup $\{(P,P,P) \mid P \in E\}$ in E^3. We define the complement $\hat{D}$ of D in E^3 by

$$\hat{D} = \{(P,Q,R) \mid P+Q+R = O\},$$

where $\hat{D}$ is a subgroup of E^3 invariant under the action of ρ. We have $(D \times \hat{D})/\mathfrak{A}_3 = D \times (\hat{D}/\mathfrak{A}_3) \cong E \times (\hat{D}/\mathfrak{A}_3)$. Moreover, we have a degree 3 isogeny $\varphi : E^3 \to D \times \hat{D}$ given by

$$\begin{aligned} \varphi: \quad E^3 &\longrightarrow D \times \hat{D}, \\ (P,Q,R) &\longmapsto ((S,S,S),(3P-S,3Q-S,3R-S)), \end{aligned}$$

where $S = P+Q+R$. Its dual isogeny $\varphi' \colon D \times \hat{D} \to E^3$ is given by

$$\begin{aligned} \varphi': \quad D \times \hat{D} &\longrightarrow E^3, \\ ((S,S,S),(P,Q,R)) &\longmapsto (P+S,Q+S,R+S). \end{aligned}$$

Since φ and φ' commute with the $\mathfrak{A}_3$-action, we take the quotients by the $\mathfrak{A}_3$-action and obtain two maps

$$\bar{\varphi} : X \longrightarrow E \times (\hat{D}/\mathfrak{A}_3), \quad \bar{\varphi}' : E \times (\hat{D}/\mathfrak{A}_3) \longrightarrow X$$

such that $\bar{\varphi}' \circ \bar{\varphi}$ is the map $\overline{[3]}$ induced by the multiplication-by-3 map $[3]$ of E^3. The quotient $\hat{D}/\mathfrak{A}_3$ is a surface, which we denote by $\bar{S}_E$.

Lemma 4.1. *A point $[P,Q,R]$ in $\bar{S}_E$ is a k-rational point if and only if one of the following is satisfied:*

1. *P, Q and R are all defined over k, and $P+Q+R=O$, or*
2. *P, Q and R are defined over a certain cyclic cubic extension K/k, and for a suitable generator $\sigma \in \mathrm{Gal}(K/k)$, we have $(P^\sigma, Q^\sigma, R^\sigma) = (Q,R,P)$, together with the relation $P + P^\sigma + P^{\sigma^2} = O$.*

Proof. It is clear that if (1) or (2) is satisfied, then $[P,Q,R]$ is stable under the Galois action, and thus $[P,Q,R] \in \bar{S}_E(k)$.

Conversely, suppose $[P,Q,R] \in \bar{S}_E(k)$. This is equivalent to saying that, for any $\sigma \in G_k$, the conjugate $(P^\sigma, Q^\sigma, R^\sigma)$ coincides with (P,Q,R), $\rho((P,Q,R)) = (Q,R,P)$ or $\rho^2((P,Q,R)) = (R,P,Q)$.

First, suppose that the triples (P,Q,R), (Q,R,P) and (R,P,Q) are mutually distinct. Then, we can define a map $\psi : G_k \to \langle\rho\rangle$ by stipulating that $(P^\sigma, Q^\sigma, R^\sigma) = \psi(\sigma)((P,Q,R))$. Since the automorphism ρ is defined over k, the map ψ is a homomorphism. Let K be the Galois extension of k corresponding to $\operatorname{Ker}\psi$ via Galois theory. Then $\mathrm{Gal}(K/k)$ is isomorphic to a subgroup of $\langle\rho\rangle$, that is, $\mathrm{Gal}(K/k) \cong \langle\rho\rangle$, or $\mathrm{Gal}(K/k) = \{\mathrm{id}\}$. If $\mathrm{Gal}(K/k) = \{\mathrm{id}\}$, then $K = k$, and P, Q and R are all defined over k. This is case (1). If $\mathrm{Gal}(K/k) \cong \langle\rho\rangle$, then K is a cyclic cubic extension. Let $\sigma \in \mathrm{Gal}(K/k)$ be the element that maps to ρ by ψ. Then we have $(P^\sigma, Q^\sigma, R^\sigma) = (Q,R,P)$. This is case (2).

Next, if (P,Q,R), (Q,R,P) and (R,P,Q) are not mutually distinct, then we must have $P = Q = R$. In this case, for any $\sigma \in G_k$, the conjugate $(P^\sigma, P^\sigma, P^\sigma)$ must equal (P,P,P). Thus, this case is included in case (1). $\square$

In order to give a concrete description of $\hat{D}/\mathfrak{A}_3$, we fix a Weierstrass model of E and consider it as a curve in $\mathbb{P}^2$. Namely, suppose that E is given by the equation

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Then, as is well known, three points P, Q and R satisfy $P+Q+R=O$ if and only if P, Q and R are collinear. Let $(\mathbb{P}^2)^*$ be the dual space of $\mathbb{P}^2$, namely, the space of all the lines in $\mathbb{P}^2$. For a point $(P,Q,R) \in \hat{D}$ we denote by ℓ_{PQR} the line passing through P, Q and R. If $P=Q=R$, we understand that ℓ_{PPP} is the tangent line to E passing through P. Consider the map

$$\begin{aligned} \pi_0 : \quad \hat{D} &\longrightarrow (\mathbb{P}^2)^*, \\ (P,Q,R) &\longmapsto \ell_{PQR}. \end{aligned}$$

It is clear that π_0 is a surjection and is invariant under the $\mathfrak{S}_3$-action. Thus we obtain an isomorphism $\hat{D}/\mathfrak{S}_3 \xrightarrow{\simeq} (\mathbb{P}^2)^*$, which sends a class $[P,Q,R]$ of $\hat{D}/\mathfrak{S}_3$ to the line ℓ_{PQR}. Now, π_0 induces the map

$$\pi_1 : \bar{S}_E = \hat{D}/\mathfrak{A}_3 \longrightarrow \hat{D}/\mathfrak{S}_3 \simeq (\mathbb{P}^2)^*,$$

where π_1 is a covering map of degree $2 = [\mathfrak{S}_3 : \mathfrak{A}_3]$. It is easy to see that $\pi_1^{-1}(\ell_{PQR})$ consists of two classes, $[P,Q,R]$ and $[P,R,Q]$. In $\bar{S}_E$ the classes $[P,Q,R]$ and $[P,R,Q]$ coincide if and only if at least two of three points coincide. In other words $[P,Q,R] = [P,R,Q]$ if and only if ℓ_{PQR} is a tangent line to the curve E. This implies that the double covering π_1 ramifies along the dual curve $E^* = \{L \in (\mathbb{P}^2)^* \mid L \text{ is tangent to } E\}$, which is an irreducible curve of degree 6, and it has nine cusps corresponding to the tangent lines at nine inflection points of E. The surface $\bar{S}_E$ thus has nine singular points of type A_2. Let S_E be the minimal desingularization of $\bar{S}_E$ obtained by blowing up twice at each singular point. Summing up, we have:

PROPOSITION 4.2. *The quotient surface $\bar{S}_E = \hat{D}/\mathfrak{A}_3$ may be regarded as a double cover of the dual projective plane $(\mathbb{P}^2)^*$ ramifying along the dual curve E^* of E, which is an irreducible curve of degree 6. As a consequence the minimal desingularization S_E of $\bar{S}_E$ is a $K3$ surface.*

REMARK 4.3. If the quotient of an abelian surface A by a finite group G is birational to a $K3$ surface, its minimal desingularization is called a generalized Kummer surface. Thus S_E is a generalized Kummer surface. For more about Kummer surfaces see Katsura [**16**] and Bertin [**2**].

Write the equation of a generic line ℓ in $\mathbb{P}^2$ in the form $y = tx + u$, using parameters t and u. The function field of $(\mathbb{P}^2)^*$ is then given by $k(t, u)$, and the function field of $\hat{D}$ can be regarded as the splitting field of the cubic equation in x obtained by substituting $y = tx + u$ in the affine Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The function field of $\bar{S}_E = \hat{D}/\mathfrak{A}_3$ is then the extension of $k(t, u)$ obtained by adding the square root of the discriminant $\Delta(u, t)$ of this cubic equation with respect to x. This implies that the surface S_E is a minimal model of the surface defined by the equation

$$\delta^2 = \Delta(u, t). \tag{4.1}$$

For simplicity, we write the explicit result only in the case where $a_1 = a_2 = a_3 = 0$, $a_4 = A$, and $a_6 = B$.

PROPOSITION 4.4. *Let $y^2 = x^3 + Ax + B$ be a Weierstrass equation for E. Then, the generalized Kummer surface S_E is birational to the affine surface in $\mathbb{A}^3 = \{(t, u, \delta)\}$ defined by the equation*

$$\begin{aligned} \delta^2 = {} & -27u^4 - 4t^3u^3 - (30At^2 - 54B)u^2 - 4t(At^4 - 9t^2 - 6A^2)u \\ & + 4Bt^6 + A^2t^4 - 18ABt^2 - (4A^3 + 27B^2). \end{aligned} \tag{4.2}$$

REMARK 4.5. The surface S_E possesses two obvious involutions, $[P, Q, R] \mapsto [Q, P, R]$ and $[P, Q, R] \mapsto [-P, -Q, -R]$. In terms of equation (4.2), the former corresponds to $(t, u, \delta) \mapsto (t, u, -\delta)$, while the latter corresponds to $(t, u, \delta) \mapsto (-t, -u, \delta)$.

Consider the map $\nu : E \to \bar{S}_E$ given by $P \mapsto [P, -P, O]$. This is an injection, and we have an embedding $\tilde{\nu} : E \to S_E$. Let $D_{\tilde{\nu}(E)}$ be the divisor associated with the image of $\tilde{\nu}$. Then the complete linear system $|D_{\tilde{\nu}(E)}|$ determines a pencil of curves of genus 1. Let $\bar{\pi} : \bar{S}_E \to \mathbb{P}^1$ be the map associated with the projection $(t, u, \delta) \mapsto t$. The fiber at $t = \infty$ corresponds exactly to the image of the embedding $P \to [P, -P, O]$, and thus the fibration π coincides with the pencil above. Let $\pi : S_E \to \mathbb{P}^1$ be the elliptic fibration obtained in this way.

Let C_t be the generic fiber of π, that is, the curve of genus 1 defined over the function field $k(t)$ given by equation (4.2).

The coefficient of u^4 in the right-hand side of (4.2) is constant, namely, -27. Thus, the curve C_t has two points at infinity defined over $k(\sqrt{-3})$. In other words, if k contains $\sqrt{-3}$, C_t has a $k(t)$-rational point and it is an elliptic curve over $k(t)$. However, if k does not contain $\sqrt{-3}$, we do not know if C_t has a $k(t)$-rational point, and whether we can consider it as an elliptic curve. Instead, we need to consider its Jacobian J_t.

Using an algorithm for calculating an equation of the Jacobian of the curve given by a quartic equation (see Connell [7]), we see that J_t is given by the equation

$$\begin{aligned} J_t:\ Y^2 = X^3 &+ (At^8 + 18Bt^6 - 18A^2t^4 - 54ABt^2 - 27(A^3+9B^2))X \\ &+ (Bt^{12} - 4A^2t^{10} - 45ABt^8 - 270B^2t^6 + 135A^2Bt^4 \\ &- 54A(2A^3+9B^2)t^2 - 243B(A^3+6B^2)). \end{aligned}$$

PROPOSITION 4.6. *The elliptic surface associated with the curve J_t has eight singular fibers of type I_3 located at t satisfying*

$$t^8 + 18At^4 + 108Bt^2 - 27A^2 = 0. \tag{4.3}$$

The Mordell–Weil group $J_t(\bar{k}(t))$ contains a point of infinite order γ_1 given by

$$\gamma_1 = \left(-\frac{1}{27}t^6 + 5At^2 - 9B, \frac{\sqrt{-3}}{243}t(t^8 + 162At^4 - 2916Bt^2 - 2187A^2)\right).$$

Proof. It is easy to determine the singular fibers using Tate's algorithm. Over $k(\sqrt{-3})$, C_t and J_t are isomorphic. Using an algorithm in [7], we can write an isomorphism which sends one of the two points at infinity on C_t to the origin of J_t and the other to γ_1. Using an algorithm in [20], we calculate the canonical height of γ_1, which turns out to be 3. This implies that it has infinite order. □

REMARK 4.7. We note that, if E does not have complex multiplication, then $J_t(\bar{k}(t))$ is isomorphic to

$$\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},$$

and $J_t(\bar{k}(t))/J_t(\bar{k}(t))_{\mathrm{tors}}$ is generated by γ_1. All the points in $J_t(\bar{k}(t))$ are defined already over $k(E[3])(t)$. We omit the proof since we do not need these facts in what follows.

5. *Vanishing of cubic twists*

Let E be an elliptic curve defined over $\mathbb{Q}$. The goal of this section is to prove Theorem B. To do so, we will prove its algebro-geometric version Theorem 5.1 and then apply Kato's theorem to conclude the vanishing of the corresponding twisted L-functions.

THEOREM 5.1. *Let E be an elliptic curve defined over a number field k. Suppose that there is at least one cyclic extension K_0/k of degree dividing 3 such that $E(K_0)$ is infinite (possibly $K_0 = k$). Then $\operatorname{rank}_{\mathbb{Z}} E(K_\lambda) > \operatorname{rank}_{\mathbb{Z}} E(k)$ for infinitely many cyclic cubic extensions K_λ/k.*

Let K/k be any finite extension and let $\mathrm{Tr}_{K/k} : E(K) \to E(k)$ denote the trace map. The kernel $\operatorname{Ker}\mathrm{Tr}_{K/k} \subset E(K)$ is the subgroup of points of $E(K)$ of trace zero. The point satisfying the second condition of Lemma 4.1 belongs to $\operatorname{Ker}\mathrm{Tr}_{K/k}$.

LEMMA 5.2. *The following are equivalent*:

(1) $\operatorname{rank}_{\mathbb{Z}} E(K) > \operatorname{rank}_{\mathbb{Z}} E(k)$,
(2) *$E(K)$ contains a trace zero point of infinite order*,
(3) $\#(\operatorname{Ker}\mathrm{Tr}_{K/k}) = \infty$.

Proof. Let $n = [K : k]$. Define the maps t and t' of abelian groups as follows:

$$\begin{array}{ccccc} E(K) & \xrightarrow{t} & E(k) \times \operatorname{Ker} \operatorname{Tr}_{K/k} & \xrightarrow{t'} & E(K) \\ P & \longmapsto & (\operatorname{Tr}_{K/k}(P), nP - \operatorname{Tr}_{K/k}(P)) & & \\ & & (Q, R) & \longmapsto & Q + R \end{array}$$

Then we see that $t' \circ t = [n]$ and $t \circ t' = [n]$, where $[n]$ is the multiplication-by-n map. Thus, we have

$$\operatorname{rank}_{\mathbb{Z}} E(K) = \operatorname{rank}_{\mathbb{Z}} E(k) + \operatorname{rank}_{\mathbb{Z}} \operatorname{Ker} \operatorname{Tr}_{K/k}.$$

The statement of the lemma follows immediately. □

We now prove some lemmas that are necessary later in the proof.

Consider the surface defined by (4.2) together with the fibration $(t, u, \delta) \mapsto t$. Suppose we have infinitely many k-rational points $\gamma_n = (u_n, t_0, \delta_n)$ for a fixed t_0. For each n, the point γ_n corresponds to a class $[P_n, Q_n, R_n]$ in S_E. Let K_n be the field over which P_n, Q_n and R_n are defined. We already know that $K_n = k$ or K_n/k is a cyclic cubic extension of k.

LEMMA 5.3. *Suppose there is a non-zero t_0 such that the fiber $C_{t_0} = \pi^{-1}(t_0)$ is a good fiber having infinitely many k-rational points $\gamma_n = (u_n, t_0, \delta_n)$. Then the compositum of all K_n is an infinite extension of k.*

Proof. For each n, the cubic polynomial $x^3 + Ax + B - (t_0 x + u_n)^2$ in x factors into three linear terms over K_n. Conversely, finding a k-rational point (u, t_0, δ) on the surface (4.2) involves finding u in k such that $x^3 + Ax + B - (t_0 x + u)^2$ factors completely over some cubic cyclic field L. This is equivalent to finding a point $(\xi_1, \xi_2, \xi_3, t_0)$ on the curve given by

$$\begin{cases} \xi_1 + \xi_2 + \xi_3 = t_0^2, \\ \xi_1\xi_2 + \xi_2\xi_3 + \xi_3\xi_1 = A - 2t_0 u, \\ \xi_1\xi_2\xi_3 = u^2 - B. \end{cases}$$

Since $t_0 \neq 0$, we obtain a plane curve of degree 4 by eliminating ξ_3 and u. A calculation shows that this degree 4 curve is non-singular if and only if $t_0^8 + 18At_0^4 + 108Bt_0^2 - 27A^2 \neq 0$. If that is the case, the genus of the curve is 3. Thus, by a theorem of Faltings, it has only finitely many K-rational points for each fixed number field K. Therefore, the compositum of all K_n cannot be a number field of finite degree over $\mathbb{Q}$. □

In the case where k contains $\sqrt{-3}$, Lemma 5.3 and Proposition 4.6 prove the following statement, which is stronger than Theorem 5.1.

THEOREM 5.4. *Let E be an elliptic curve defined over a number field k containing $\sqrt{-3}$. Then there exist infinitely many cyclic cubic extensions K_λ such that $\operatorname{rank}_{\mathbb{Z}} E(K_\lambda) > \operatorname{rank}_{\mathbb{Z}} E(k)$.*

For the general case, we need another lemma.

LEMMA 5.5. *Let S be a smooth surface and C a smooth curve both defined over k. Let $\pi : S \to C$ be a fibration defined over k such that the generic fiber is a curve of genus 1 equipped with an involution ι with a fixed point. Suppose that the set of k-rational points, $S(k)$, is Zariski* *dense in* S; *then there exist infinitely many* k*-rational points* P *on* C *such that the fiber* $\pi^{-1}(P)$ *contains infinitely many* k*-rational points.*

Proof. Let $\pi' : J \to C$ be the Jacobian fibration associated with $\pi : S \to C$. There is a map $f : S \to J$ of degree 4 defined over k sending a point $P \in S$ to the divisor class $(P) - (\iota(P))$. Since f is dominant, the image of $S(k)$ under f is Zariski dense.

By Merel's theorem on the bound for the torsion points defined over a number field on an elliptic curve [**23**], the set consisting of all the k-rational torsion points of all the fibers is contained in a proper Zariski closed set. Thus if we denote by $f(S(k))'$ the set consisting of all the points in the image of $f(S(k))$ that have infinite order, then $f(S(k))'$ is still Zariski dense in J. This means that there are infinitely many k-rational points P on C such that the fiber $\pi'^{-1}(P)$ contains points in $f(S(k))'$. For such P the $\pi^{-1}(P)$ contains infinitely many k-rational points. □

Proof of Theorem 5.1. Let K_0/k be a cyclic extension of degree dividing 3 such that $E(K_0)$ is infinite. Let $P \in E(K_0)$ be a point of infinite order. First, we show that the set of k-rational points in S_E is Zariski dense in S_E.

If $K_0 = k$ and P is defined already over k, then the set $\{[mP, nP, -(m+n)P] \mid n, m \in \mathbb{Z}\}$ is clearly Zariski dense in S_E. We thus assume that K_0/k is a cubic extension and P is defined over K_0, but not over k. Let σ be a generator of $\mathrm{Gal}(K_0/k)$. Then $R = \mathrm{Tr}_{K_0/k}(P)$ is a point defined over k. If R is a point of infinite order, then we are in the previous case. If not, replacing P by nP if necessary, we may assume that $\mathrm{Tr}_{K_0/k}(P) = O$.

We consider $E(K_0)$ as an $\mathrm{End}_k(E)$-module, and we claim that P and P^σ are $\mathrm{End}_k(E)$-linearly independent, except when E has complex multiplication over $\mathbb{Q}(\sqrt{-3})$ and k contains $\sqrt{-3}$. Suppose $[\alpha]$ and $[\beta]$ are two non-zero endomorphsims of E defined over k, and suppose we have the relation

$$[\alpha]P + [\beta]P^\sigma = O. \tag{5.1}$$

Apply σ to both sides of (5.1). Since σ commutes with $[\alpha]$ and $[\beta]$, we have another relation

$$[\alpha]P^\sigma + [\beta](-P - P^\sigma) = O. \tag{5.2}$$

Eliminating P^σ from (5.1) and (5.2), we obtain

$$([\alpha]^2 - [\alpha][\beta] + [\beta]^2)P = O.$$

This occurs only when E has complex multiplication by $\mathbb{Q}(\sqrt{-3})$. Moreover, since $[\alpha]$ is defined over k, $\sqrt{-3}$ must be contained in k. We have thus verified the claim. The case where k contains $\sqrt{-3}$ has been treated already. In what follows, we assume $\sqrt{-3} \notin k$.

Next we claim that the subgroup $\{(nP, nP^\sigma, nP^{\sigma^2}) \mid n \in \mathbb{Z}\}$ is Zariski dense in $\hat{D}$. To prove this, it suffices to show that $\{(nP, nP^\sigma) \mid n \in \mathbb{Z}\}$ is Zariski dense in $E \times E$. Let F be the Zariski closure of this subgroup. Suppose F does not equal $E \times E$; then F is a closed subgroup of dimension 1 in $E \times E$. Let F^0 be the connected component of F containing the identity. We then have two isogenies ϕ_1 and ϕ_2 from F^0 to E, corresponding to two projections $E \times E \to E$. Choose $m \in \mathbb{Z}$ such that (mP, mP^σ) is in F^0. Let $\hat{\phi}_1$ be the dual isogeny of ϕ_1. Consider the endomorphism $\phi_2\hat{\phi}_1$ of E. Let d be the degree of ϕ_1. Since $\hat{\phi}_1\phi_1$ equals the multiplication-by-d map, we have

$$\begin{aligned} \phi_2\hat{\phi}_1(mP) &= \phi_2\hat{\phi}_1\phi_1((mP, mP^\sigma)) \\ &= \phi_2((dmP, dmP^\sigma)) \quad (d = \deg \phi_1) \\ &= dmP^\sigma. \end{aligned}$$

This contradicts the independence of P and P^σ.

Since the projection map $\hat{D} \to \bar{S}_E$ is a dominant map, the set $\{[nP, nP^{\sigma}, nP^{\sigma^2}] \mid n \in \mathbb{Z}\}$ is also Zariski dense in S_E. We have thus proved that $S_E(k)$ is Zariski dense in all cases.

The fibration $\pi : \bar{S}_E \to \mathbb{P}^1$ constructed in § 4 satisfies the hypotheses of Lemma 5.5. Thus, there exist infinitely many $t \in \mathbb{P}^1$ such that the fiber $\pi^{-1}(t)$ has infinitely many k-rational points. In particular, we have at least one such t such that $t \neq 0$ and $\pi^{-1}(t)$ is a good fiber. Then Lemma 5.3 implies that there exist infinitely many different cyclic cubic extensions K_λ such that the elliptic curve E possesses a point P_λ defined over K_λ.

In order to complete the proof we have to show that P_λ has infinite order except for a finite number of λ. But this is true because the bound of the order of torsion points given by Merel's theorem depends only on the degree of the field. □

6. *Elliptic curves with at least six rational torsion points*

In this section, we prove the following statement.

THEOREM 6.1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Suppose that there are at least six points in $E(\mathbb{Q})$. Then, for infinitely many cyclic cubic extensions $K/\mathbb{Q}$, we have* $\operatorname{rank}_{\mathbb{Z}} E(K) > \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

Proof. If $E(\mathbb{Q})$ has infinitely many points, then this is nothing but Theorem 5.1. Suppose $E(\mathbb{Q})$ is finite. Then, by Mazur's bound for the torsion of elliptic curves over $\mathbb{Q}$, either $E(\mathbb{Q})$ is a cyclic group of order $6, 7, 8, 9, 10, 12$, or it contains $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a subgroup. In view of Lemma 5.3, it suffices to show that one of the fibers C_{t_0} of the fibration defined by (4.2) has infinitely many rational points. In what follows, we use detailed calculations to find a particular fiber that has infinitely many rational points for the case where $E(\mathbb{Q})$ has a point of order 6, or $E(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the case of higher torsion points, we can prove it similarly to the 6-torsion case. The actual calculations, however, become more complicated, and so we omit them here. □

6.1. *Elliptic curve with 6-torsion point*

Let us consider the universal elliptic curve having a point of order 6. It is given by the equation

$$y^2 + (1-\lambda)xy - \lambda(\lambda+1)y = x^3 - \lambda(\lambda+1)x^2.$$

When $\lambda \neq 0$, -1 or $-1/9$, this is an elliptic curve and the point $P = (0, 0)$ is a point of order 6. The line passing through P, $2P$ and $3P$ is given by $y = \lambda x$. Consider the surface in $\mathbb{A}^2 = \{(t, u, \delta)\}$ defined by (4.1) with the fibration $\pi : (t, u, \delta) \mapsto t$ and with parameter λ.

We show that the fiber at $t = \lambda$ has infinitely many rational points. First, we see that it has two points $(u, \delta) = (0, \pm\lambda^4(\lambda+1))$ corresponding to the line $y = \lambda x$ we mentioned above. Choosing one of them, say $(0, -\lambda^4(\lambda+1))$, as the origin, we can convert the equation of the fiber $C_\lambda = \pi^{-1}(\lambda)$ into Weierstrass form using the method described in Connell [7]:

$$\begin{aligned} C_\lambda\colon y^2 &+ (8\lambda + 2\lambda^2 + 2)xy - 4\lambda(7\lambda+1)(\lambda-2)(\lambda+1)^2 y \\ &= x^3 - 2\lambda(\lambda+1)(2\lambda^2 - 4 - \lambda)x^2 + 108\lambda^4(\lambda+1)^2 x \\ &\quad - 216\lambda^5(2\lambda^2 - 4 - \lambda)(\lambda+1)^3, \end{aligned} \tag{6.1}$$

where C_λ is an elliptic curve if and only if λ satisfies

$$\lambda(1+9\lambda)(2\lambda+1)(\lambda+1)(\lambda^4 + 3\lambda^3 + 4\lambda^2 + 1) \neq 0.$$

The point $(0, \lambda^4(\lambda+1))$ is sent to the point $\gamma_1 = (2\lambda(\lambda+1)(2\lambda^2 - 4 - \lambda), 0)$.

LEMMA 6.2. *For all $\lambda \in \mathbb{Q}$ such that C_λ is an elliptic curve, the point $(2\lambda(\lambda+1)(2\lambda^2-4-\lambda),0)$ is a point of infinite order. When $\lambda = -\frac{1}{2}$, C_λ is not an elliptic curve, but $(3/2,0)$ is still a point of infinite order.*

Proof. We consider C_λ as the curve defined over $\mathbb{Q}(\lambda)$, and calculate $n\gamma_1$, $n = 1,2,\ldots,10,12$. For all those n we observe that the denominator of the x-coordinate of $n\gamma_1$ does not vanish for any value of λ except for $\lambda = 0$. For $\lambda = -1/2$, the group is isomorphic to $\mathbb{Q}^\times$. Thus, it suffices to see that it is not a 2-torsion point. □

6.2. *Elliptic curves with $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ torsion*

The elliptic curve

$$y^2 = x(x+\mu^2)(x+\lambda^2)$$

is the universal elliptic curve with $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ torsion [18]. Without loss of generality, we may set $\mu = 1$ giving

$$E_\lambda : y^2 = x(x+1)(x+\lambda^2)$$

with 4-torsion points

$$\pm P = (\lambda, \pm\lambda(1+\lambda)), \quad \pm P' = (-\lambda, \pm\lambda(1-\lambda))$$

and 2-torsion points

$$[2]P = (0,0), \quad [2]P' = (-1,0), \quad Q = (-\lambda^2, 0).$$

For all λ different from $\lambda = 0, \pm 1$, E_λ is an elliptic curve.

E_λ is an elliptic curve for all λ different from $\lambda = 0, \pm 1$.

Consider the surface in $\mathbb{A}^2 = \{(t,u,\delta)\}$ defined by (4.1) with the fibration $\pi : (t,u,\delta) \mapsto t$ and with parameter λ. For this case, we show that the fiber $t = 1$ has infinitely many points. Setting $t = 1$ and $u = \lambda^2$, the line $y = x + \lambda^2$ passes through three torsion points

$$P = (\lambda, \lambda(1+\lambda)), \quad Q = (-\lambda^2, 0), \quad -P-Q = (-\lambda, -\lambda(1-\lambda)).$$

This triple of points gives rise to rational points $(\lambda^2, \pm 2\lambda^3(\lambda^2-1))$ in C_1, and we may proceed to convert the curve to Weierstrass form using the method described in Connell [7]. We then simplify it to obtain

$$\begin{aligned} C_1 : y^2 = {} & x^3 + 27\lambda^2(7\lambda^4 - \lambda^6 + 5\lambda^2 - 27)x \\ & + 27\lambda^2(2\lambda^{10} - 21\lambda^8 + 204\lambda^6 - 826\lambda^4 + 1242\lambda^2 - 729), \end{aligned}$$

and a rational point

$$(3(\lambda^4 + 16\lambda^2 + 3), \pm 27(7\lambda^4 + 10\lambda^2 - 1)).$$

The discriminant of C_1 is

$$-2^4 3^{12} \lambda^4 (\lambda-1)^2(\lambda+1)^2(3\lambda^4 - 14\lambda^2 + 27)^3.$$

LEMMA 6.3. *For all $\lambda \in \mathbb{Q}$ different from $0, \pm 1$, the curve C_1 is an elliptic curve and point $(3(\lambda^4 + 16\lambda^2 + 3), \pm 27(7\lambda^4 + 10\lambda^2 - 1))$ is a point of infinite order.*

Proof. Considering the fiber C_1 as a curve over $\mathbb{Q}(\lambda)$, this point is a point of infinite order, which can be verified by a height calculation. Just as the case of 6-torsion points, C_1 has infinitely many rational points for all $\lambda \neq 0$. For $\lambda = \pm 1$, the group is isomorphic to $\mathbb{Q}^\times$. Thus, it suffices to see that it is not a 2-torsion point. □

7. *An example – the curve $E\,37B$*

We now consider one of the curves of conductor 37 which is denoted $37B$ in Antwerp Table [3], and which has Weierstrass equation

$$E\,37B\colon y^2 + y = x^3 + x^2 - 3x + 1.$$

(In Cremona's tables [9], it is denoted 37b3.) We decided to study this example because the computations of [12] indicated an unusually large number of twists by cubic characters χ for which $L(E\,37B, 1, \chi) = 0$.

Substituting (x, y) by $(x + 1, y + 2x)$ in the equation above, we obtain another model of $E\,37B$:

$$E\colon y^2 + 4xy + y = x^3.$$

Note that $(0, 0)$ is a point of order 3. Intersecting the line $y = tx + u$ with this curve E, we obtain an affine model of $\bar{S}_E : \delta^2 = \Delta(u, t)$ with the fibration $(t, u, \delta) \mapsto t$. The fiber at $t = 0$ is a singular fiber given by the equation

$$\delta^2 = -u^2(27u^2 - 202u + 27).$$

This curve has a $\mathbb{Q}$-rational parametrization if and only if $-(27u^2 - 202u + 27)$ is a square for some rational value of u. It turns out that when $u = 7/9$, it becomes $(32/3)^2$. Using this solution, we can parametrize the fiber at $t = 0$:

$$u = \frac{7r^2 + 12r + 9}{9r^2 - 12r + 7}, \quad \delta = \frac{32(7r^2 + 12r + 9)(3r^2 + r - 3)}{(9r^2 - 12r + 7)^2},$$

where r is the parameter. This means that the cubic equation $u^2 + 4xu + u = x^3$ in x with u given by the above formula is a cyclic polynomial. Let ξ_r be a root of the cubic polynomial

$$\begin{aligned} F_r(Z) = Z^3 &- 4(7r^2 + 12r + 9)(9r^2 - 12r + 7)Z \\ &- 16(r^2 + 1)(7r^2 + 12r + 9)(9r^2 - 12r + 7). \end{aligned}$$

Then, $K_r = \mathbb{Q}(\xi_r, r)$ is a cyclic cubic extension of the field $\mathbb{Q}(r)$, and the point

$$P_r = \left(\frac{\xi_r}{9r^2 - 12r + 7}, \frac{7r^2 + 12r + 9}{9r^2 - 12r + 7} \right)$$

belongs to $E(K_r)$. A straightforward height calculation shows that P_r is a point of infinite order.

Let a and b be relatively prime integers. By Silverman's result [32], the specializations of P_r to $r = a/b$ also have infinite order except maybe for finitely many exceptions.

The discriminant of $K_r/\mathbb{Q}(r)$ is

$$2^{10}(7r^2 + 12r + 9)^2(9r^2 - 12r + 7)^2(3r^2 + r - 3)^2.$$

Let $K_{a/b}$ be the specialization of K_r with $r = a/b$. Then, $K_{a/b}$ has square discriminant dividing

$$2^{10}(7a^2 + 12ab + 9b^2)^2(9a^2 - 12ab + 7b^2)^2(3a^2 + ab - 3b^2)^2,$$

and the conductor of $K_{a/b}$ is the square root of its discriminant. We let

$$H_1 = 7a^2 + 12ab + 9b^2, \qquad H_2 = 9a^2 - 12ab + 7b^2, \qquad G = a^2 + b^2.$$

We note that the resultant of any pair of H_1, H_2 and G is supported only at the primes $2, 3$ and 37. Hence, if p is a rational prime $p \neq 2, 3$ or 37, which divides H_1H_2 to the first power, then $b^6F_{a/b}(Z)$ is an Eisenstein polynomial at p, and therefore p ramifies (totally) in $K_{a/b}/\mathbb{Q}$.

On the other hand, if p divides $3a^2 + ab - 3b^2$, then we have

$$H_1 H_2 - 27G^2 = 4(3a^2 + ab - 3b^2) \equiv 0 \bmod p$$

and thus

$$b^6 F_{a/b}(Z) \equiv Z^3 - 108\, G^2 Z - 432\, G^3 \equiv (Z + 6G)^2 (Z - 12G) \bmod p.$$

It follows that the completion of $K_{a/b}$ at the prime over p which contains $Z - 12G$ is $\mathbb{Q}_p$ and hence p splits completely in $K_{a/b}$.

Therefore, we see that the conductor of $K_{a/b}$ divides $2^{10} H_1 H_2$. But $H_1 H_2$ is a separable binary form of degree 4 which is primitive. It follows from Stewart and Top [**34**, Theorem 1] that there is a positive constant $C > 0$ such that that the number of square-free values less than X of $H_1 H_2$ is greater than $CX^{1/2}$ as X tends to infinity. We note that distinct square-free values of $H_1 H_2$ yield distinct fields $K_{a/b}$.

Therefore we have proved:

Theorem 7.1. *For the elliptic curve $E\,37B$, the number of cubic Dirichlet characters χ for which $L(E37B, 1, \chi) = 0$ satisfies*

$$\mathfrak{F}_E(3, X) = \#\{\chi \in \mathcal{X}(3) \mid \mathfrak{f}_\chi < X, L(E37B, 1, \chi) = 0\} \gg X^{1/2}.$$

We note that the calculations done above for the curve $E37B$ actually work for any elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point P of order 3 and which satisfies the condition below. We send the point P to $(0, 0)$ and express E in the form

$$y^2 + 3Uxy + Ty = x^3,$$

where $U, T \in \mathbb{Q}$. The fiber over $t = 0$, on the surface $\bar{S}_E$ takes the form

$$\delta^2 = -27u^2 (u^2 - (4U^3 - 2T)u + T^2).$$

This may be expressed as a conic in the variables $z = \delta/3u$ and $w = u + 2U^3 - T$

$$z^2 + 3w^2 = 12U^3 (U^3 - T).$$

This is a curve of genus zero and may be parameterized over $\mathbb{Q}$ if a single rational point can be found. This occurs if and only if the right-hand side is a norm from $\mathbb{Q}(\sqrt{-3})$, that is, if and only if $U(U^3 - T)$ is a norm from $\mathbb{Q}(\sqrt{-3})$.

These curves give examples for which $\mathfrak{F}_E(3, X) \gg X^{1/2}$, as mentioned in the introduction.

Acknowledgement. We wish to express our appreciation to the referee for his careful reading of the manuscript and for his useful comments.

References

1. A. Akbary, 'Non-vanishing of weight k modular L-functions with large level', *J. Ramanujan Math. Soc.* 14 (1999) 37–54.

2. J. Bertin, 'Réseaux de Kummer et surfaces de $K3$', *Invent. Math.* 93 (1988) 267–284.

3. B. J. Birch and W. Kuyk (ed.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics 476 (Springer, Berlin, 1975).

4. C. Breuil, B. Conrad, F. Diamond and R. Taylor, 'On the modularity of elliptic curves over **Q**: wild 3-adic exercises', *J. Amer. Math. Soc.* 14 (2001) 843–939 (electronic).

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

6. G. Chinta, 'Nonvanishing twists of $GL(2)$ L-functions', preprint, 11 pp.

7. I. Connell, 'Addendum to a paper of Harada and Lang', *J. Algebra* 145 (1992) 463–467.

8. B. Conrey, J. Keating, M. Rubinstein and N. Snaith, 'On the frequency of vanishing of quadratic twists of modular L-functions', *Number theory for the Millennium I* (eds M. A. Bennett, B. C. Berndt, N. Boston, H. G. Diamond, A. J. Hildebrand and W. Philipp, A.K. Peters Ltd, Natick, MA, 2002) 301–315.

9. J. E. Cremona, *Algorithms for modular elliptic curves* (Cambridge University Press, Cambridge, 1992).

10. C. David, J. Fearnley and H. Kisilevsky, 'On the vanishing of twisted L-functions of elliptic curves', *Experiment. Math.* 13 (2004) 185–198.

11. C. David, J. Fearnley and H. Kisilevsky, 'Vanishing of L-functions of elliptic curves over number fields', *Ranks of elliptic curves and random matrix theory*, London Mathematical Society Lecture Note Series 341 (Cambridge University Press, Cambridge, 2007) 247–259.

12. J. Fearnley, 'Vanishing and non-vanishing of L-series of elliptic curves twisted by dirichlet characters', PhD Thesis, Concordia University, 2001.

13. D. Goldfeld, 'Conjectures on elliptic curves over quadratic fields', *Number theory, Carbondale 1979* (Proceedings of the Southern Illinois Conference, Southern Illinois University, Carbondale, IL., 1979), Lecture Notes in Mathematics 751 (Springer, Berlin, 1979), 108–118.

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

15. K. Kato, 'p-adic Hodge theory and values of zeta functions of modular forms Cohomologies p-adiques et applications arithmétiques. III', Astérisque 295 (2004) 117–290.

16. T. Katsura, 'Generalized Kummer surfaces and their unirationality in characteristic p', *J. Fac. Sci., Univ. Tokyo, Sect. I A* 34 (1987) 1–41.

17. N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications 45 (American Mathematical Society, Providence, RI, 1999).

18. A. W. Knapp, *Elliptic curves* (Princeton University Press, Princeton, NJ, 1992).

19. V. A. Kolyvagin, 'Finiteness of $E(\mathbf{Q})$ and $\mathrm{Sh}(E, \mathbf{Q})$ for a subclass of Weil curves', *Izv. Akad. Nauk SSSR Ser. Mat.* 52 (1988) 522–540, 670–671.

20. M. Kuwata, 'Canonical height and elliptic $K3$ surfaces', *J. Number Theory* 36 (1990) 399–406.

21. L. Mai, 'The average analytic rank of a family of elliptic curves', *J. Number Theory* 45 (1993) 45–60.

22. 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.

23. L. Merel, 'Bornes pour la torsion des courbes elliptiques sur les corps de nombres', *Invent. Math* 124 (1996) 437–449.

24. D. Mumford, *Abelian varieties* (Oxford University Press, Oxford, 1970).

25. K. Ono and C. Skinner, 'Fourier coefficients of half-integral weight modular forms modulo l', *Ann. of Math.* (2) 147 (1998) 453–470.

26. M. Ram Murty, 'On simple zeros of certain L-series', *Number theory* (Proceedings of the First Conference of the Canadian Number Theory Association, Banff, AB, 1988) (de Gruyter, Berlin, 1990), 427–439.

27. M. Ram Murty and V. Kumar Murty, 'Mean values of derivatives of modular L-series', *Ann. of Math.* (2) 133 (1991) 447–475.

28. D. E. Rohrlich, 'The vanishing of certain Rankin–Selberg convolutions', *Automorphic forms and analytic number theory* (Proceedings of the Conference held at Montreal, Quebec, 1989) (Centre de recherches mathématiques, Montreal, Quebec, 1990) 123–133.

29. D. E. Rohrlich, 'Nonvanishing of L-functions and structure of Mordell–Weil groups', *J. reine angew. Math.* 417 (1991) 1–26.

30. A. J. Scholl, 'An introduction to Kato's Euler systems', *Galois representations in arithmetic algebraic geometry*, London Mathematical Society Lecture Note Series 254 (eds A. J. Scholl and R. L. Taylor; Cambridge University Press, Cambridge, 1998) 379–460.

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

32. J. H. Silverman, 'Heights and the specialization map for families of abelian varieties', *J. reine angew. Math.* 342 (1983) 197–251.

33. T. Stefanicki, 'Non-vanishing of L-functions attached to automorphic representations of GL(2) over $\mathbf{Q}$', *J. reine angew. Math.* 474 (1996) 1–24.

34. C. L. Stewart and J. Top, 'On ranks of twists of elliptic curves and power-free values of binary forms', *J. Amer. Math. Soc.* 8 (1995) 943–973.

35. R. Taylor and A. Wiles, 'Ring-theoretic properties of certain Hecke algebras', *Ann. of Math. (2)* 141 (1995) 553–572.

36. J.-L. Waldspurger, 'Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie', *Compositio Math.* 54 (1985) 173–242.

J. Fearnley and H. Kisilevsky
Department of Mathematics and Statistics and CICMA
Concordia University
1455 de Maisonneuve Blvd. West
Montréal, Québec
Canada H3G 1M8

jack@mathstat.concordia.ca

kisilev@mathstat.concordia.ca

M. Kuwata
Faculty of Economics
Chuo University
Hachioji-shi
Tokyo 192-0393
Japan

kuwata@tamacc.chuo-u.ac.jp