Collect. Math. **48**, 1–2 (1997), 31–39

Elliptic curves and special values of L-series

MASSIMO BERTOLINI*

Dipartimento di Matematica, Università di Pavia, Via Abbiategrasso 209, 27100 Pavia, Italy

ABSTRACT

Let $E/\mathbb{Q}$ be an elliptic curve, and let $L(E/\mathbb{Q}, s)$ be its Hasse-Weil L-series. In this paper, working under certain simplifying assumptions, we sketch a proof of the following result: $L(E/\mathbb{Q}, 1) \neq 0 \Longrightarrow E(\mathbb{Q})$ finite.

0. Let $E/\mathbb{Q}$ be an elliptic curve, and let $L(E/\mathbb{Q}, s)$ be its Hasse-Weil L-series. Following the methods of our joint paper with Henri Darmon [2], and working under certain simplifying assumptions, we sketch a proof of the following result:

$$L(E/\mathbb{Q}, 1) \neq 0 \Longrightarrow E(\mathbb{Q}) \text{ finite}\,.$$

Such a result was first proved for elliptic curves with complex multiplication by Coates and Wiles [3]. About ten years later, Kolyvagin [11], [12] found a proof for all modular elliptic curves. Kolyvagin's method uses in a crucial way the family of Heegner points defined over the anticyclotomic extensions of an imaginary quadratic field, and the limit formula of Gross-Zagier [8]. Kato [10] has announced a new proof of Kolyvagin's result, based on the construction of certain elements in the second K-group of modular function fields, defined over cyclotomic extensions of $\mathbb{Q}$. In [2], Darmon and I present a proof of the above statement for modular elliptic curves having at least one prime of multiplicative reduction (we actually assume semistability, to simplify matters), which differs in essential ways from the other

* Partially supported by GNSAGA (C.N.R.); M.U.R.S.T., national project "Geometria algebrica" and Human Capital and Mobility Programme of the European Community, under contract ERBCHRXCT940557.

known proofs. We do use Heegner points, but we relate them directly to special values of L-series rather than to first derivatives, using a slight generalization of a formula of Gross [6] instead of [8]. We do not have to compute global heights of Heegner points, but only a local term, corresponding to the image of the Heegner points in the group of connected components of E at a multiplicative prime. This computation is based on the work of Bas Edixhoven [5] on the specialization map from the jacobian of certain (analogues of) modular curves to its groups of connected components.

In this paper, we work in a somewhat simplified setting. This allows us to bypass some of the technical complications arising in [2], which contains more general results, without hiding the new features of the proofs. Therefore, we hope that this note may also serve as an introduction to [2].

1. We assume throughout the paper that $E/\mathbb{Q}$ is an elliptic curve of squarefree conductor, containing at least one prime p of non-split multiplicative reduction, and that $L(E/\mathbb{Q},1)$ is non-zero. Write the conductor of E as Np. (Since the sign of the functional equation for $L(E/\mathbb{Q},s)$ is $+1$, observe that E has a non-split multiplicative prime whenever the number of prime divisors of the conductor is even).

The fundamental work of Wiles [19] and Taylor-Wiles [17] implies that E is modular, i.e., there exists a non-constant morphism of abelian varieties defined over $\mathbb{Q}$

$$\varphi : J_0(Np) \to E,$$

where $J_0(Np)$ is the jacobian of the modular curve $X_0(Np)$ of level Np.

By a result of Waldspurger [18] – see also chapter 6 of [14] and [15] for different proofs – we can find an imaginary quadratic field $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ such that p is inert in K, all primes dividing N are split in K, and $L(E/K,1)$ is non-zero.

Write K_{nr} for the Hilbert class field of K, and K_n for the ring class field of K of conductor p^{n+1}, $n \geq 0$. The fields K_{nr} and K_n are abelian extensions of K, and Galois extensions of dihedral type of $\mathbb{Q}$. Let $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ denote the maximal order of K, and let $\mathcal{O}_n = \mathbb{Z} + \mathbb{Z}p^{n+1}\omega$ be the order of K of conductor p^{n+1}. Upon fixing an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$, we may view K_{nr} and K_n as the subfields of $\mathbb{C}$ generated over K by the values $j(\mathcal{O}_K)$ and $j(\mathcal{O}_n)$ of the modular j-function. Let $G_n := \mathrm{Gal}(K_n/K_{\mathrm{nr}})$ and $\Delta := \mathrm{Gal}(K_{\mathrm{nr}}/K)$. The group G_n is cyclic of order $e_n := (p+1)p^n$. Since p is inert in K, it is totally split in K_{nr}/K, and the primes of K_{nr} above p are totally ramified in K_n.

In this setting, we can construct a compatible collection of Heegner points over the extensions K_n as follows. A point on the modular curve $X_0(Np)$ defined over a

number field F corresponds to the isomorphism class of a triple (A, C, C') defined over F, where A is an elliptic curve and C and C' are cyclic subgroups of A of orders p and N, respectively. For any prime q dividing N, choose a prime $\mathfrak{q}$ of K above it, and let $\mathfrak{n} = \prod \mathfrak{q}$. Define $A_n := \mathbb{C}/\mathcal{O}_n$, $C_n := \mathbb{Z}/p\mathbb{Z} \cdot [p^n\omega]$ and $C'_n := (\mathfrak{n} \cap \mathcal{O}_n)^{-1}/\mathcal{O}_n$, where $[p^n\omega]$ denotes the point of order p of A_n corresponding to the complex number $p^n\omega$. Thus, A_n is an elliptic curve with complex multiplication by $\mathcal{O}_n$, and the triple (A_n, C_n, C'_n) corresponds to a point β_n of $X_0(Np)$. The theory of complex multiplication shows that the Heegner point β_n is defined over K_n. Denote by δ_n the divisor class $(\beta_n) - (w_{Np}\beta_n)$ in $J_0(Np)$, w_{Np} being the Fricke involution on $X_0(Np)$. Finally, write $\alpha_n \in E(K_n)$ for the image of $(-1)^n\delta_n$ by the modular parametrization φ. (Note that w_{Np} acts as -1 on the normalized cusp form attached to E, since the root number of $L(E/\mathbb{Q}, s)$ is $+1$).

The next Lemma states the compatibility properties of the Heegner points we shall need in the sequel of the paper. Let τ be the complex conjugation corresponding to our fixed embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$. Given a finite Galois extension M/L with Galois group G, let $\mathrm{Norm}_{M/L} \in \mathbb{Z}[G]$ be the norm operator $\sum_{\sigma \in G} \sigma$.

Lemma 1.1

(i) For $n \geq 0$, we have $\mathrm{Norm}_{K_{n+1}/K_n}\alpha_{n+1} = \alpha_n$.
(ii) We have $\mathrm{Norm}_{K_n/K_{\mathrm{nr}}}\alpha_n = 0$.
(iii) The equality $\tau\alpha_n = -g\alpha_n$ holds for some $g \in \mathrm{Gal}(K_n/K)$.

Proof. We have the equality of divisors on $X_0(Np)$

$$U_p\beta_n = \sum_{\sigma \in \mathrm{Gal}(K_{n+1}/K_n)} \beta_{n+1}^{\sigma}\,,$$

where U_p denotes the Hecke correspondence at p on $X_0(Np)$. Since p is a non-split multiplicative prime for E, the operator U_p acts as -1 on E. Part (i) follows. As for part (ii), note that the divisor on $X_0(Np)$

$$\sum_{\sigma \in \mathrm{Gal}(K_0/K_{\mathrm{nr}})} \beta_0^{\sigma}$$

is equal to the pull-back of the point $(\mathbb{C}/\mathcal{O}_K, \mathfrak{n}^{-1}/\mathcal{O}_K)$ of $X_0(N)$ by the covering map

$$\pi \circ w_p : X_0(Np) \to X_0(N)\,.$$

Here w_p is the Atkin-Lehner involution at p on $X_0(Np)$ and π is the natural projection of $X_0(Np)$ onto $X_0(N)$. Therefore, δ_n belongs to the old part of $J_0(Np)$,

and the claim follows. Finally, Proposition 2.6 of [1] states that $\tau\beta_n = gw_N\beta_n$ for a g in $\mathrm{Gal}(K_n/K)$. Since the root number of $L(E/\mathbb{Q}, s)$ is $+1$ and p is a non-split multiplicative prime, the involution w_N acts as -1 on E. This concludes the proof of Lemma 1.1. □

2. Given a generator γ_n for the cyclic group G_n, define Kolyvagin's derivative operator $D_n := \sum_{i=1}^{e_n-1} i\gamma_n^i \in \mathbb{Z}[G_n]$. A direct computation yields the equality

$$(\gamma_n - 1)D_n = e_n - \mathrm{Norm}_{K_n/K_{\mathrm{nr}}}. \tag{1}$$

By abuse of notation, let $D_n\alpha_n$ denote also the image in $E(K_n)/p^nE(K_n)$ of the point $D_n\alpha_n$ of $E(K_n)$. By Lemma 1.1, $D_n\alpha_n$ belongs to $(E(K_n)/p^nE(K_n))^{G_n}$.

In order to simplify the exposition, we assume from now on that $E_p(K_0)$ is zero, and that p is an odd prime which does not divide the class number of K and the order of the groups of connected components of the Néron model of E at the primes dividing N. (These assumptions can be avoided at the cost of introducing some technical complications in the arguments: see [2]).

Since $E_p(K_0) = 0$ and K_n/K_0 is an abelian p-extension, we also have that $E_p(K_n) = 0$ for all $n \geq 1$. Thus, multiplication by p^n induces the exact sequence of G_n-modules

$$0 \to E(K_n) \xrightarrow{p^n} E(K_n) \to E(K_n)/p^nE(K_n) \to 0\,.$$

Upon taking G_n-cohomology, we find

$$0 \to E(K)/p^nE(K) \to (E(K_n)/p^nE(K_n))^{G_n} \to H^1(G_n, E(K_n))_{p^n} \to 0\,.$$

Let d_n be the image in $H^1(G_n, E(K_n))_{p^n}$ of $D_n\alpha_n$ by the coboundary map. More explicitly, d_n is the cohomology class corresponding to the cocycle

$$G_n \ni \sigma \mapsto \frac{(\sigma - 1)D_n\alpha_n}{p^n}\,. \tag{2}$$

By the formula (1), $((\gamma_n - 1)D_n\alpha_n)/p^n$ is equal to $(p+1)\alpha_n$. More generally, if $\sigma = \gamma_n^i$ for $i = 1, \ldots, e_n$, then $((\sigma - 1)D_n\alpha_n)/p^n$ is equal to $(p+1)(\gamma_n^{i-1} + \ldots + 1)\alpha_n$. When convenient, we shall identify d_n with its image in $H^1(K_{\mathrm{nr}}, E)_{p^n}$ by the inflation map.

It turns out that the class d_n restricts to zero at all primes not equal to p, and that its restriction at p is related to the special value $L(E/K, 1)$.

We begin with some preliminaries. Write $K_{n,p}$ for $K_n \otimes \mathbb{Q}_p = \oplus_{\mathfrak{p}|p} K_{n,\mathfrak{p}}$, and $U_{n,p}$ for the units of $K_{n,p}$. Our functors on abelian categories will always be additive,

so that for example $E(K_{n,p})$ stands for $\oplus_{\mathfrak{p}|p} E(K_{n,\mathfrak{p}})$. If $\mathfrak{p}$ is as before a prime of K_n above p, write $\Phi_{\mathfrak{p}}$ for the group of connected components of the Néron model of E over the ring of integers of $K_{n,\mathfrak{p}}$, and let

$$\Phi_n := \oplus_{\mathfrak{p}|p} \Phi_{\mathfrak{p}}.$$

By Tate's theory of p-adic uniformization ([16], ch. V), Φ_n is defined by an exact sequence

$$0 \to U_{n,p} \to E(K_{n,p}) \to \Phi_n \to 0\,. \tag{3}$$

It follows that $\Phi_{\mathfrak{p}}$ is a cyclic group of order $r_n := e_n \cdot \mathrm{ord}_p(q_E)$, q_E being Tate's p-adic period of E, and that Φ_n is isomorphic as a Δ-module to the group ring $(\mathbb{Z}/r_n\mathbb{Z})[\Delta]$. The G_n-cohomology of (3) yields a map from $H^1(G_n, E(K_{n,p}))_{p^n}$ to $\mathrm{Hom}(G_n, \Phi_n)_{p^n}$, and, by evaluating homomorphisms on the fixed generator γ_n of G_n, also a map

$$j_n : H^1(G_n, E(K_{n,p}))_{p^n} \to (\Phi_n)_{p^n}. \tag{4}$$

(One checks directly that j_n is injective, and it can be shown that j_n is in fact an isomorphism. We will not need these facts in the sequel of the paper).

The next proposition describes the localization properties of the class d_n. Given a rational prime ℓ, let $\mathrm{res}_\ell : H^1(K_n, E)_{p^n} \to H^1(K_{n,\ell}, E)_{p^n}$ be the natural restriction map, where $K_{n,\ell}$ denotes $K_n \otimes \mathbb{Q}_\ell$.

Proposition 2.1

(i) If $\ell \neq p$, then $\mathrm{res}_\ell d_n = 0$.
(ii) The local class $\mathrm{res}_p d_n$ belongs to $H^1(G_n, E(K_{n,p}))_{p^n}$, and we have

$$j_n(\mathrm{res}_p d_n) = (p+1)\bar{\alpha}_n\,,$$

where $\bar{\alpha}_n$ denotes the natural image of α_n in Φ_n.

Proof. The local cohomology group $H^1(G_n, E(K_{n,\ell}))$ is trivial for all primes ℓ of good reduction for E, since K_n/K_{nr} is unramified outside p. The same is true for the primes $\ell \mid N$, by our assumption on the groups of connected components at the primes dividing N. This proves part (i). Part (ii) follows from the definition of j_n and the explicit description of d_n given in (2). □

If M is a Δ-module and m is an element of M, we write $M^{\mathbf{1}}$ and $m^{\mathbf{1}}$ as shorthands for $\mathrm{Norm}_{K_{\mathrm{nr}}/K} M \subset M^{\Delta}$ and $\mathrm{Norm}_{K_{\mathrm{nr}}/K} m \in M^{\mathbf{1}}$.

Since p does not divide the class number of K under our assumptions, the inflation-restriction sequence identifies the groups $H^1(K,E)_{p^n}$ and $H^1(K_{\mathrm{nr}},E)^{\Delta}_{p^n}$, and similarly for their local counterparts. Thus, we may view the class $d_n^{\mathbf{1}}$ as an element of $H^1(K,E)_{p^n}$.

Proposition 2.2

Assume that $(p+1)\bar{\alpha}_n^{\mathbf{1}} \in (\Phi_n)^{\Delta}_{p^n}$ is non-zero for some $n \geq 0$. Then $E(\mathbb{Q})$ is finite.

Proof. By Proposition 2.1,

$$j_n(\mathrm{res}_p d_n^{\mathbf{1}}) = (p+1)\bar{\alpha}_n^{\mathbf{1}}\,.$$

In view of the compatibility properties of the Heegner points stated in Lemma 1.1, $(p+1)\bar{\alpha}_n^{\mathbf{1}}$ is non-zero for some $n \geq 1$, and the order of $(p+1)\bar{\alpha}_{n+1}^{\mathbf{1}}$ is p times the order of $(p+1)\bar{\alpha}_n^{\mathbf{1}}$. Hence, the order of $\mathrm{res}_p d_n^{\mathbf{1}}$ goes to infinity with n.

Since $D_n^{\tau} = -D_n$ modulo $e_n\mathbb{Z}[G_n]$, part (iii) of Lemma 1.1 shows that τ acts as $+1$ on the class $d_n^{\mathbf{1}}$. It follows directly that $d_n^{\mathbf{1}}$ belongs to $H^1(\mathbb{Q},E)_{p^n}$, and thus $\mathrm{res}_p d_n^{\mathbf{1}}$ belongs to $H^1(\mathbb{Q}_p,E)_{p^n}$.

Write $\hat{E}(\mathbb{Q}_p)$ for the p-adic completion $\varprojlim_n E(\mathbb{Q}_p)/p^n E(\mathbb{Q}_p)$ of $E(\mathbb{Q}_p)$. In our setting, one checks that $\hat{E}(\mathbb{Q}_p)$ is a free $\mathbb{Z}_p$-module of rank 1. The local duality theorem of Tate ([13], ch. 1) states the existence of a perfect pairing

$$\langle\ ,\ \rangle_p : \hat{E}(\mathbb{Q}_p) \times H^1(\mathbb{Q}_p,E)_{p^\infty} \to \mathbb{Q}_p/\mathbb{Z}_p\,.$$

It follows that $H^1(\mathbb{Q}_p,E)_{p^\infty}$ is isomorphic to the p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$, and hence it is generated by the classes $\mathrm{res}_p d_n^{\mathbf{1}}$ with n varying.

Since the global classes $d_n^{\mathbf{1}} \in H^1(\mathbb{Q},E)_{p^n}$ restrict to zero at all primes $\ell \neq p$, the global duality theorem of class field theory ([13], ch. 1) implies that the local classes $\mathrm{res}_p d_n^{\mathbf{1}}$ pair to zero with the natural image of $E(\mathbb{Q})$ in $\hat{E}(\mathbb{Q}_p)$. But $E(\mathbb{Q})$ maps to $\hat{E}(\mathbb{Q}_p)$ with finite kernel, equal to its torsion subgroup. Therefore, $E(\mathbb{Q})$ has to be a finite group. □

3. Combining the next theorem with Proposition 2.2 completes our argument.

Theorem 3.1

The element $(p+1)\bar{\alpha}_n^{\mathbf{1}} \in (\Phi_n)^{\Delta}_{p^n}$ is non-zero for n sufficiently large.

Sketch of proof.

Step 1. By definition, the Heegner point α_n is (up to sign) the image by the modular parametrization φ of the Heegner divisor class $\delta_n = (\beta_n) - (w_{Np}\beta_n)$ in $J_0(Np)(K_n)$. For a prime $\mathfrak{p}$ of K_n above p, let $\Psi_\mathfrak{p}$ be the group of connected components of the Néron model of $J_0(Np)$ over the ring of integers of $K_{n,\mathfrak{p}}$, and let $\Psi_n := \oplus_{\mathfrak{p}|p}\Psi_\mathfrak{p}$. It is crucial to determine the image in Ψ_n of the divisor class δ_n.

We first recall Grothendieck's description of Ψ_n. It is known that the reduction modulo p of (a suitable model of) the curve $X_0(Np)$ is equal to the union of two copies of $X_0(N)_{/\mathbb{F}_p}$, crossing at the supersingular points. Let $s_1, \ldots, s_h$ be these supersingular points. They correspond to supersingular elliptic curves in characteristic p, equipped with a cyclic N-isogeny. Let w_i denote one half the order of the group of automorphisms of the modulus s_i. Write $\mathbb{M}$, resp. $\mathbb{M}^0$ for the free $\mathbb{Z}$-module of divisors, resp. degree-zero divisors with integral coefficients supported on the points s_i. Define a non-degenerate pairing

$$\langle\ ,\ \rangle : \mathbb{M}^0 \times \mathbb{M}^0 \to \mathbb{Z} \tag{5}$$

to be the restriction to $\mathbb{M}^0$ of the diagonal pairing on $\mathbb{M}$ given by $\langle s_i, s_j\rangle := \delta_{ij} w_i$. Let $\psi : \mathbb{M}^0 \to (\mathbb{M}^0)^\vee$ be the map from $\mathbb{M}^0$ to its $\mathbb{Z}$-dual $(\mathbb{M}^0)^\vee$ induced by the pairing (5). If $\mathfrak{p}$ is a prime of K_n above p, the points $s_1, \ldots, s_h$ can be identified with the double points of the fiber at $\mathfrak{p}$ of $X_0(Np)$, and $\mathbb{M}^0$ can be identified with the character group $\mathbb{M}^0_\mathfrak{p}$ of the maximal torus at $\mathfrak{p}$ of the Néron model of $J_0(Np)$. Write $s_{i,\mathfrak{p}}$, $\psi_\mathfrak{p}$, etc. for the objects corresponding to s_i, ψ, etc. via the above identifications.

A theorem of Grothendieck ([9], thm. 11.5) states that the group $\Psi_\mathfrak{p}$ of connected components at $\mathfrak{p}$ fits in the canonical exact sequence

$$0 \to \mathbb{M}^0_\mathfrak{p} \xrightarrow{e_n} \mathbb{M}^0_\mathfrak{p} \xrightarrow{\psi_\mathfrak{p}} (\mathbb{M}^0_\mathfrak{p})^\vee \to \Psi_\mathfrak{p} \to 0, \tag{6}$$

where the first map is multiplication by $e_n = (p+1)p^n$.

Observe that the Heegner points β_n and $w_{Np}\beta_n$ reduce modulo $\mathfrak{p}$ to supersingular points, say $s_{i_0,\mathfrak{p}}$ and $s_{i_1,\mathfrak{p}}$. For, β_n corresponds to an elliptic curve A_n with complex multiplication by the order $\mathcal{O}_n$ of K, together with a certain level Np-structure. Since p is inert in K, the reduction of A_n at $\mathfrak{p}$ is supersingular. Similarly for $w_{Np}\beta_n$. It follows that the divisor class δ_n reduces modulo $\mathfrak{p}$ to $\mu_\mathfrak{p} := s_{i_0,\mathfrak{p}} - s_{i_1,\mathfrak{p}} \in \mathbb{M}^0_\mathfrak{p}$.

We can prove that the natural image of δ_n in $\Psi_\mathfrak{p}$ corresponds via the sequence (6) to the element $\psi_\mathfrak{p}(\mu_\mathfrak{p})$ of $(\mathbb{M}^0_\mathfrak{p})^\vee$.

More precisely, the work of Edixhoven [5] shows that the image of δ_n in $\Psi_\mathfrak{p}$ is equal to the image via (6) of $\psi_\mathfrak{p}(m_{i_0} s_{i_0,\mathfrak{p}} - m_{i_1} s_{i_1,\mathfrak{p}})$, where the constants m_{i_0} and

m_{i_1} can be described as follows. Let $\mathcal{O}_\mathfrak{p}$ be the ring of integers of the completion of the maximal unramified extension of $K_{n,\mathfrak{p}}$. Write $\mathrm{F} : A_n \to A_n^{(p)}$ for the Frobenius morphism over $\mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$, with A_n as before. Then m_{i_0} is defined to be the largest positive integer $m \leq e_n$ such that A_n and $A_n^{(p)}$ are isomorphic over the ring $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^m\mathcal{O}_\mathfrak{p}$. The constant m_{i_1} is defined similarly. Our claim amounts to proving that m_{i_0} and m_{i_1} are both equal to 1. In other words, A_n and $A_n^{(p)}$ are not isomorphic over $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^2\mathcal{O}_\mathfrak{p}$, and similarly for the curves corresponding to $w_{Np}\beta_n$. This follows from Gross' theory of quasi-canonical liftings [7], by looking at the formal groups of A_n and $A_n^{(p)}$. We refer the interested reader to [5] and [2] for more details on these somewhat technical arguments.

Step 2. We can use the above description of the image $\bar{\delta}_n$ in Ψ_n of the divisor δ_n to show that $(p+1)\bar{\alpha}_n^{\mathbf{1}}$ is non-zero for n large enough. Equivalently, by the proof of Proposition 2.2, to show that the order of $\bar{\alpha}_n^{\mathbf{1}}$ is unbounded with n varying.

Write $\mathbb{T}$ for the algebra generated over $\mathbb{Z}$ by the Hecke operators acting on $J_0(Np)$, and f for the normalized cusp form with rational coefficients attached to E. Let π_f be the projector in $\mathbb{T}\otimes\mathbb{Q}$ corresponding to f, and let n_f be the smallest positive integer such that the operator $\eta_f := n_f\pi_f$ belongs to $\mathbb{T}$. Note that Ψ_n is a $\mathbb{T}[\Delta]$-module. Let $\Psi_n^{f,\mathbf{1}}$ be $\eta_f\Psi_n^{\mathbf{1}}$, and let $\bar{\delta}_n^{f,\mathbf{1}} \in \Psi_n^{f,\mathbf{1}}$ be $\eta_f\bar{\delta}_n^{\mathbf{1}}$. One checks directly that the order of $\bar{\alpha}_n^{\mathbf{1}}$ is unbounded with n varying if and only if the same is true for the order of $\bar{\delta}_n^{f,\mathbf{1}}$.

The fact that the order of $\bar{\delta}_n^{f,\mathbf{1}}$ is unbounded follows from a slight generalization of a formula of Gross (see [6] and [4]) for the special value $L(E/K,1)$, combined with Step 1. Consider the $\mathbb{T}[\Delta]$-module $\mathbb{M}_n := \oplus_{\mathfrak{p}|p}\mathbb{M}_\mathfrak{p}$, and define $\mathbb{M}_n^{f,\mathbf{1}}$ to be $\eta_f\mathbb{M}_n^{\mathbf{1}}$. The pairing (5) induces a pairing

$$\langle\ ,\ \rangle_{f,\mathbf{1}} : \mathbb{M}_n^{f,\mathbf{1}} \times \mathbb{M}_n^{f,\mathbf{1}} \to \mathbb{Z}\,.$$

If $\mu := (\mu_\mathfrak{p})_{\mathfrak{p}|p}$ is the natural image of δ_n in $\mathbb{M}_n$, write $\mu^{f,\mathbf{1}}$ for $\eta_f\mu^{\mathbf{1}}$. Then,

$$L(E/K,1) = C\cdot\langle\mu^{f,\mathbf{1}},\mu^{f,\mathbf{1}}\rangle_{f,\mathbf{1}}$$

for a non-zero constant C independent of n (which can be described explicitly). Since in our setting $L(E/K,1)$ is non-zero, this concludes the argument. □

References

1. M. Bertolini and H. Darmon, Heegner points on Mumford-Tate curves, *Invent. Math.,* to appear.
2. M. Bertolini and H. Darmon, A rigid analytic Gross-Zagier formula and arithmetic applications (With an appendix by B. Edixhoven), submitted.
3. J. Coates and A. Wiles, On the Birch and Swinnerton-Dyer conjecture, *Invent. Math.* **39** (1977), 223–251.
4. H. Daghigh, McGill PhD Thesis, in preparation.
5. B. Edixhoven, Appendix to [2].
6. B.H. Gross, *Heights and special values of L-series,* CMS Conference Proceedings, H. Kisilevsky, J. Labute, Eds., Vol. 7, 1987.
7. B.H. Gross, On canonical and quasi-canonical liftings, *Invent. Math.* **84** (1986), 321–326.
8. B.H. Gross and D. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320.
9. A. Grothendieck, *Groupes de monodromie en geometrie algébrique,* SGA 7 I, ch. IX, LNM 281, Springer.
10. K. Kato, Forthcoming work.
11. V.A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves, *Izv. Akad. Nauk. SSSR Ser. Mat.* **52** (1988), 522–540; English transl. in Math. USSR Izv. 32, 1989.
12. V.A. Kolyvagin, Euler Systems, The Grothendieck Festschrift, P. Cartier, et al., Eds., vol. II, *Progr. in Math.* **87**, Birkhäuser, (1990), 435–483.
13. J.S. Milne, *Arithmetic duality theorems,* Perspective in Math., Academic Press, 1986.
14. M.R. Murty and V.K. Murty, Non-vanishing of L-functions and applications, 1995, submitted.
15. V.K. Murty and T. Stefanicki, Average values of quadratic twists of modular L-functions, submitted.
16. J.H. Silvermann, *Advanced topics in the arithmetic of elliptic curves,* GTM 151, Springer, 1994.
17. R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, *Ann. of Math.* **141**, n. 3 (1995), 553–572.
18. J-L. Waldspurger, Correspondances de Shimura et quaternions, preprint.
19. A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141**, n. 3 (1995), 443–551.