Invent. math. 110, 123–146 (1992)

Inventiones mathematicae

A refined conjecture of Mazur-Tate type for Heegner points

Henri Darmon
School of Mathematics, Princeton University, Princeton, NJ 08544, USA

Oblatum 19-XII-1991, & 25-II-1992

Contents

Summary. In [MT1], Mazur and Tate present a "refined conjecture of Birch and Swinnerton-Dyer type" for a modular elliptic curve E. This conjecture relates congruences for certain integral homology cycles on $E(\mathbf{C})$ (the modular symbols) to the arithmetic of E over $\mathbf{Q}$. In this paper we formulate an analogous conjecture for E over a suitable imaginary quadratic field K, in which the role of the modular symbols is played by Heegner points. A large part of this conjecture can be proved, thanks to the ideas of Kolyvagin on the Euler system of Heegner points. In effect the main result of this paper can be viewed as a generalization of Kolyvagin's result relating the structure of the Selmer group of E over K to the Heegner points defined in the Mordell–Weil groups of E over ring class fields of K. An explicit application of our method to the Galois module structure of Heegner points is given in Sect. 2.2.

1 Preliminaries

Let E be a modular elliptic curve. There is a morphism

$$\phi : X_0(N) \to E$$

defined over $\mathbf{Q}$, where N is the arithmetic conductor of E and $X_0(N)$ is the algebraic curve which classifies pairs of elliptic curves related by a cyclic N-isogeny.

The pull-back of a Néron differential ω on E is an eigenform f of weight 2 on $X_0(N)$ with Fourier expansion given by

$$\phi^*(\omega) = c(\phi) \sum_{n=1}^{\infty} a_n q^n dq/q, \quad q = e^{2\pi i \tau}.$$

The Fourier expansion is normalized so that $a_1 = 1$, and $c(\phi)$ is the *Manin constant* associated to the modular parametrization ϕ. The Hasse–Weil L-function $L(E/\mathbf{Q}, s)$ can be identified with the L-series attached to f,

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

From Hecke's theory one knows that $L(f, s)$ has an Euler product and a functional equation relating its value at s to its value at $2 - s$. The parity of the order of vanishing of the L-function at the central point $s = 1$ can be read off from the functional equation. More precisely, let ε denote the eigenvalue of the Atkin–Lehner involution w_N acting on f. Then $L(f, s)$ vanishes to odd order at $s = 1$ if $\varepsilon = 1$, and to even order if $\varepsilon = -1$.

Fix a quadratic imaginary field K of discriminant D in which all primes dividing N are split. If $N = p_1^{e_1} \cdots p_k^{e_k}$, one may choose for each p_i an ideal $\mathscr{P}_i$ of K above it, and set

$$\mathscr{N} = \mathscr{P}_1^{e_1} \cdots \mathscr{P}_k^{e_k}.$$

Given a positive integer T which is relatively prime to ND, let $\mathscr{O}_T$ denote the order of K of conductor T. Because T is prime to N, the ideal $\mathscr{O}_T \cap \mathscr{N}$ is invertible, and the natural projection of complex tori

$$\mathbf{C}/\mathscr{O}_T \to \mathbf{C}/(\mathscr{O}_T \cap \mathscr{N})^{-1}$$

corresponds to a cyclic N-isogeny of elliptic curves. Hence it can be identified with a point of $X_0(N)$. By the theory of complex multiplication, this point is defined over K_T, the ring class field of K of conductor T. Let $\alpha(T)$ denote the image of this point in $E(K_T)$ by the modular parametrization ϕ.

2 Statement of the results

2.1 The conjecture of Mazur Tate type

Given a square-free integer $S = l_1 \cdots l_t$ prime to ND, write

$$G_S = \mathrm{Gal}(K_S/K_1), \quad \Gamma_S = \mathrm{Gal}(K_S/K).$$

Define the *regularized* Heegner points by the formulas

$$\beta_S = \sum_{T \mid S} \mu(T)\alpha(T), \quad \beta_S^{\omega} = \sum_{T \mid S} \mu(T)\omega(T)\alpha(T),$$

where μ is the Möbius function, and ω is the quadratic Dirichlet character associated to K. Let $A(E, S)$ (resp. $A^{\omega}(E, S)$) denote the formal resolvent associated to the Heegner point β_S (resp. β_S^{ω}):

$$A(E, S) := \sum_{\sigma \in \Gamma_S} \sigma\beta_S \otimes \sigma \in E(K_S) \otimes \mathbf{Z}[\Gamma_S] ,$$

$$A^{\omega}(E, S) := \sum_{\sigma \in \Gamma_S} \sigma\beta_S^{\omega} \otimes \sigma^{-1} \in E(K_S) \otimes \mathbf{Z}[\Gamma_S] .$$

The role of the θ-element of [MT1] will be played by the element

$$\theta'(E, S) := A(E, S) \otimes_{\mathbf{Z}[\Gamma_S]} A(E, S)^{\omega} = \sum_{\sigma, \tau \in \Gamma_S} \sigma\beta_S \otimes \tau\beta_S^{\omega} \otimes \sigma\tau^{-1};$$

it belongs to the triple tensor product $E(K_S)^{\otimes 2} \otimes \mathbf{Z}[\Gamma_S]$.

For technical reasons it will be convenient to replace $\mathbf{Z}$ by a subring Z of $\mathbf{Q}$ and view $\theta'(E, S)$ as belonging to $E(K_S)^{\otimes 2} \otimes Z[\Gamma_S]$ by extending scalars from $\mathbf{Z}$ to Z. For the time being we make no assumptions on Z. Let I denote the augmentation ideal in the group ring $Z[\Gamma_S]$, and let r denote the rank of the Mordell– Weil group of E over K. We conjecture the following:

Conjecture 2.1 (order of vanishing) *For any Z, the element $\theta'(E, S)$ belongs to the subgroup $E(K_S)^{\otimes 2} \otimes I^{r-1}$ of $E(K_S)^{\otimes 2} \otimes Z[\Gamma_S]$.*

Remarks. 1. This statement is analogous to the part of the Birch Swinnerton-Dyer conjecture which predicts that the order of vanishing of the complex L-function of E over K is equal to r. Our conjecture involves $r - 1$, and not r, because of the philosophy that $\theta'(E, S)$ should mirror the behavior of $L'(E/K, s)$ at $s = 1$. A justification for this philosophy is provided by the analytic formula of Gross and Zagier [GZ]. More precisely, let $h: E(K_S)^{\otimes 2} \to \mathbf{R}$ be the canonical Néron–Tate height over K_S, and let $\chi: \Gamma_S \to \mathbf{C}^*$ be a complex character of Γ_S, extended by linearity to the group ring of $Z[\Gamma_S]$. Combining h and χ gives rise to a natural linear map:

$$h \otimes \chi: E(K_S)^{\otimes 2} \otimes Z[\Gamma_S] \to \mathbf{C} .$$

Theorem 2.2 (Gross Zagier) *Suppose that $S = 1$ so that K_S is the Hilbert class field of K. Then*

$$h \otimes \chi(\theta'(E, S)) = c(\phi)^2 [K_S : K] \sqrt{\mathrm{Disc}(K)} \frac{L'(E/K, \chi, 1)}{\iint_{E(\mathbf{C})} \omega \wedge \bar{\omega}} .$$

2. Conjecture 2.1 is inspired by the refined conjectures of Birch Swinnerton-Dyer type introduced by Mazur and Tate. For an explanation of these conjectures, the reader may consult the fundamental reference [MT1], or [D2]. It seems that such refined conjectures provide a congenial setting for the Euler Systems of Kolyvagin to express themselves: the properties of such Euler systems (relations between special elements and arithmetic) are naturally formulated as conjectures of Mazur Tate type. This program has been carried out in the simpler case of cyclotomic units [D1], where one finds conjectural formulas which are a slight generalization of those of Thaine [Th].

3. What of the original Mazur Tate conjectures? At present, still no proof is known. What one might need in this case is a cyclotomic Euler system, consisting in a compatible system of cohomology classes

$$c_{n, p} \in H^1(\mathbf{Q}(\mu_n), T_p(E)) .$$

In a remarkable recent development, Kato [Ka] has succeeded in constructing precisely such an Euler system, using elements in K_2 of modular curves constructed from Steinberg symbols of Siegel units. He has also succeeded in relating his Euler system to the special values of the complex L-function $L(f, \chi, 1)$ twisted by Dirichlet characters, and hence to modular symbols. It seems possible that this work of Kato will shed light on the Mazur Tate conjectures.

Assuming Conjecture 2.1, we can project $\theta'(E, S)$ to an element $\tilde{\theta}'(E, S)$ in the group $E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r)$. This element plays the role of the leading coefficient in the refined Birch and Swinnerton-Dyer conjecture. To make a conjecture about its value, let

$$u = \tfrac{1}{2} \# (\mathcal{O}_K^*), \quad \tau = \# E(K)_{\text{tor}} .$$

Given a prime p dividing N, let m_p denote the order of the group of connected components in the special fiber at p for the Néron model of E over $\text{Spec}(\mathbf{Z})$. Let

$$m = \prod_{p|N} m_p .$$

Finally, let B denote the "Birch Swinnerton-Dyer constant"

$$B = c(\phi) \cdot u \cdot m \cdot \sqrt{\# Ш(E/K)} \cdot \tau^{-1} .$$

It is conjectured (cf. [GZ, p. 311]) that B is an integer and that, when $E(K)/E(K)_{\text{tor}}$ is generated by a single element P, the following identity is true in $E(K)/E(K)_{\text{tor}}$:

$$\text{Trace}_{K_1'/K}(\alpha(1)) = \pm BP. \tag{1}$$

This conjecture follows by comparing the Gross Zagier formula with the classical Birch and Swinnerton-Dyer conjecture.

Now we define a regulator term belonging to $E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r)$. Let

$$E_S(K) = \ker(E(K) \to (\otimes_{v|S} E(k_v)) \oplus (\oplus_v E/E_0(K_v))) ,$$

and let J_S be the order of the cokernel of this map. In [MT1, MT2], Mazur and Tate define a height pairing

$$\langle \ \rangle_S : E(K) \times E_S(K) \to I/I^2 .$$

(In fact, their height pairing takes values in G_S, but we use here the isomorphism $I/I^2 \simeq G_S$.)

Suppose first that $E(K)$ is free over $\mathbf{Z}$, and let $P_1, \ldots, P_r$ (resp. $Q_1, \ldots, Q_r$) denote integral bases for $E(K)$ (resp. $E_S(K)$) which induce compatible orientations. The *partial regulator* R_{ij} in I^{r-1}/I^r is defined to be the determinant of the ijth minor of the pairing matrix $(\langle P_i, Q_j \rangle_S)$ with entries in I/I^2. The regulator R_S is given by the formula

$$R_S = \sum_{i,j=1}^{r} (-1)^{i+j} P_i \otimes Q_j \otimes R_{ij} . \tag{2}$$

When $E(K)$ is not free, one normalizes this definition as in [MT1, p. 735]: choose finite index subgroups A and B of $E(K)$ and $E_S(K)$ which are free, and define the regulator $R(A, B)$ by picking bases $P_1, \ldots, P_r$ and $Q_1, \ldots, Q_r$ for A and B, and using the formula (2). If the multiplication by the product of indexes $j = [E(K) : A][E_S(K) : B]$ induces an isomorphism on the abelian group $E(K)^{\otimes 2} \otimes I^{r-1}/I^r$, then one defines

$$R_S = R(A, B) j^{-1} .$$

This quantity, when it is defined, does not depend on the choice of A and B. Furthermore, suitable A and B for which j is invertible exist, say, if $r > 1$ and τ is prime to the order of Γ_S, or if τ is invertible in the ring Z. From now on to simplify we assume that Z contains $\mathbf{Z}[\tau^{-1}]$. Under this assumption we can state the main conjecture:

Conjecture 2.3 *Assume that* $\tau^{-1} \in Z$. *Then*

1. *The element* $\theta'(E, S)$ *belongs to* $E(K_S)^{\otimes 2} \otimes I^{r-1}$.
2. *The leading coefficient* $\tilde{\theta}'(E, S) \in E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r)$ *belongs to the image of the natural map*

$$t : E(K)^{\otimes 2} \otimes (I^{r-1}/I^r) \to E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r) .$$

3. $\tilde{\theta}'(E, S) = t(c(\phi)^2 \cdot u^2 \cdot \#\text{Ш}(E/K) \cdot J_S R_S)$.

Remark. 1. When $r = 1$ and $S = 1$, we have:

$$J_1 R_1 = m^2 \tau^{-2} P \otimes P ,$$

where P is a generator (modulo torsion) for $E(K)$. Note that this equation is true in $E(K) \otimes Z$ regardless of the choice of P, since τ is invertible in Z. Hence Conjecture 2.3 follows in this case from the conjectured equation (1), which is itself a consequence of the classical Birch and Swinnerton-Dyer conjecture.

2. The conjecture we have formulated is compatible under the norm from K_S to K_T, when T is a divisor of S (cf. Sect. 3.2). This is the motivation for working with the regularized Heegner points.

We now state the main results of this paper which give evidence for conjecture 2.3.

To do this we suppose that the following primes are invertible in Z:

1. The primes 2 and 3.
2. All primes $p < (r-1)/2$.
3. All primes p such that $\mathrm{Gal}(\mathbf{Q}(E_{p^\infty})/\mathbf{Q})$ is not isomorphic to $\mathbf{GL}_2(\mathbf{Z}_p)$.
4. All primes p which divide m.

Note that assumption 3 forces τ to be invertible in Z. The set of primes satisfying condition 3 (and hence, all four of the above) is a finite set if and only if E has no complex multiplications, by a result of Serre [Se].

Complex conjugation acts on the Mordell–Weil group $E(K)$. Let r^+ and r^- denote the ranks of the $+$ and $-$ eigencomponents $E(K)^+$ and $E(K)^-$ of $E(K)$ under this involution, and let

$$\rho = \max(r^+, r^-) - 1, \quad \text{if } r^+ \neq r^- ,$$

$$\rho = r^+ = r^- = r/2, \quad \text{if } r^+ = r^- .$$

Note that the order of vanishing of $L(E/K, s)$ is odd; hence by the Birch Swinnerton-Dyer conjecture, one expects that r is odd, so that r^+ and r^- should have opposite parities and equality $r^+ = r^-$ should never hold in our situation.

Theorem 2.4 (Main result) *Suppose that* S *is a product of primes which are inert in* K. *Then* $\theta'(E, S)$ *belongs to the subgroup* $E(K_S)^{\otimes 2} \otimes I^{2\rho}$ *of* $E(K_S)^{\otimes 2} \otimes Z[G]$.

Since $2\rho \geqq r - 1$ (with equality holding if and only if $|r^+ - r^-| = 1$), Theorem 2.4 implies part 1 of conjecture 2.3 about the order of vanishing, slightly weakened because of the assumptions which were made on Z.

If $|r^+ - r^-| > 1$, then $2\rho > r - 1$, and the Theorem 2.4 proves more than what is predicted by Conjecture 2.3. Can one give a conceptual account of this extra vanishing? At least one can show that when $|r^+ - r^-| > 1$, the regulator term R_S vanishes (cf. Proposition 5.12). However, in that case, the leading coefficient should be defined to be the projection of $\theta'(E, S)$ in the group $E(K_S)^{\otimes 2} \otimes (I^{2\rho}/I^{2\rho+1})$. We were not able to supply a prediction, even a conjectural one, for the value of this leading coefficient, except when $2\rho = r - 1$.

Assume now that $|r^+ - r^-| = 1$. Given a prime p, let $\tilde{\theta}'(E, S)_{(p)}$ denote the reduction modulo p of $\tilde{\theta}'(E, S)$, i.e., the natural image of $\tilde{\theta}'(E, S)$ in the group $E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r) \otimes \mathbf{Z}/p\mathbf{Z}$. Let t_p be the natural map induced by t,

$$t_p : E(K)^{\otimes 2} \otimes (I^{r-1}/I^r) \otimes \mathbf{Z}/p\mathbf{Z} \to E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r) \otimes \mathbf{Z}/p\mathbf{Z} .$$

Note that the module $(I^{r-1}/I^r) \otimes \mathbf{Z}/p\mathbf{Z}$ is trivial unless p divides the order of Γ_S and p is not invertible in the ring Z. A p-descent argument establishes the following:

Theorem 2.5 1. *$\tilde{\theta}'(E, S)_{(p)}$ belongs to the image of t_p.*
2. *If p divides $\#\,Ш(E/K)J_S$, then $\tilde{\theta}'(E, S)_{(p)} = 0$.*

2.2 Application to the Galois module structure of Heegner points

In stating the following result, we do not strive for the greatest generality of what can be shown by our methods, but only present an illustrative special case.

An abelian extension L of K is said to be of dihedral type if it is normal over $\mathbf{Q}$ and the involution τ in $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathrm{Gal}(L/K)$ by $\tau\sigma\tau^{-1} = \sigma^{-1}$. Let L be a dihedral type extension of K with Galois group $G = \mathbf{Z}/p\mathbf{Z}$, where p is a prime which does not divide $6m$, and satisfies

$$\mathrm{Gal}(\mathbf{Q}(E_{p^\alpha})/\mathbf{Q}) = \mathrm{Aut}(T_p(E)) .$$

Assume that L is ramified only at primes of $\mathbf{Q}$ which are inert in $K/\mathbf{Q}$. Then L can be embedded in a ring class field of K, whose conductor over K is a product of inert primes. Let $\tilde{L}$ denote the smallest such field, and let $\alpha \in E(L)$ be the trace of the Heegner point in $E(\tilde{L})$ defined in section 1. The $\mathbf{Z}[G]$-module $\mathscr{E}(L)$ generated by α is a quotient of a free $Z[G]$-submodule of rank 1 of $E(L)$. The work of Kolyvagin tells us that the position of the module $\mathscr{E}(L)$ in $E(L)$ is strongly related to the arithmetic of $E(L)$, a fact which was foreshadowed by the analytic formula of Gross and Zagier.

Denote by $\mathscr{E}(L)_{\mathbf{C}}$ the complex representation of G attached to $\mathscr{E}(L)$, i.e., the image of $\mathscr{E}(L) \otimes \mathbf{C}$ in $E(L) \otimes \mathbf{C}$. Given a prime $l \neq p$, let $\mathscr{E}(L)_l$ denote the image of $\mathscr{E}(L)$ in $E(L) \otimes \bar{\mathbf{F}}_l$, where $\bar{\mathbf{F}}_l$ is the algebraic closure of the finite field $\mathbf{F}_l$ with l elements.

The representation $\mathscr{E}(L)_{\mathbf{C}}$ splits into a direct sum of eigencomponents $\mathscr{E}(L)^\chi_{\mathbf{C}}$ attached to complex characters χ of G. By applying the methods of Kolyvagin one can show (cf. [BD]) that

$$\text{if } \mathscr{E}(L)^\chi_{\mathbf{C}} \neq 0 \text{ then } \dim_{\mathbf{C}}(E(L) \otimes \mathbf{C})^\chi = 1 .$$

Likewise one has a decomposition of the representation $\mathscr{E}(L)_l$ into eigencomponents $\mathscr{E}(L)^\chi_l$ associated this time to $\bar{\mathbf{F}}_l$-valued characters of G. From the methods of Kolyvagin one expects (at least if l is large enough) that

$$\text{if } \mathscr{E}(L)^\chi_l \neq 0 \text{ then } \dim_{\bar{\mathbf{F}}_l}(\mathrm{Sel}_l(E/L))^\chi = 1 ,$$

where $\mathrm{Sel}_l(E/L)$ is the l-Selmer group. Evidence for this is given in [BD].

In both cases the module of Heegner points tells us whether the ranks of certain eigenspaces in Mordell Weil groups or l-Selmer groups are one or not.

The situation changes greatly when one considers the module $\mathscr{E}(L)_p$, the image of $\mathscr{E}(L)$ in $E(L) \otimes \mathbf{F}_p$. This module no longer decomposes into eigenspaces for the G-action, since the representation is a modular representation: the group ring $\mathbf{F}_p[G]$ is isomorphic to the local ring $\mathbf{F}_p[\varepsilon]/(\varepsilon^p)$. Let

$$r_p^{\pm} = \dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/K)^{\pm} ,$$

where the superscripts of $+$ and $-$ denote the $+$ and $-$ eigenspaces for the action of complex conjugation on $\mathrm{Sel}_p(E/K)$. Let

$$\rho_p = \max(r_p^+, r_p^-) - 1, \quad \text{if } r_p^+ \neq r_p^- ,$$

$$\rho_p = r_p^+ = r_p^- = r_p/2, \quad \text{if } r_p^+ = r_p^- .$$

Theorem 2.6 $\dim_{\mathbf{F}_p}(\mathscr{E}(L)_p) \leqq p - \rho_p$.

Thus the $\mathbf{F}_p$-dimension of $\mathscr{E}(L)_p$ reflects some quantitative information about the rank of the p-Selmer group of E over K. This result leads to several natural questions:

1 Is the bound of Theorem 2.6 sharp? We can only provide a conjectural answer when $Ш_p = 1$ and when $|r_p^+ - r_p^-| = 1$ by relying on the philosophy of conjecture 2.3.

2. What is the nature of the module of G-invariants $(\mathscr{E}(L)_p)^G$? This module is necessarily non-trivial and one-dimensional if $(\mathscr{E}(L)_p)$ is non-trivial. In many cases one can show that it gives rise to elements in the Selmer group $\mathrm{Sel}_p(E/K)$. Can one predict what these elements are?

The remainder of this paper is devoted to the proofs of Theorems 2.4, 2.5, and 2.6. In Sect. 3 we state an explicit result about congruences for certain combinations of Heegner points over ring class fields (Theorem 3.15 of Sect. 3.3), and show that this result implies Theorem 2.4. Section 4 is devoted to the construction and study of certain cohomology classes made from Heegner points which generalize those that were studied by Kolyvagin. Finally, the Sect. 5 is devoted to a proof of Theorem 3.15.

3 Restatement of the results

3.1 Calculus of abelian group rings

Let G be a finite abelian group. Given an element σ of order n_σ in G, define the derivative operator in the group ring $Z[G]$ by the formula:

$$\mathrm{D}_\sigma^k = \sum_{i=0}^{n_\sigma - 1} \binom{i}{k} \sigma^i .$$

If $G = \langle \sigma \rangle$ is cyclic, then D_σ^0 is the norm element in the group ring and D_σ^1 is the derivative operator used by Kolyvagin.

One can decompose G as a product of cyclic groups

$$G = G_1 \times \cdots \times G_t ,$$

where the order n_i of G_i is a multiple of the order n_j of G_j whenever $i < j$. This decomposition is not unique, but the orders n_i are well-defined. Choose a generator σ_i for each G_i, and view these generators as elements of G. Given a multi-index $\underline{k} = (k_1, \ldots, k_t)$ of integers, the partial derivative operator $D_{\underline{k}}$ in the group ring $\mathbf{Z}[G]$ is defined to be

$$D_{\underline{k}} = D_{\sigma_1}^{k_1} \cdots D_{\sigma_t}^{k_t} .$$

Let M be a $Z[G]$-module, and let a be an element of M. We wish to study the resolvent element

$$\sum_{\sigma \in G} \sigma a \otimes \sigma \in M \otimes_Z Z[G].$$

The following gives a Taylor expansion formula for this resolvent element around the augmentation ideal.

Theorem 3.1 (Taylor formula)

$$\theta = \sum_{\underline{k}} D_{\underline{k}} a \otimes (\sigma_1 - 1)^{k_1} \cdots (\sigma_t - 1)^{k_t} ,$$

where the sum is taken over all t-tuples $\underline{k} = (k_1, \ldots, k_t)$ *of positive integers.*

The proof is a routine computation, and we omit it. Observe that although the sum is taken over an infinite set, all but finitely many of the terms are zero: the partial derivative $D_{\underline{k}}$ vanishes once one of the k_i is greater than n_i.

Let p be a prime that is not invertible in Z. The natural inclusion of $\mathbf{Q}$ in $\mathbf{Q}_p$ induces a map $Z \to \mathbf{Z}_p$. Let I_p denote the augmentation ideal in the group ring $\mathbf{Z}_p[G]$, and let θ_p denote the image of θ in $M \otimes \mathbf{Z}_p[G]$.

Lemma 3.2 *The element* θ *belongs to* $M \otimes I^r$ *if and only if* θ_p *belongs to* $M \otimes I_p^r$ *for all primes p which are not invertible in Z.*

Proof. The successive quotients I^k/I^{k+1} are finite abelian groups whose orders are divisible only by the primes which are not invertible in Z. Since an element in a finite abelian group is trivial if and only if it maps to zero in each p-primary part of the group, the result follows.

Let $\varepsilon_p : \mathbf{Z}_p[G] \to \mathbf{Z}_p$ denote the augmentation map on the group ring.

Lemma 3.3 *Assume that x and y belong to the group ring* $\mathbf{Z}_p[G]$ *and that the product xy belongs to* I_p^r. *If* $\varepsilon_p(y)$ *is invertible in* $\mathbf{Z}_p$, *then x belongs to* I_p^r.

Proof. Multiplication by y induces an isomorphism on I_p^k/I_p^{k+1} for all k.

Lemma 3.4 *If* σ *is of order prime to p, then* $(\sigma - 1)$ *belongs to* I_p^r *for all r.*

Proof. Let n be the order of σ. Then

$$0 = \sigma^n - 1 = n(\sigma - 1) + \binom{n}{2}(\sigma - 1)^2 + \cdots + (\sigma - 1)^2 .$$

The right-hand side is equal to

$$(\sigma - 1)\left(n + \binom{n}{2}(\sigma - 1) + \cdots + (\sigma - 1)^n\right).$$

Since the second factor maps to n by ε_p, and n belongs to $\mathbf{Z}_p^*$, the result follows from Lemma 3.3.

Lemma 3.5 *If the order of σ is q, a power of p, then $q(\sigma - 1)$ belongs to I_p^p.*

Proof. As in the proof of Lemma 3.4 one finds

$$q(\sigma - 1) + \binom{q}{2}(\sigma - 1)^2 + \cdots + (\sigma - 1)^q = 0 .$$

Hence

$$q(\sigma - 1)\left(1 + \binom{q}{2}\Big/ q(\sigma - 1) + \binom{q}{3}\Big/ q(\sigma - 1)^2 + \cdots + \binom{q}{p-1}\Big/ q(\sigma - 1)^{p-2}\right)$$
$$= -\binom{q}{p}(\sigma - 1)^p + \cdots + (\sigma - 1)^q .$$

Applying Lemma 3.3, one finds that $q(\sigma - 1)$ belongs to I_p^p.

Lemma 3.6 *Let q be the maximal power of p dividing the order of σ. Then $q(\sigma - 1)$ belongs to I_p^p.*

Proof. Write $\sigma = \sigma_1\sigma_2$, where σ_1 is of order q and σ_2 is of order prime to p. The result follows from the identity

$$(\sigma - 1) = (\sigma_1 - 1)(\sigma_2 - 1) + (\sigma_1 - 1) + (\sigma_2 - 1)$$

combined with Lemmas 3.4 and 3.5.

Given $\underline{k} = (k_1, \ldots, k_t)$, let

$$n(\underline{k}) = \gcd_{k_i > 0} n_i .$$

(Recall that the n_i are the orders of the σ_i). Let $n_p(\underline{k})$ denote the maximal power of p dividing $n(\underline{k})$.

Lemma 3.7 *Suppose $r \leqq p$. The element θ_p belongs to I_p^r if for all t-tuples $\underline{k} = (k_1, \ldots, k_t)$ with $k_1 + \cdots + k_t < r$, we have*

$$D_{\underline{k}} a \equiv 0 \pmod{n_p(\underline{k})}.$$

Proof. This follows from the Taylor formula 3.1 together with Lemma 3.6.

We say that an element a in a $\mathbf{Z}$-module M is divisible by an integer n if there exists a' in M with $a = na'$.

Lemma 3.8 *Suppose that all primes which are strictly less than r are invertible in Z. Then the element θ in $Z[G]$ belongs to I^r if*

$$n(\underline{k}) \text{ divides } \mathrm{D}_{\underline{k}} a \text{ for all } \underline{k} = (k_1, \ldots, k_t) \text{ with } k_1 + \cdots + k_t < r .$$

Proof. Combine Lemmas 3.2 and 3.7.

We conclude this section with a property of the derivatives D_σ^k that will be useful later:

Lemma 3.9 *If σ is of order n, then*

$$(\sigma - 1)\mathrm{D}_\sigma^k = \binom{n}{k} - \sigma \mathrm{D}_\sigma^{k-1} .$$

This is proved by a straightforward computation.

3.2 Generalities on Heegner points

We give ourselves fixed embeddings $\bar{\mathbf{Q}} \to \mathbf{C}$ and $\bar{\mathbf{Q}} \to \bar{\mathbf{Q}}_p$ for every prime p. Complex conjugation $\mathrm{Frob}_\infty \in \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ acts by Galois automorphisms on any Galois extension of $\mathbf{Q}$. Similarly, the Frobenius element at p, Frob_p acts on any Galois extension of $\mathbf{Q}$ which is unramified at p.

We recall some standard facts on Heegner points over ring class fields of K. We do not strive for the greatest generality, but only state the results in the form which we shall need in the proofs. A more thorough discussion can be found in [Gr1] or [Gr4].

Let $\mathscr{S}$ be the set of square-free integers prime to ND which are products of primes which are inert in K. For all $T \in \mathscr{S}$ we are given the following data:

1. An abelian extension K_T of K, the ring class field of K associated to the order of conductor T. It is ramified only at the places of K which lie above the primes dividing T. Thus K_1 is the Hilbert class field of K. One writes $G = \mathrm{Gal}(K_1/K)$, $G_T = \mathrm{Gal}(K_T/K_1)$ and $\Gamma_T = \mathrm{Gal}(K_T/K)$.
2. The Heegner point $\alpha(T)$ in $E(K_T)$.

Writing $T = l_1 \ldots l_s$, the extension K_T is a compositum of the fields K_{l_i} which are linearly disjoint over K_1. Hence there is a canonical direct product decomposition

$$G_T = G_{l_1} \times \cdots \times G_{l_s}$$

which gives inclusions $G_S \subset G_T$ and $\Gamma_S \subset \Gamma_T$ for all divisors S of T. We will implicitly identify elements of G_S with their images in G_T. For any S dividing T, the partial norm operator $\mathbf{N}_S$ in the group ring $\mathbf{Z}[G_T]$ is defined by

$$\mathbf{N}_S = \mathbf{N}_{G_S} = \sum_{\sigma \in G_S} \sigma .$$

For each prime l, choose a generator σ_l of G_l, and write D_l^k for the partial derivative $\mathrm{D}_{\sigma_l}^k$. Thus D_l^1 is the derivative operator studied by Kolyvagin. These operators acts on the field K_T and on the Mordell–Weil group $E(K_T)$ in the natural way.

Given $S \in \mathscr{S}$ and l a prime in $\mathscr{S}$ which is prime to S, let λ denote a prime of K above l and let $\sigma_{\lambda,S} \in \Gamma_S$ be the Frobenius automorphism associated to λ.

Proposition 3.10 $\mathbf{N}_l(\alpha(Sl)) = a_l \alpha(S)$.

Proof. See [Gr4, p. 240, Proposition 3.7].

Proposition 3.11 $\alpha(Sl) \equiv \sigma_{\lambda,S}\alpha(S) \pmod{\lambda'}$, *where* λ' *is any prime of* K_{Sl} *above* λ.

Proof. See [Gr4, p. 240, Proposition 3.7].

Propositions 3.10 and 3.11 make up the axioms of an Euler system for Heegner points in the sense of Kolyvagin [Ko3].

The action of complex conjugation Frob_∞ on the Heegner points is given by the following proposition:

Proposition 3.12 $\mathrm{Frob}_\infty \alpha(T) = \varepsilon\sigma_0\alpha(T) + (\text{torsion})$ *for some* $\sigma_0 \in \Gamma_T$.

(Recall that ε is the eigenvalue for the operator w_N acting on f; it is opposite to the sign in the functional equation for $L(f, s)$.)

Proof. See [Gr4, p. 243, Proposition 5.3].

We make a brief digression concerning the compatibility of Conjecture 2.3 under norms. Writing $T = Sl$, let μ_l denote the map

$$\mu_l : E(K_T)^{\otimes 2} \otimes \mathbf{Z}[\Gamma_T] \to E(K_T)^{\otimes 2} \otimes \mathbf{Z}[\Gamma_S]$$

induced by the homomorphism $\Gamma_T \to \Gamma_S$.

Proposition 3.13 *$\mu_l(\tilde{\theta}'(E, T)) = \# E(k_l) \cdot \tilde{\theta}'(E, S)$, where $k_l = \mathcal{O}_K/l\mathcal{O}_K$.*

Proof. By Proposition 3.10 combined with a direct computation, the behavior of the regularized Heegner points β_T and β_T^ω under norms is given by:

$$\mathbf{N}_l \beta_T = (l + 1 - a_l)\beta_S, \quad \beta_T^\omega = (l + 1 + a_l)\beta_S^\omega .$$

The result now follows from the formula

$$\# E(k_l) = (l + 1 - a_l)(l + 1 + a_l) .$$

On the other hand the naturality of the Mazur Tate pairing implies that

$$\mu_l \circ \langle\ ,\ \rangle_T = \langle\ ,\ \rangle_S$$

on $E(K) \times E_T(K)$, so that

$$\mu_l(J_T R_T) = \# E(k_l) \cdot J_S R_S .$$

Hence Conjecture 2.3 is compatible with the map μ_l when l is inert in $K/\mathbf{Q}$. A similar compatibility can be shown when l is split in $K/\mathbf{Q}$. Hence in particular, Conjecture 2.3 in the case $r = 1$ follows from the classical Birch Swinnerton-Dyer conjecture, thanks to the formula of Gross and Zagier.

The compatibility under norms is the reason for using the regularized Heegner points β_S instead of the simpler points $\alpha(S)$ in the definition of $\theta'(E, S)$.

3.3 A divisibility theorem for Heegner points

In this section, we state a theorem on congruences for certain combinations of Heegner points over ring class fields. Using the results of Sects. 3.1 and 3.2, we show that it implies Theorem 2.4.

Let q be a power of a prime p which is not invertible in the ring Z. Let

$$\mathcal{L}_q = \{l \text{ rational prime, } \mathrm{Frob}_l = \mathrm{Frob}_\infty \text{ in } K(\mu_q)/\mathbf{Q}\} .$$

Lemma 3.14 *The prime l belongs to $\mathcal{L}_q$ if and only if it is inert in $K/\mathbf{Q}$ and q divides $l + 1$.*

Any finitely generated $\mathbf{Z}/q\mathbf{Z}$-module M can be decomposed as

$$M = (\mathbf{Z}/q\mathbf{Z})^{r_q(M)} \times M',$$

where the exponent of M' divides q strictly. The integer $r_q(M)$ does not depend on the decomposition.

Let $\mathrm{Sel}_q(M)$ be the q-Selmer group for E/K which arises out of the descent for the isogeny of multiplication by q. Complex conjugation Frob_∞ acts on $\mathrm{Sel}_q(M)$ and splits it into $+$ and $-$ eigenspaces since q is odd. Let r_q^+ and r_q^- denote the values of $r_q(\mathrm{Sel}_q(E/K)^+)$ and $r_q(\mathrm{Sel}_q(E/K)^-)$ respectively. Let

$$\rho_q = \max(r_q^+, r_q^-) - 1, \quad \text{if } r_q^+ \neq r_q^- ,$$
$$\rho_q = r_q^+ = r_q^- = r_q/2, \quad \text{if } r_q^+ = r_q^- .$$

The class group C of K can be decomposed (non-canonically) as a product

$$C = C' \times \langle \xi_1 \rangle \times \cdots \times \langle \xi_a \rangle ,$$

where q does not divide the exponent of C' and each ξ_i is of order a power of p which is greater or equal to q.

Given $S = l_1 \cdots l_s$ a product of distinct primes in $\mathscr{L}_q$, let $\mathrm{D}_{\underline{k}}$ be the partial derivative operator in the group ring $Z[\Gamma_S]$ of the form:

$$\mathrm{D}_{\underline{k}} = \mathbf{N}_{C'} \mathrm{D}_{\xi_1}^{j_1} \cdots \mathrm{D}_{\xi_a}^{j_a} \mathrm{D}_{l_1}^{k_1} \cdots \mathrm{D}_{l_s}^{k_s},$$

where $\underline{k} = (j_1, \ldots, j_a, k_1, \ldots, k_s)$ is an $(a+s)$-tuple of positive integers. One defines the support of $\mathrm{D}_{\underline{k}}$ to be the integer S, its conductor S' to be the product of the l_i with $k_i > 0$, and its order to be $k = j_1 + \cdots + j_a + k_1 + \cdots + k_s$. There is an obvious partial ordering on the set of partial derivatives with support S. Given $\underline{k}' = (j_1', \ldots, j_a', k_1', \ldots, k_s')$, one says that $\mathrm{D}_{\underline{k}'}$ is less than $\mathrm{D}_{\underline{k}}$ if

$$j_t' \leqq j_t, \quad k_t' \leqq k_t \quad \forall t .$$

Theorem 3.15 *Let q be a power of a prime which is not invertible in Z. If* $\mathrm{order}(\mathrm{D}_{\underline{k}}) < \rho_q$, *then*

$$\mathrm{D}_{\underline{k}} \alpha(S) \equiv 0 \pmod{q} .$$

Claim 3.16 *Theorem* 3.15 *implies Theorem* 2.4.

Proof. Let $S = l_1 \cdots l_t$ be a product of primes which are inert in K. Let $\mathrm{D}_{\underline{k}}$ be a partial derivative of support S and conductor S' which is of order $< \rho$. We can write

$$\mathrm{D}_{\underline{k}} = \mathrm{D}' \mathbf{N}_{S/S'} ,$$

where D' has support S'. By Proposition 3.10,

$$\mathrm{D}_{\underline{k}} \alpha(S) = \left(\prod_{l | S/S'} a_l \right) \mathrm{D}' \alpha(S') .$$

Fix a prime p which is not invertible in Z and let q be the largest power of p dividing $n(\underline{k})$. By definition all the primes dividing S' belong to $\mathscr{L}_q$. Since $\rho \leqq \rho_q$, we can apply Theorem 3.15 to conclude that $\mathrm{D}'\alpha(S') \equiv 0 \pmod{n_p(\underline{k})}$. Hence $n(\underline{k})$ divides $\mathrm{D}_{\underline{k}} \alpha(S)$ whenever $\mathrm{order}(\mathrm{D}_{\underline{k}}) < \rho$. By Lemma 3.8 it follows that the resolvent element

$$\theta_S = \sum_{\sigma \in \Gamma_S} \sigma \alpha(S) \otimes \sigma \in E(K_S) \otimes Z[\Gamma_S]$$

belongs to $E(K_S) \otimes I^{\rho}$. Similarly the elements θ_T for all T dividing S belong to $E(K_S) \otimes I^{\rho}$, as well as the elements θ_T^* which are obtained by applying to θ_T the involution sending $\sigma \in \Gamma_S$ to σ^{-1}. The elements $A(E, S)$ and $A(E, S)^{\omega}$ introduced in Sect. 2.1 can be expressed as combinations of the θ_T and the θ_T^* over the integral group ring $Z[\Gamma_S]$. Hence they belong to $E(K_S) \otimes I^{\rho}$ as well. Therefore

$$\theta'(E, S) \text{ belongs to } E(K_S)^{\otimes 2} \otimes I^{2\rho} .$$

4 The Heegner cohomology classes

4.1 More on derivatives

Let $q = p^M$ be a power of a prime p which is not invertible in Z.

Lemma 4.1 1. $(\sigma_l - 1)\mathrm{D}_l^k = \binom{l+1}{k} - \sigma_l \mathrm{D}_l^{k-1}$.

2. *For all* $0 < k < p$,

$$(\sigma_l - 1)\mathrm{D}_l^k \equiv -\sigma_l \mathrm{D}_l^{k-1} \pmod{q},$$

and a similar formula hold for the $D_{\xi_j}^k$.

Proof. Part 1 is a restatement of Lemma 3.9. For part 2, one uses the fact that q divides $l+1$ (Lemma 3.14), and hence the binomial coefficient $\binom{l+1}{k}$.

The group $\mathrm{Gal}(K_S/\mathbf{Q})$ is a semi-direct product of $\mathrm{Gal}(K/\mathbf{Q}) = \langle \mathrm{Frob}_\infty \rangle$ with Γ_S. Complex conjugation Frob_∞ acts on Γ_S by the formula:

$$\mathrm{Frob}_\infty \sigma \mathrm{Frob}_\infty^{-1} = \sigma^{-1}.$$

Extending this action to the group ring $\mathbf{Z}/q\mathbf{Z}[\Gamma_S]$, one has the following action of Frob_∞ on $\mathrm{D}_{\underline{k}}$:

Lemma 4.2 $\mathrm{Frob}_\infty \mathrm{D}_{\underline{k}} \mathrm{Frob}_\infty^{-1} = (-1)^k \mathrm{D}_{\underline{k}} + (\textit{lower order derivatives})$.

Proof. It suffices to show this for a partial derivative operator of the form D_l^k. In this case, one has

$$\mathrm{Frob}_\infty \mathrm{D}_l^k \mathrm{Frob}_\infty^{-1} - (-1)^k \mathrm{D}_l^k = \sum_{i=0}^{\#G_l} f(i)\sigma_l^i, \tag{3}$$

where $f(i) = \binom{\#G_l - i}{k} - (-1)^k \binom{i}{k}$. The function $f(i)$ is the reduction mod q of a polynomial with rational coefficients taking integral values at integral arguments. Moreover the degree of f is strictly less than k. The $\mathbf{Z}$-module of all such polynomial functions is spanned by the $\binom{i}{k'}$ with $k' < k$. Hence the left-hand side of (3) can be expressed as an integral combination of partial derivatives of lower order.

4.2 The Heegner cohomology classes

Fix a product S of primes in $\mathscr{L}_q$, and let $\mathrm{D}_{\underline{k}}$ be a fixed partial derivative in the group ring $Z[\Gamma_S]$. Define a set $\mathscr{L}_{q,E}$ of rational primes as follows:

$$\mathscr{L}_{q,E} = \{l \text{ rational prime} \mid l \nmid NDp \text{ and } \mathrm{Frob}_l = \mathrm{Frob}_\infty \text{ in } K(E_q)/\mathbf{Q}\}.$$

Lemma 4.3 *A prime* l *not dividing* NDp *belongs to* $\mathscr{L}_{q,E}$ *if and only if it belongs to* $\mathscr{L}_q$ *and in addition* q *divides* a_l.

Proof. If $l \in \mathscr{L}_{q,E}$, we have the equalities of the minimal polynomials of Frob_l and Frob_∞ acting on E_q:

$$x^2 - a_l x + l = x^2 - 1 \pmod{q}.$$

The lemma follows by equating coefficients of these two polynomials.

Lemma 4.4 *If* L *is a solvable extension of* $\mathbf{Q}$, *then* $E_q(L) = 0$.

Proof. Suppose $E_p(L) \neq 0$. Since $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts transitively on the p-torsion in E, this implies that L contains all of the p-torsion points, which is impossible since $\mathbf{GL}_2(\mathbf{Z}/p\mathbf{Z})$ is not solvable when $p > 3$.

Choose a prime l which satisfies the following conditions:

$$l \not| ND \cdot p \cdot S, \quad \mathrm{Frob}_l = \mathrm{Frob}_\infty \text{ in } K_S(E_q)/\mathbf{Q} .$$

Clearly this implies that l belongs to $\mathscr{L}_{q,E}$. Let P denote the class of $D_{\underline{k}}\alpha(S)$ in $E(K_S)/qE(K_S)$. Let $T = Sl$, and let $P(l)$ denote the class of $D_{\underline{k}} \cdot D_l^1 \alpha(T)$ in $E(K_T)/qE(K_T)$. We make the following assumption:

Hypothesis 4.5 *For all the partial derivatives* D′ *which are strictly less than* $D_{\underline{k}}D_l^1$, *the class of* $D'\alpha(T)$ *is* 0 *in the group* $E(K_T)/qE(K_T)$.

Under hypothesis 4.5, one has:

Lemma 4.6 *The class of* $P(l)$ *is fixed under the action of* Γ_T.

Proof. Let $\sigma = \sigma_l$ for some l dividing T or $\sigma = \xi_j$ for some j. Then $(1 - \sigma)D_{\underline{k}}D_l^1 = D'$, where D′ is some partial derivative which is strictly less than $D_{\underline{k}}D_l^1$, by Lemma 4.1. Hence $(1 - \sigma)P(l) = 0$, by Hypothesis 4.5.

From Lemma 4.4, the group $E_q(K_T)$ is trivial and hence the following sequence is exact:

$$0 \to E(K_T) \xrightarrow{q} E(K_T) \to E(K_T)/qE(K_T) \to 0 .$$

Taking Γ_T-invariants yields an exact cohomology sequence

$$0 \to E(K)/qE(K) \to (E(K_T)/qE(K_T))^{\Gamma_T} \xrightarrow{\delta} H^1(\Gamma_T, E(K_T))_q .$$

Let $d(l) = \delta P(l)$. We will identify $d(l)$ with its image by inflation in $H^1(K, E)_q$.

The class $d(l)$ is the global cohomology class which plays a key role in Kolyvagin's method. We now undertake to analyze its properties.

Behavior of the class $d(l)$ *under complex conjugation*: Complex conjugation Frob_∞ acts on the group $H^1(K, E)_q$ in the natural way. Let $\varepsilon_k = (-1)^{k+1}\varepsilon$ be the parity of the order of $D_{\underline{k}}$, times the sign in the functional equation.

Proposition 4.7 *The class* $d(l)$ *is in the* ε_k*-eigenspace for the action of* Frob_∞.

Proof. By Lemma 4.4, the group $E(K_T)$ has no q-torsion, and hence the torsion subgroup $E(K_T)_{\mathrm{tor}}$ is killed in $E(K_T)/qE(K_T)$. Hence by Lemma 3.12 we have

$$\mathrm{Frob}_\infty[\alpha(T)] = \varepsilon\sigma_0[\alpha(T)] ,$$

where $[\alpha(T)]$ denotes the image of $\alpha(T)$ in $E(K_T)/qE(K_T)$. Combining Lemma 4.2 with the Hypothesis 4.5 that all lower order partial derivatives of $\alpha(T)$ vanish, we find:

$$\mathrm{Frob}_\infty P(l) = \varepsilon_k\sigma_0 P(l) = \varepsilon_k P(l) .$$

The last equality follows from Lemma 4.6. Since the map δ used to construct the class $d(l)$ from $P(l)$ is equivariant with respect to the Galois actions, it follows that $d(l)$ is in the ε_k-eigenspace for Frob_∞.

Local behavior of the class $d(l)$: Given a place v of K, let $d(l)_v$ denote the restriction of $d(l)$ in $H^1(K_v, E)_q$. The prime l is inert in $K/\mathbf{Q}$. Let λ be the place of K above it. The prime λ splits completely in K_S/K; choose a place λ' of K_S above λ. Finally, the

extension K_T/K_S is completely ramified at λ'; let λ'' denote the unique place of K_T above λ'. The localization $d(l)_\lambda$ belongs to

$$H^1(\mathrm{Gal}((K_T)_{\lambda''}/K_\lambda), E((K_T)_{\lambda''}))_q = H^1(G_l, E((K_T)_{\lambda''}))\ .$$

Fact 4.8 *The choice of generator σ_l of G_l determines a canonical inclusion of $H^1(G_l, E((K_T)_{\lambda''}))_q$ inside $E_q(k_\lambda)$.*

Proof. Since the kernel of the reduction map $E((K_T)_{\lambda''}) \to E(k_\lambda)$ is a pro-l group, the group $H^1(G_l, E((K_T)_{\lambda''}))_q$ injects into $H^1(G_l, E(k_\lambda))_q = \hom(G_l, E(k_\lambda))_q$. The latter group can be identified with $E(k_\lambda)_q$ thanks to the chosen generator σ_l of G_l.

Theorem 4.9 1. *For all archimedean places and all places which do not divide l or the conductor S' of $\mathrm{D}_{\underline{k}}$, the class $d(l)_v$ is equal to* 0.
2. *The image of $d(l)_\lambda$ in $E(k_\lambda)_q$ is equal to*

$$\frac{(l+1)\mathrm{Frob}_\infty - a_l}{q}\,\tilde{P}\ ,$$

where $\tilde{P}$ is the reduction of P mod λ'.

Proof. 1. If v is archimedean, then $K_v = \mathbf{C}$ and E/K_v has trivial Galois cohomology. Suppose now that v is a non-archimedean place not lying above $S'l$. By construction the class $d(l)_v$ is inflated from a class in $H^1(K_{S'l}/K, E)_q$. Since the extension $K_{S'l}$ is unramified at v, the class $d(l)_v$ comes from a class in $H^1(K_v^{\mathrm{unram}}/K_v, E)_q$. Let E^0 denote the connected component of the Néron model at v, and let $J_v = E/E_0$. The group $H^1(K_v^{\mathrm{unram}}/K_v, E^0)$ vanishes, (cf. [Mi, Chap. I, Proposition 3.8]), and hence $H^1(K_v^{\mathrm{unram}}/K_v, E)_q$ injects into $H^1(K_v^{\mathrm{unram}}/K_v, J_v)_q$. By the assumption that q is not invertible in Z, we know that q is prime to m and hence to the order of J_v. Hence the group $H^1(K_v^{\mathrm{unram}}/K_v, J_v)_q$ is trivial, and the class $d(l)_v$ vanishes.
2. The image of $d(l)_\lambda$ in $E(k_\lambda)$ by the isomorphism defined above is the point

$$\mathrm{red}_{\lambda''}\left(\frac{(\sigma_l - 1)P(l)}{q}\right) = \mathrm{red}_{\lambda''}\left(\frac{(\sigma_l - 1)D_l D_{\underline{k}}\alpha(T)}{q}\right),$$

where $\mathrm{red}_{\lambda''}: E((K_T)_{\lambda''}) \to E(k_\lambda)$ is the reduction map. But

$$\begin{aligned}(\sigma_l - 1)\mathrm{D}_l\mathrm{D}_{\underline{k}}\alpha(T) &= (l + 1 - \mathbf{N}_l)\mathrm{D}_{\underline{k}}\alpha(T) \text{ (by Lemma 4.1)}\\ &= (l+1)\mathrm{D}_{\underline{k}}\alpha(T) - a_l\mathrm{D}_{\underline{k}}\alpha(S) \text{ (by Proposition 3.10).}\end{aligned}$$

Hence,

$$\mathrm{red}_{\lambda''}\left(\frac{(\sigma_l - 1)P(l)}{q}\right) = \mathrm{red}_{\lambda''}\left(\frac{l+1}{q}\,\mathrm{Frob}_\infty \mathrm{D}_{\underline{k}}\alpha(S) - \frac{a_l}{q}\,\mathrm{D}_{\underline{k}}\alpha(S)\right),$$

by Proposition 3.11 combined with the fact that $\mathrm{Frob}_{\lambda'} = \mathrm{Frob}_\infty$. Since $\tilde{P} = \mathrm{red}_{\lambda''}(\mathrm{D}_{\underline{k}}\alpha(S))$, the lemma is proved.

4.3 Tate duality

The cup product in cohomology combined with the Weil pairing

$$E_q \otimes E_q \to \mu_q$$

give rise to a pairing

$$H^1(K_\lambda, E_q) \times H^1(K_\lambda, E_q) \to H^2(K_\lambda, \mu_q) = \mathbf{Z}/q\mathbf{Z} .$$

(The identification $H^2(K_\lambda, \mu_q) = \mathbf{Z}/q\mathbf{Z}$ is provided by the map

$$\mathrm{inv}_\lambda : H^2(K_\lambda, \mu_q) \to \mathbf{Z}/q\mathbf{Z}$$

of local class field theory.) It is a result of Tate that this local pairing is non-degenerate (cf. [Mi, Chap. I, Corollary 2.3]).

The local q-descent exact sequence

$$0 \to E(K_\lambda)/qE(K_\lambda) \to H^1(K_\lambda, E_q) \to H^1(K_\lambda, E)_q \to 0$$

allows us to view $E(K_\lambda)/qE(K_\lambda)$ as a submodule of $H^1(K_\lambda, E_q)$. This subspace is maximal isotropic for the local Tate pairing (cf. [Gr4, p. 247, Proposition 7.5], or [Mi, Chap. I, Theorem 2.6]). Therefore one gets a perfect pairing

$$\langle\ ,\ \rangle : E(K_\lambda)/qE(K_\lambda) \times H^1(K_\lambda, E)_q \to \mathbf{Z}/q\mathbf{Z} ,$$

i.e., an isomorphism

$$H^1(K_\lambda, E)_q \to (E(K_\lambda)/qE(K_\lambda))^* . \tag{4}$$

Here the superscript $*$ denotes Pontryagin dual, i.e., for a $\mathbf{Z}/q\mathbf{Z}$-module M,

$$M^* = \hom(M, \mathbf{Z}/q\mathbf{Z}) .$$

By composing the dual of the natural map $\mathrm{Sel}_q(E/K) \to E(K_\lambda)/qE(K_\lambda)$ with the isomorphism (4), one obtains a map

$$\phi_\lambda : H^1(K_\lambda, E)_q \to \mathrm{Sel}_q(E/K)^* .$$

Similarly, if S is any submodule of the Selmer group $\mathrm{Sel}_q(E/K)$, one obtains by restriction a map $H^1(K_\lambda, E)_q \to S^*$, which by abuse of notation we denote by the same letter ϕ_λ. The map ϕ_λ commutes with the action of complex conjugation on the modules $H^1(K_\lambda, E_q)$ and $\mathrm{Sel}_q(E/K)$, and hence preserves the decomposition into eigenspaces of the modules.

We will be exploiting the cohomology class $d(l)$ in the following way. Let $\mathrm{Sel}_q(S') \subset \mathrm{Sel}_q(E/K)$ be the kernel of the map

$$\mathrm{Sel}_q(E/K) \to \oplus_{v \mid S'} E(K_v)/qE(K_v) .$$

Proposition 4.10 *The local class $d(l)_\lambda$ is in the kernel of the map*

$$\phi_\lambda : H^1(K_\lambda, E)_q^{\varepsilon_\lambda} \to (\mathrm{Sel}_q(S')^*)^{\varepsilon_\lambda} .$$

Proof. Let s belong to $\mathrm{Sel}_q(S')$, and let s_λ denote its image in $E(K_\lambda)/qE(K_\lambda)$. We need to show that

$$\langle s_\lambda, d(l)_\lambda \rangle = 0 .$$

Let $\tilde{d}(l)$ denote a lift of $d(l)$ to the group $H^1(K, E_q)$. The cup-product $s \cup \tilde{d}(l)$ belongs to the global Brauer group $H^1(K, \mu_q)$. By the definition of the local pairing, we have:

$$\sum_v \langle s_v, d(l)_v \rangle = \sum_v \mathrm{inv}_v(s \cup \tilde{d}(l)) .$$

The latter sum is 0, by the reciprocity law of global class field theory. On the other hand, if the place v does not divide $S'\lambda$, then $d(l)_v = 0$, by theorem 4.9. If the place v divides S', then $s_v = 0$, since $s \in \mathrm{Sel}_q(S')$. Hence all of the terms in the first sum are zero, with the possible exception of $\langle s_\lambda, d(l)_\lambda \rangle$. It follows that $\langle s_\lambda, d(l)_\lambda \rangle = 0$.

4.4 Application of the Chebotarev density theorem

We make the following hypotheses:

Hypothesis 4.11 *The point* $P = D_{\underline{k}}\alpha(S)$ *is not the q-th power of a point in* $E(K_S)$.

Hypothesis 4.12 $r_q(\mathrm{Sel}_q(S')^{\varepsilon_k}) \geqq 1$.

Set $F = K_S(E_q)$. We start with a few cohomological lemmas.

Lemma 4.13 *The fields* K_S *and* $K(E_q)$ *are linearly disjoint over* K.

Proof. The intersection of the K_S and $K(E_q)$ is a subfield of $K(E_q)$ which is abelian over K and hence is contained in $K(\mu_q)$, since $\mathrm{Gal}(K(E_q)/K) = \mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$. But $K_S \cap K(\mu_q) = K$, since S and q are relatively prime.

Lemma 4.14 *Let* $(\mathbf{Z}/q\mathbf{Z})^2$ *be equipped with the natural action of* $\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$. *Then*

$$H^p(\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z}), (\mathbf{Z}/q\mathbf{Z})^2) = 0 .$$

Proof. Let $C \simeq (\mathbf{Z}/q\mathbf{Z})^*$ be the center of $\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$ consisting of the scalar matrices. The Hochschild–Serre spectral sequence

$$H^p(\mathbf{PGL}_2(\mathbf{Z}/q\mathbf{Z}), H^q(C, (\mathbf{Z}/q\mathbf{Z})^2)) \Rightarrow H^{p+q}(\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z}), (\mathbf{Z}/q\mathbf{Z})^2)$$

shows that $H^p(\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z}), (\mathbf{Z}/q\mathbf{Z})^2) = 0$, since C has order prime to q, and $H^0(C, (\mathbf{Z}/q\mathbf{Z})^2) = 0$ (here we use the fact that q is odd).

Lemma 4.15 *The restriction map* $H^1(K, E_q) \to H^1(K_S, E_q)$ *is injective.*

Proof. Its kernel is the group $H^1(K_S/K, E_q(K_S))$ which is trivial since $E_q(K_S) = 0$ by lemma 4.13.

Lemma 4.16 *The restriction map* $H^1(K_S, E_q) \to H^1(F, E_q)$ *is injective.*

Proof. By Lemma 4.13, we have $\mathrm{Gal}(F/K_S) = \mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$, and the kernel of the restriction map is the group

$$H^1(F/K_S, E_q) = H^1(\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z}), E_q) .$$

This group is trivial by lemma 4.14, and the result follows.

Lemma 4.17 *The restriction map* $H^1(K, E_q) \to H^1(F, E_q)$ *is injective.*

Proof. Combine Lemma 4.15 and 4.16.

Let l be a rational prime satisfying the condition

Condition 4.18 $l \nmid ND \cdot p \cdot S$, $\mathrm{Frob}_l = \mathrm{Frob}_\infty$ *in* $F/\mathbf{Q}$.

In this case, l is inert in $K/\mathbf{Q}$. Let λ be the unique prime of K above l. The prime λ splits completely in F/K. Choose a prime λ_F of F above it. The residue field of F at λ_F is identified with k_λ.

Proposition 4.19 *There exists a prime* l *satisfying the Condition* 4.18 *such that*

1. *The image of* $\tilde{P}$ *in* $E(k_\lambda)/qE(k_\lambda)$ *is non-zero.*
2. *The map* $\mathrm{Sel}_q(S')^{\varepsilon_k} \to (E(k_\lambda)/qE(k_\lambda))^{\varepsilon_k}$ *is surjective.*

Proof. By the Hypothesis 4.11, the class P in $E(K_S)/qE(K_S)$ is non-trivial. Complex conjugation acts on $E(K_S)/qE(K_S)$ in a natural way, and P can be written uniquely as a sum of projections onto the $+$ and $-$ eigencomponents for this action. At

least one of these projections is non-trivial: call it P'. The cohomology class in $H^1(K_S, E_q)$ corresponding to P' is also non trivial; hence, so is its restriction in $H^1(F, E_q)$, by Lemma 4.16. Let ζ_1 denote this restriction.

By Hypothesis 4.12, we may choose an element of order exactly q in $\mathrm{Sel}_q(S')^{\varepsilon_k}$, and the image ζ_2 of this element in $H^1(F, E_q)$ is still of order exactly q, by Lemma 4.17.

Both ζ_1 and ζ_2 are homomorphisms from $\mathrm{Gal}(F^{ab}/F)$ into E_q. Let $\tilde{F}$ be the smallest extension of F which is cut out by ζ_1 and ζ_2 and is Galois over $\mathbf{Q}$. Let $U = \mathrm{Gal}(\tilde{F}/F)$. There is an exact sequence

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{Gal}(\tilde{F}/F) & \to & \mathrm{Gal}(\tilde{F}/K_S) & \to & \mathrm{Gal}(F/K_S) & \to & 1 \\ & & \| & & & & \| & & \\ & & U & & & & \mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z}) & & \end{array}$$

which determines a $\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$-action on U. Similarly, complex conjugation Frob_∞ acts on U by inner automorphisms. The cohomology classes ζ_1, and ζ_2 are fixed under the action of $\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$ on $\hom(U, E_q)$, since they come from classes in $H^1(K_S, E_q)$ by inflation. Let U^+ denote the subspace of U which is fixed by Frob_∞. The class ζ_1 belongs to a fixed eigenspace of $\hom(U, E_q)$ for the action of Frob_∞, by construction. The class ζ_2 belongs to the ε_k-eigenspace, since it comes from a class in $\mathrm{Sel}_q(S')^{\varepsilon_k}$. Hence both ζ_1 and $p^{M-1}\zeta_2$ are non-zero on U^+. Otherwise, they would map U onto a given eigenspace of E_q for the Frob_∞-action, contradicting the $\mathbf{GL}_2(\mathbf{Z}/q\mathbf{Z})$-invariance of the image. Thus, we can find $\gamma \in U^+$ such that

$$\zeta_1(\gamma) \neq 0, \quad \zeta_2(\gamma) \text{ is of order exactly } q\ .$$

Now choose l such that

$$\mathrm{Frob}_l = \mathrm{Frob}_\infty \gamma \text{ in } \tilde{F}/\mathbf{Q}\ ,$$

where the equality is one of conjugacy classes in the group $\mathrm{Gal}(\tilde{F}/\mathbf{Q})$. One can find such a prime, by the Chebotarev density theorem. Clearly, l satisfies the Condition 4.18. In addition,

$$\zeta_1(\mathrm{Frob}_{\lambda_P}) = \zeta_1(\mathrm{Frob}_l^2) = \zeta_1(\gamma^{\mathrm{Frob}_\infty} \cdot \gamma) = \zeta_1(\gamma^2) \neq 0\ .$$

Hence, P is not a q-th power in $E(k_\lambda)/qE(k_\lambda)$, and condition 1 is satisfied. By the same computation, one shows that $\zeta_2(\mathrm{Frob}_{\lambda_P})$ is of order exactly q in E_q, which implies that the image of ζ_2 in $H^1(K_\lambda, E_q)^{\varepsilon_k}$ is itself of order exactly q, so that condition 2 is satisfied as well, since

$$(E(K_\lambda)/qE(K_\lambda))^{\varepsilon_k} \simeq \mathbf{Z}/q\mathbf{Z}\ .$$

This proves the proposition.

5 Proof of the main results

5.1 Proof of Theorem 3.15

Given a $\mathbf{Z}/q\mathbf{Z}$-module M, define $r_p(M)$ to be

$$r_p(M) = \dim_{\mathbf{F}_p}(M \otimes \mathbf{F}_p)\ .$$

Lemma 5.1 *If* $0 \to A' \to A \xrightarrow{f} A''$ *is an exact sequence of* $\mathbf{Z}/q\mathbf{Z}$*-modules, then*

$$r_q(A) \leqq r_q(A') + r_p(A'') .$$

Proof. We may assume without loss of generality that f is surjective. Let N denote the image of $A_{p^{M-1}}$ in A''. Because of the surjectivity assumption, the module A''/N is annihilated by p. There is a natural exact sequence of $\mathbf{F}_p$-vector spaces:

$$0 \to p^{M-1}A' \to p^{M-1}A \to A''/N$$
$$p^{M-1}a \mapsto f(a) .$$

Hence

$$\dim_{\mathbf{F}_p}(p^{M-1}A) \leqq \dim_{\mathbf{F}_p}(p^{M-1}A') + \dim_{\mathbf{F}_p}(A''/N) .$$

The lemma now follows from the fact that $\dim_{\mathbf{F}_p}(p^{M-1}A) = r_q(A)$ (and likewise for A') and from the inequality $\dim_{\mathbf{F}_p}(A''/N) \leqq r_p(A'')$.

Lemma 5.2 *For any prime* v *of* K *which lies above a prime of* $\mathscr{L}_q$,

$$r_p(E(K_v)/qE(K_v)^{\varepsilon_K}) \leqq 1 .$$

Proof. We have

$$r_p(E(K_v)/qE(K_v)) = r_p(E(K_v)/pE(K_v)) = r_p(E(k_v)/pE(k_v)) ,$$

because the norm of v is prime to p. Since $E(k_v)$ is a finite group, the group $E(k_v)/pE(k_v)$ is isomorphic to $E_p(k_v)$ which is at most 2 dimensional. Moreover, we know that

$$\# E(k_v)^{\pm} = l + 1 \mp a_l .$$

Since p divides $l+1$, the order of $E(k_v)$ is divisible by p if and only if p divides a_l, and then p divides the order of each eigenspace so that

$$r_p(E(k_v)/pE(k_v)^{\pm}) = 1.$$

Let $D_{\underline{k}}$ be as in the previous section a partial derivative of order k with support S and conductor S', and let $\varepsilon_k = (-1)^{k+1}\varepsilon$. Consider the modules

$$\mathrm{Sel}_q(S'), \quad A(S') = \oplus_{v|S'} E(K_v)/qE(K_v)$$

which fit into the exact sequence

$$0 \to \mathrm{Sel}_q(S')^{\pm} \to \mathrm{Sel}_q(E/K)^{\pm} \to A(S')^{\pm} .$$

Let $\mathrm{Sel}_q^{\pm}$ denote the plus and minus eigenspaces for the action of complex conjugation on $\mathrm{Sel}_q(E/K)$.

Theorem 5.3 *If* $\mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q(S')^{\varepsilon_K}) + r_p(A(S')^{\varepsilon_K})$, *then*

$$D_{\underline{k}}\alpha(S) \equiv 0 \pmod{q} .$$

Proof. The weight of $D_{\underline{k}}$ is defined to be

$$\mathrm{wt}(D_{\underline{k}}) = \mathrm{order}(D_{\underline{k}}) - \#\{l | S \text{ such that } l \text{ belongs to } \mathscr{L}_{q,E}\} .$$

We will show Theorem 5.3 by induction on $\mathrm{wt}(D_{\underline{k}})$.

Step 1 Case where $\mathrm{wt}(D_{\underline{k}}) < 0$. In that case, $D_{\underline{k}}$ contains a factor of the form D_l^0, with $l \in \mathscr{L}_{q,E}$. But then, by Proposition 3.10,

$$D_l^0\alpha(S) = a_l \cdot \alpha(S/l) ,$$

which is 0, since q divides a_l by Lemma 4.3. Thus one always has $D_{\underline{k}}\alpha(S) = 0$, without assuming any inequality for the order of $D_{\underline{k}}$.

Step 2 Proof for $\mathrm{wt}(D_{\underline{k}}) = w \geqq 0$: We make the induction hypothesis that Theorem 5.3 holds in weight strictly less than w. We argue by contradiction, assuming that $P = D_{\underline{k}}\alpha(S)$ is non-zero but that

$$\mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q(S')^{\varepsilon_K}) + r_p(A(S')^{\varepsilon_K}) .$$

Lemma 5.4 $r_q(\mathrm{Sel}_q(S')^{\varepsilon_K}) > 0$.

Proof. Otherwise we would have

$$\mathrm{order}(D_{\underline{k}}) < r_p(A(S')^{\varepsilon_K}) .$$

The right-hand side in this inequality is less than or equal to the number of primes dividing S', by Lemma 5.2, and thus cannot be greater than $\mathrm{order}(D_{\underline{k}})$.

Invoking Proposition 4.19, we choose a prime l satisfying the conditions

Conditions 5.5 1. $\mathrm{Frob}_l = \mathrm{Frob}_\infty$ *in* $K_S(E_q)/\mathbf{Q}$.

2. $\tilde{P} \neq 0$ *in* $E(k_\lambda)/qE(k_\lambda)$.

3. *The map* $\mathrm{Sel}_q(S')^{\varepsilon_K} \to (E(K_\lambda)/qE(K_\lambda))^{\varepsilon_K}$ *is surjective* (*or, dually, the map*

$$\phi_\lambda : H^1(K_\lambda, E)_q^{\varepsilon_K} \to (\mathrm{Sel}_q(S')^{\varepsilon_K})^*$$

is injective).

The crucial observation is that the Hypothesis 4.5 of Sect. 4.2 is still satisfied in our new setting.

Lemma 5.6 *The partial derivative* $D_{\underline{k}}D_l^1$ *satisfies the Hypothesis* 4.5 *of Sect.* 4.2.

Proof. Let D' be a partial derivative which is strictly less than $D_{\underline{k}}D_l^1$. We assume without loss of generality that the order of D' is equal to k, the order of $D_{\underline{k}}$. Lemma 5.1, applied to the exact sequence

$$1 \to \mathrm{Sel}_q(S'l)^{\varepsilon_K} \to \mathrm{Sel}_q(S')^{\varepsilon_K} \to (E(K_\lambda)/qE(K_\lambda))^{\varepsilon_K}$$

shows that

$$\begin{aligned} r_q(\mathrm{Sel}_q(S')^{\varepsilon_K}) &\leqq r_q(\mathrm{Sel}_q(S'l)^{\varepsilon_K}) + r_p(E(K_\lambda)/qE(K_\lambda)^{\varepsilon_K}) \\ &= r_q(A'(S'l)^{\varepsilon_K}) + 1 \text{ (by Lemma 5.2).} \end{aligned}$$

Also, by Lemma 5.2,

$$r_p(A(S')^{\varepsilon_K}) = r_p(A(S'l)^{\varepsilon_K}) - 1 .$$

Combining these two inequalities, we find that

$$\mathrm{order}(D') = k < r_q(\mathrm{Sel}_q(S'l)^{\varepsilon_K}) + r_p(A(S'l)^{\varepsilon_K}) .$$

Since the support of D' is divisible by an extra prime in $\mathscr{L}_{q,E}$,

$$\mathrm{wt}(D') < \mathrm{wt}(D_{\underline{k}}) .$$

Thus we may apply the induction hypothesis to conclude that $D'\alpha(S) = 0$.

Because of this lemma, we can apply the construction of Sect. 4.2, to obtain a class $d(l)$ in $H^1(K, E)_q$. Combining 1 and 2 of Conditions 5.5 satisfied by l with Theorem 4.9, we find

$$d(l)_\lambda \neq 0 .$$

By Proposition 4.10, it follows that the map

$$\phi_\lambda : H^1(K_\lambda, E)_q^{\varepsilon_k} \to (\mathrm{Sel}_q(S')^{\varepsilon_k})^*$$

fails to be injective, contradicting the third of the Conditions 5.5.

We now derive some consequences of the main result.

Corollary 5.7 *If* $\mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q(S')^{-\varepsilon_k}) + r_p(A(S')^{-\varepsilon_k}) - 1$, *then*

$$D_{\underline{k}}\alpha(S) \equiv 0 \pmod{q} .$$

Proof. Suppose that $P = D_{\underline{k}}\alpha(S) \neq 0 \pmod{q}$. Then, by Proposition 4.19, we can choose a prime l such that

1. $\mathrm{Frob}_l = \mathrm{Frob}_\infty$ in $K_S(E_q)/\mathbf{Q}$.
2. $\tilde{P} \neq 0$ in $E(k_\lambda)/qE(k_\lambda)$.

We observe that the point $D_{\underline{k}}D_l^1\alpha(T) = P(l)$ is non-zero in $E(K_T)/qE(K_T)$. For, either there is a partial derivative D' strictly less than $D_{\underline{k}}D_l^1$ such that $D'\alpha(T)$ is non-zero mod q, in which case $D_{\underline{k}}D_l^1$ is also non-zero mod q by Lemma 4.1; or $D_{\underline{k}}D_l^1$ satisfies the Hypothesis 4.5, in which case we can apply the general construction of Sect. 4.2 to obtain a cohomology class $d(l)$ in $H^1(K, E)_q$. By Theorem 4.9, this class is non-zero locally at λ, and hence a fortiori globally. Hence the point $P(l)$ from which it comes is non-zero as well. By the assumption,

$$\mathrm{order}(D_{\underline{k}}D_l^1) < r_q(\mathrm{Sel}_q(S')^{-\varepsilon_k}) + r_p(A(S')^{-\varepsilon_k}) .$$

on the other hand,

$$r_q(Sel_q(S')^{-\varepsilon_k}) + r_p(A(S')^{-\varepsilon_k}) \leqq r_q(\mathrm{Sel}_q(S'l)^{-\varepsilon_k}) + r_p(A(S'l)^{-\varepsilon_k}) ,$$

by the same calculation as in the proof of Lemma 5.6. Combining the two inequalities together, we find

$$\mathrm{order}(D_{\underline{k}}D_l^1) < r_q(\mathrm{Sel}_q(S'l)^{-\varepsilon_k}) + r_p(A(S'l)^{-\varepsilon_k}) .$$

Let $k' = \mathrm{order}(D_{\underline{k}}D_l^1) = k + 1$. Since $(-1)^{k'} = -\varepsilon_k$, we can apply Theorem 5.3 to conclude that $D_k D_l^1 = 0 \bmod p$, which is a contradiction.

Corollary 5.8 1. *If* $\mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q^{\varepsilon_k})$, *then* $D_{\underline{k}}\alpha(S) \equiv 0 \pmod{q}$.
2. *If* $\mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q^{-\varepsilon_k}) - 1$, *then* $D_{\underline{k}}\alpha(S) \equiv 0 \pmod{q}$.

Proof. By Lemma 5.1,

$$r_q(\mathrm{Sel}_q^{\varepsilon_k}) \leqq r_q(A'(S')^{\varepsilon_k}) + r_p(A''(S')^{\varepsilon_k}) .$$

Hence Part 1 follows from Theorem 5.3. Part 2 of the corollary follows similarly from Corollary 5.7.

We finally come to the proof of Theorem 3.15 whose statement we recall:

Theorem 3.15: *Let q be a power of a prime which is not invertible in Z, and let $D_{\underline{k}}$ be a partial derivative whose support S is a product of primes in $\mathscr{L}_q$. If* $\mathrm{order}(D_{\underline{k}}) < \rho_q$, *then*

$$D_{\underline{k}}\alpha(S) \equiv 0 \pmod{q} .$$

Proof. If the inequality is true, then either

$$\mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q^{\varepsilon_k}) \quad \text{or} \quad \mathrm{order}(D_{\underline{k}}) < r_q(\mathrm{Sel}_q^{-\varepsilon_k}) - 1 .$$

The result then follows from Corollary 5.8.

5.2 Proof of Theorem 2.5

We now turn to the proof of Theorem 2.5. We assume that $|r^+ - r^-| = 1$, so that $2\rho = r - 1$. To study the leading coefficient $\tilde{\theta}'(E, S)_{(p)}$, we must study the images of the elements $D_{\underline{k}}\alpha(S)$ in $E(K_S)/pE(K_S)$, where $D_{\underline{k}}$ is a partial derivative of order ρ and support S.

Part 2 of Theorem 2.5 will follow from:

Proposition 5.9 *If* $D_{\underline{k}}\alpha(S) \neq 0 \bmod p$, *then* $Ш_p(E/K) = 0$, *and the map*

$$\mathrm{Sel}_p(E/K) \to \otimes_{v|S} E(K_v)/pE(K_v)$$

is surjective (*i.e.*, $J_S \otimes \mathbf{F}_p = 0$).

Proof. If $D_{\underline{k}}\alpha(S) \neq 0 \bmod p$, then by Theorem 5.3 and Corollary 5.7, we have:

$$\rho \geqq r_p(\mathrm{Sel}_p(S)^{\varepsilon_k}) + r_p(A(S)^{\varepsilon_k}) \geqq r_p(\mathrm{Sel}_p(E/K)^{\varepsilon_k}) \geqq r^{\varepsilon_k},$$

$$\rho \geqq r_p(\mathrm{Sel}_p(S)^{-\varepsilon_k}) + r_p(A(S)^{-\varepsilon_k}) - 1 \geqq r_p(\mathrm{Sel}_p(E/K)^{-\varepsilon_k}) - 1 \geqq r^{-\varepsilon_k} - 1 .$$

Since $2\rho = r - 1$, we have equalities everywhere, and hence $Ш_p(E/K) = 0$. Also, since $r_p(\mathrm{Sel}_p(E/K)) = r_p(\mathrm{Sel}_p(S)) + r_p(A(S))$, the map

$$\mathrm{Sel}_p(E/K) \to A(S)$$

is surjective.

To show Part 1, we must show that

Proposition 5.10 $D_{\underline{k}}\alpha(S)$ *is in the image of the natural map*

$$E(K)/pE(K) \to E(K_S)/pE(K_S) .$$

Proof. Consider the exact sequence

$$0 \to E(K)/pE(K) \to E(K_S)/pE(K_S) \to H^1(K, E)_p$$

(cf. Sect. 4.2). Let P be the image of $D_{\underline{k}}\alpha(S)$ in $E(K_S)/pE(K_S)$, and let d be the image of P in $H^1(K, E)_p$. The cohomology class d is the obstruction for the point P to come from $E(K)/pE(K)$; we want to show that it vanishes. By Theorem 4.9, the class d is trivial locally except possibly at the places dividing S. Hence by the definition of the local Tate pairing and the reciprocity law of global class field theory (cf. Sect. 4.3), the image of d in $\oplus_{v|S} H^1(K_v, E)_p$ maps to 0 in $\mathrm{Sel}_p(E/K)^*$. But by Proposition 5.9, the map $\mathrm{Sel}_p(E/K) \to A(S) \otimes \mathbf{F}_p$ is surjective, and hence dually the map

$$\oplus_{v|S} H^1(K_v, E)_p \to \mathrm{Sel}_p(E/K)^*$$

is injective. Therefore the class d is locally trivial everywhere; it belongs to $Ш_p(E/K)$. By Proposition 5.9, $Ш_p(E/K) = 0$, and hence $d = 0$.

To conclude, we make some remarks concerning the Mazur Tate height pairing

$$\langle\ ,\ \rangle_S : E(K) \times E_S(K) \to (I/I^2) ,$$

where I denotes the augmentation ideal in the group ring $Z[\Gamma_S]$.

Claim 5.11 *If* $P \in E(K)$ *and* $Q \in E_S(K)$ *belong to the same eigenspaces for the action of complex conjugation, then* $\langle P, Q \rangle = 0$.

Proof. Let $\tau = \mathrm{Frob}_\infty$ denote complex conjugation. By the linearity of the Mazur Tate pairing and the fact that P and Q belong to the same eigenspace for τ, we have:

$$\langle \tau P, \tau Q \rangle = \langle P, Q \rangle .$$

On the other hand, the behavior of the Mazur Tate pairing under Galois action (cf. [MT2, p. 216, (3.4.2)]),

$$\langle \tau P, \tau Q \rangle_S = \tau \langle \tau P, Q \rangle_S \tau^{-1} = - \langle P, Q \rangle_S ,$$

and hence since I/I^2 is of odd order, $\langle P, Q \rangle_S = 0$.

Because of this claim, the pairing matrix has all of its $(r-1)\times(r-1)$-minors equal to 0 whenever $|r^+ - r^-| > 1$. Hence the regulator R_S vanishes. Since the leading coefficient $\tilde{\theta}'(E, S)$ is also zero in $E(K_S)^{\otimes 2} \otimes I^{r-1}/I^r$ (because $2\rho > r-1$), we have shown:

Proposition 5.12 *If $|r^+ - r^-| > 1$, then both the regulator R_S and the leading coefficient $\tilde{\theta}'(E, S)$ are zero in $E(K_S)^{\otimes 2} \otimes (I^{r-1}/I^r)$, where I denotes the augmentation ideal in the group ring $Z[\Gamma_S]$. Hence Conjecture 2.3 is true in this case, after tensoring with Z.*

5.3 Proof of Theorem 2.6

We finish with the proof of Theorem 2.6 (cf. Sect. 2.2).

Theorem 2.6 $\dim_{\mathbf{F}_p}(\mathscr{E}(L)_p) \leqq p - \rho_p$.

Proof. Let σ be a generator for the group G, and let α be the Heegner point in $E(L)$. By applying Lemma 4.1, one sees that the non-zero vectors among

$$\mathrm{D}_\sigma^0 \alpha, \mathrm{D}_\sigma^1 \alpha, \ldots, \mathrm{D}_\sigma^{p-1} \alpha$$

give a basis for the vector space $\mathscr{E}_p$ over $\mathbf{F}_p$. By Theorem 3.15 the partial derivatives of α of order $< \rho_p$ are 0 mod p, and the result follows.

Acknowledgements. I wish to thank Massimo Bertolini with whom I have had many fruitful discussions on the topics of this paper. I am also grateful to my advisor Benedict Gross for guiding me towards this topic. This research was funded in part by a Natural Sciences and Engineering Research Council of Canada (NSERC) '67 award, and by a Sloan doctoral dissertation fellowship.

References

[BD] Bertolini, M., Darmon, H.: Kolyvagin's descent and Mordell-Weil groups over ring class fields, J. Reine Angew. Math. **412**, 63–74 (1990)

[D1] Darmon, H.: Refined Class Number Formulas for Derivatives of L-series. Thesis, Harvard University (May 1991)

[D2] Darmon, H.: Euler systems and refined conjectures of Birch Swinnerton-Dyer type. In: Proceedings of a workshop on p-adic monodromy and the Birch Swinnerton-Dyer conjecture. Boston University, August 1991 (to appear)

[Gr1] Gross, B.H.: Heegner points on $X_0(N)$. In: Modular Forms, pp 87–105 Rankin, R.A. (ed.) Chichester: Ellis Horwood 1984

[Gr2] Gross, B.H.: Heights and the special values of L-series. In: Kisilevsky, H., Labute, J. (eds.) Proceedings of the 1985 Montreal conference on number theory, June 17–29, 1985. CMS. Conf. Proc., vol. 7, Providence, RI: Am. Math. Soc. 1987, pp. 115–188

[Gr4] Gross, B.H.: Kolyvagin's work on modular elliptic curves. In: Proc. Durham symposium on L-functions and arithmetic, 1989 (to appear)

[GZ] Gross, B.H., Zagier, D.B.: Heegner points and derivatives of L-series. Invent. Math. **84**, 225–320 (1986)

[H1] Alfred W. Hales, Augmentation terminals of finite abelian groups. In: Gòbel, R. et al. (eds.) Abelian Group Theory. (Lect. Notes. Math., vol. 1006, pp. 720–733) Berlin Heidelberg New York: Springer 1983

[H2] Alfred, W.: Hales, Stable augmentation quotients of abelian groups, Pac. J. Math. 118, no. 2, 1985, 401–410

[Ka] Kato, K.: Iwasawa theory and p-adic Hodge theory. Manuscript

[Ko1] Kolyvagin, V.A.: Finiteness of $E(\mathbf{Q})$ and $Ш(E/\mathbf{Q})$ for a subclass of Weil curves. Izv. Akad. Nauk. SSSR Ser. Mat. 52(3) (1988), 522–540; Math USSR Izv. **32**, 523–541 (1989)

[Ko2] Kolyvagin, V.A.: On the Mordell-Weil group and Shafarevich-Tate group of Weil elliptic curves. Izv. Akad. Nauk. SSSR Ser. Mat. 52 (6) (1988), 1154–1179

[Ko3] Kolyvagin, V.A.: Euler Systems, (1988). Birkhäuser volume in honor of Grothendieck (to appear)

[Ma1] Mazur, B.: Courbes elliptiques et symbole modulaire. In: Séminaire Bourbaki 414 (1971/1972) (Lect. Notes Math., vol. 317) Berlin Heidelberg New York: Springer 1972

[Ma2] Mazur, B.: Modular curves and arithmetic. In: Proceedings of the International Congress of Mathematicians, August 16–24, 1983. Warszawa: Polish Scientific Publishers 1984

[MS] Mazur B., Swinnerton-Dyer, P.: Arithmetic of Weil curves. Invent. Math. **25**, 1–61 (1974)

[MT1] Mazur B., Tate, J.: Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math J. 54, No. 2, 1987, p. 711

[MT2] Mazur, B. and Tate, J.: Canonical height pairings via biextensions. In: Arithmetic and Geometry, vol. I, pp. 195–237. Boston Basel Stuttgart Birkhäuser 1983

[Mi] Milne, J.S.: Arithmetic duality theorems. (Prespect. Math.) Boston: Academic Press 1986

[Pa] I.B.S. Passi, Group rings and their augmentation ideals. (Lect. Notes. Math., vol. 715) Berlin Heidelberg New York: Springer 1979

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

[Th] Thaine, F.: On the ideal class groups of real abelian number fields, Ann. Math. **128**, 1–18 (1988)

[Wal] Waldspurger, J-L.: Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie. Comp. Math. **54**, 173–242 (1985)