Canad. J. Math. Vol. **62** (5), 2010 pp. 1060–1081
doi:10.4153/CJM-2010-039-8

Heegner Points over Towers of Kummer Extensions

Henri Darmon and Ye Tian

Abstract. Let E be an elliptic curve, and let L_n be the Kummer extension generated by a primitive p^n-th root of unity and a p^n-th root of a for a fixed $a \in \mathbb{Q}^\times - \{\pm 1\}$. A detailed case study by Coates, Fukaya, Kato and Sujatha and V. Dokchitser has led these authors to predict unbounded and strikingly regular growth for the rank of E over L_n in certain cases. The aim of this note is to explain how some of these predictions might be accounted for by Heegner points arising from a varying collection of Shimura curve parametrisations.

1 Introduction

Let E be an elliptic curve defined over a number field F. For each finite extension L of F, write $r_E(L)$ for the rank of the group $E(L)$ of L-rational points on E. A *p-adic Lie extension* of F is a Galois extension L_∞/F whose Galois group G is a p-adic Lie group (for example, the splitting field of any continuous representation of the absolute Galois group of F acting on a finite dimensional $\mathbb{Q}_p$-vector space). The present note is motivated by the following general problem:

Problem 1.1 *To understand the variation of $r_E(L)$ as L ranges over all finite extensions of F contained in L_∞.*

This problem dates back at least to the foundational article [Ma], which considers the case when $G = \mathbb{Z}_p$, and makes the first steps towards examining this problem by the methods of Iwasawa theory. As in classical descent theory, it is convenient to replace the Mordell–Weil group $E(L)$ by the p-power Selmer group of E over L, thus sidestepping the difficulties associated with the Shafarevich–Tate conjecture. This Selmer group is defined to be

$$\mathrm{Sel}_p(E/L) := \ker\Big(H^1(L, E[p^\infty]) \longrightarrow \bigoplus_v H^1(L_v, E)[p^\infty]\Big),$$

where $E[p^\infty]$ denotes the Galois module of all p-power division points on E, and v runs over all places of L. The idea of Iwasawa theory is to exploit the structure of the Selmer group of E over L_∞ as a module for the Galois group G to show that the groups $\mathrm{Sel}_p(E/L)$ exhibit some coherence as L varies.

A rich, well-developed theory now paints a fairly precise picture when $F = \mathbb{Q}$ and G is either abelian or dihedral.

The last decade has seen the emergence of a program of non-abelian Iwasawa theory whose goal is to study Problem 1.1 in settings which are further removed from

Received by the editors November 29, 2007.
Published electronically July 16, 2010.
AMS subject classification: **11G05**, 11R23, 11F46.

the abelian setting. A prototypical example is the case where $L_\infty = \mathbb{Q}(A[p^\infty])$ is the field generated over $\mathbb{Q}$ by the coordinates of the p-power division points of an elliptic curve A over $\mathbb{Q}$. The article [Har] exhibits cases where $r_E(\mathbb{Q}(A[p^n]))$ is unbounded with n, but it is fair to say that the type of growth it could exhibit is at present only poorly understood.

An intermediate case which appears more tractable, while still representing a significant departure from the cyclotomic and anti-cyclotomic situations, is the case of *Kummer towers* (sometimes also called *false Tate curve extensions*), where L_n is an extension of the form $\mathbb{Q}(\mu_{p^n}, q^{1/p^n})$ for some $q \in \mathbb{Q}^\times$ which is p-power free, and L_∞ is the union of the L_n. In that case $G = \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ contains no abelian subgroup of finite index. Studies by Coates, Fukaya, Kato, and Sujatha [CFKS] and V. Dokchitser [Do-V] has led these authors to predict unbounded and strikingly regular growth for $r_E(L_n)$ in certain cases. The aim of this note is to explain how some of these predictions might be accounted for by Heegner points arising from a *varying* collection of Shimura curve parametrisations.

From now on, let E be an elliptic curve defined over $\mathbb{Q}$. We recall the deep fact that E is known to be modular, a result which underlies all of our subsequent work. We begin by reviewing earlier results in the (abelian) Iwasawa theory of elliptic curves which provide both a context and some essential tools for our study.

A. Cyclotomic towers. Let $L_\infty = \mathbb{Q}(\mu_{p^\infty})$ be the field obtained by adjoining the group μ_{p^∞} of all p-power roots of unity to $\mathbb{Q}$. Thus $\mathrm{Gal}(L_\infty/\mathbb{Q}) = \mathbb{Z}_p^\times$. Any finite extension $L \subset L_\infty$ is contained in $L_n = \mathbb{Q}(\mu_{p^n})$ for some n, where μ_{p^n} denotes the group of p^n-th roots of unity. A qualitative answer to Problem 1.1 in this case is supplied by the following.

***Theorem 1.2* (Kato–Rohrlich)** *The rank $r_E(L_n)$ is bounded as $n \to \infty$.*

The proof of Theorem 1.2 falls naturally into two parts. A non-vanishing theorem of Rohrlich [Ro] shows that $\mathrm{ord}_{s=1} L(E/L_n, s)$ remains bounded as $n \to \infty$, or equivalently that the twisted L-values $L(E, \chi, 1)$ are non-zero for all but finitely many Dirichlet characters χ of p-power conductor. Secondly, a deep theorem of Kato [Ka] shows that the χ-part of $E(L_\infty) \otimes \mathbb{C}$ is trivial when $L(E, \chi, 1) \neq 0$. It follows that $E(L_\infty)$ must have the same rank as $E(L_n)$ for all sufficiently large n.

B. Anticyclotomic towers. It will be assumed from now on that $p > 2$. Let K be an imaginary quadratic field, and let L_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K. This is the unique $\mathbb{Z}_p$-extension of K which is Galois over $\mathbb{Q}$ and for which $G = \mathrm{Gal}(L_\infty/\mathbb{Q})$ is a semi-direct product of the form $\mathbb{Z}_p \rtimes \mathbb{Z}/2\mathbb{Z}$, where the quotient of order two acts nontrivially on $\mathbb{Z}_p$. For each $n \geq 0$, let L_n be the unique subfield of L_∞ of degree p^n over K. The group $\mathrm{Gal}(L_n/\mathbb{Q})$ is a dihedral group of order $2p^n$. Suppose for simplicity that the conductor of E is relatively prime to p and the discriminant of K. Then one has the following.

Theorem 1.3 *The ranks $r_E(L_n)$ are either bounded or of the form $p^n + O(1)$, as $n \to \infty$.*

The dichotomy in Theorem 1.3 is controlled by the sign in the functional equation for the L-series $L(E/K, s)$. Let $\mathrm{sign}(E, K) \in \{-1, 1\}$ denote this sign. If χ is a

finite order character of $\mathrm{Gal}(L_\infty/K)$, the functional equation for the twisted L-series $L(E/K,\chi,s)$ relates $L(E/K,\chi,s)$ to $L(E/K,\chi,2-s)$, and the sign occurring in this functional equation is *equal* to $\mathrm{sign}(E,K)$.

If $\mathrm{sign}(E,K)=1$, a non-vanishing result of Vatsal [Va1] establishes the analogue of Rohrlich's theorem: $L(E/K,\chi,1)\neq 0$ for almost all finite order characters of $\mathrm{Gal}(L_\infty/K)$. The main result of [BD4] supplies the analogue of the theorem of Kato alluded to in the discussion of the cyclotomic case. It then follows that $E(L_\infty)=E(L_n)$ for n sufficiently large.

If $\mathrm{sign}(E,K)=-1$, the twisted L-series $L(E/K,\chi,s)$ all vanish to odd order, and therefore

$$\mathrm{ord}_{s=1}\, L(E/L_n,s)\geq p^n.$$

The Birch and Swinnerton-Dyer conjecture therefore predicts a growth for $r_E(L_n)$ which is at least linear in $[L_n:K]$. *Heegner points* arising from the modularity of E and the theory of complex multiplication can be used to construct an explicit subgroup $HP(n)$ of $E(L_n)$. The main theorem of [Cor] and [Va2] states that the rank of $HP(n)$ is equal to $p^n+O(1)$. The methods of Kolyvagin [Ko1], [Ko2] (suitably adapted to ring class characters, as in [BD1]) then prove the result.

The key novelty of the anticyclotomic setting is the possibility of unbounded (and in fact, linear in the degree) growth of $r_E(L_n)$; up to a bounded error term, this linear growth is accounted for by Heegner points. (We remark that, although the case where $\mathrm{sign}(E,K)=1$ seems closer to the cyclotomic case, Heegner points still play a crucial role in the proof of the main results of [BD4].)

Note that the group $\mathrm{Gal}(L_n/\mathbb{Q})$, while non-abelian, is still not far from abelian, in the sense that it contains an abelian normal subgroup of index 2.

C. Kummer towers. Fix an odd prime p, and an integer $q>1$ which is p-power free. Then define

$$L_n=\mathbb{Q}(\mu_{p^n},q^{1/p^n}),\quad (n\geq 1);\quad L_\infty=\bigcup_{n\geq 1}L_n.$$

Thus

$$\mathrm{Gal}(L_n/\mathbb{Q})\simeq(\mathbb{Z}/p^n\mathbb{Z})\rtimes(\mathbb{Z}/p^n\mathbb{Z})^\times,\quad G=\mathrm{Gal}(L_\infty/\mathbb{Q})\simeq\mathbb{Z}_p\rtimes\mathbb{Z}_p^\times.$$

The study of elliptic curves over this tower has been undertaken by a number of authors, notably in [HV] (from the algebraic point of view of descent, and Iwasawa theory) and in [Do-V] (from the analytic point of view of L-functions and root numbers.)

On the algebraic side, assuming that E has good ordinary reduction at p, it is proven in [HV] that there exists a positive constant $C>0$ such that the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_p(E/L_n)$ is at most Cp^n for all n.

On the analytic side, if we write

$$F_n=\mathbb{Q}(\mu_{p^n})^+,\quad K_n=\mathbb{Q}(\mu_{p^n}),$$

it follows from the modularity of E over $\mathbb{Q}$ and the theory of abelian base change that the Hasse–Weil L-series $L(E/K_n,s)$ is entire, and has a functional equation of the

standard type; the same also holds for its twists $L(E/K_n, \chi, s)$ by abelian characters χ of K_n. It follows that

$$L(E/L_n, s) = \prod_{\chi \in \widehat{\mathrm{Gal}(L_n/K_n)}} L(E/K_n, \chi, s)$$

is entire and has a functional equation and analytic continuation. Alternately (and more germane to the methods of this article), abelian base change shows that E/F_n arises from a Hilbert modular form f_n on $GL_2(F_n)$. The L-series $L(E/K_n, \chi, s)$ can be expressed in terms of the Rankin convolution of f_n with a theta-series over F_n associated to $\mathrm{Ind}_{F_n}^{K_n} \chi$, and the analytic continuation of $L(E/K_n, \chi, s)$ follows from Rankin's method. The following result is proved in [Do2]:

Proposition 1.4 *Suppose that*

(i) *p is an odd prime of good reduction for E;*
(ii) *q is an odd prime of multiplicative reduction for E;*
(iii) *q generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$;*
(iv) $\mathrm{sign}(E, \mathbb{Q}(\mu_p)) = 1$.

Then

$$\mathrm{ord}_{s=1} L(E/L_n, s) \geq p^n - 1.$$

In the setting of Proposition 1.4, the Birch and Swinnerton-Dyer conjecture predicts that

$$r_E(L_n) \geq p^n - 1. \tag{1.1}$$

The following result (Theorem 11 of [Do-TV1], improved by [CFKS]) singles out some special cases where the inequality (1.1) is expected to be sharp.

Proposition 1.5 *Assume the hypothesis of Proposition* 1.4*, and assume in addition that* $\mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^\infty})) = 0$. *Then*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_p(E/L_n) = p^n - 1.$$

The assumption on $\mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^\infty}))$ is used in the proof via p-descent in the spirit of the methods of non-commutative Iwasawa Theory developed in [HV].

In the setting of Proposition 1.5, both the Birch and Swinnerton-Dyer conjecture and the Shafarevich–Tate conjecture predict that

$$r_E(L_n) = p^n - 1, \quad \text{for all } n \geq 0. \tag{1.2}$$

The purpose of this note is to point out a possible strategy for verifying (1.2) independently of these deep conjectures. Our main result (Theorem 1.8 below) removes the dependence on the Birch and Swinnerton-Dyer conjecture and the Shafarevich-Tate conjecture, but remains conditional on Conjecture 1.7 below, which might be viewed as a natural extension of the ongoing work of Skinner and Urban [Sk] to the

setting of totally real fields. We now introduce the notations and concepts that are needed to formulate Conjecture 1.7 precisely.

Let f_0 be the elliptic modular form associated with the elliptic curve $E/\mathbb{Q}$. Let F be a totally real abelian extension of $\mathbb{Q}$, and let f denote the (normalized) Hilbert modular eigenform on $\mathrm{GL}_2(F)$ associated with f_0 by abelian base change. For each prime λ of F, let $a_\lambda(f)$ be the coefficient attached to λ in the Fourier expansion of f, and let $\mathbb{T}$ be the Hecke algebra over F. Let $\varphi\colon \mathbb{T} \to \mathbb{Z}$ be the homomorphism on $\mathbb{T}$ that sends the Hecke operator T_λ to $a_\lambda(f)$.

Let K be a totally imaginary quadratic extension of F and ω the associated quadratic Hecke character over F. Assume for simplicity that the discriminant of K is relatively prime to the conductor N of E over F. Let Σ' denote the following finite set of places of F:

$$\Sigma' = \{ \text{ places } v \text{ of } F : \quad v|\infty \quad \text{or} \quad \omega_v(N) = -1\}. \tag{1.3}$$

Lemma 1.6 *If $L(E/K,1) \neq 0$, then Σ' has even cardinality.*

Proof The non-vanishing of $L(E/K,1)$ implies that $\mathrm{sign}(E,K) = 1$. A standard formula (for example, [Zh2, (1.1.2)]) for the root number asserts that $\mathrm{sign}(E,K)$ is equal to $(-1)^{\#\Sigma'}$. ∎

Let B' denote the (unique, up to isomorphism) quaternion algebra over F which is ramified precisely at the places of Σ'. Such a quaternion algebra exists by Lemma 1.6, and is totally definite. Fix an embedding $K \hookrightarrow B'$ (such an embedding exists since $K_v := K \otimes_F F_v$ is a field whenever B' is ramified at v) and choose an order R' in B' containing $\mathcal{O}_K$ as a subring of relative discriminant N. Write $\hat{\mathbb{Z}}$ for the profinite completion of $\mathbb{Z}$, and set $\widehat{R}' := R' \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$, $\widehat{B}' = \widehat{R}' \otimes \mathbb{Q}$. Let G' denote the algebraic group over F representing the functor on F-algebras given by $A \to (B' \otimes_F A)^\times$. Let U' be the compact open subgroup $\widehat{R}'^{\times}$ of $G'(\mathbb{A}_f)$ where $\mathbb{A}_f$ is the ring of finite adèles of F. By strong approximation, the set

$$X' = G'(F)\backslash G'(\mathbb{A}_f)/U' \tag{1.4}$$

is finite. (It can be viewed as the points on the Shimura variety of dimension 0 associated with the pair (G', U').) The set X' is also in bijection with the conjugacy classes of Eichler orders in B' that are locally conjugate to R', equipped with an *orientation* at N in the sense [BD2, §2.2]. Let $\mathbb{Z}[X']$ denote the finitely generated $\mathbb{Z}$-module of $\mathbb{Z}$-valued functions on X'. We call it the space of integral *automorphic forms for G'* of weight 2 and level N. This module is equipped with an action of the Hecke algebra $\mathbb{T}$ and with a natural non-degenerate $\mathbb{Z}$-valued bilinear form

$$\langle\, \cdot\,, \cdot\, \rangle : \mathbb{Z}[X'] \times \mathbb{Z}[X'] \longrightarrow \mathbb{Z} \tag{1.5}$$

for which the Hecke operators T_λ (with $\lambda \nmid N$) are self-adjoint. By the Jacquet–Langlands correspondence and multiplicity one, there is a unique rank one $\mathbb{Z}$-module in $\mathbb{Z}[X']$ on which $\mathbb{T}$ acts via the homomorphism φ. Let ϕ' denote a generator of this

$\mathbb{Z}$-module. Note that ϕ' is well defined up to sign, so the quantity $\langle \phi', \phi' \rangle$ is a well-defined integer. The *algebraic part* of $L(E/K, 1)$ is defined by the formula

$$\mathbb{L}(E/K, 1) := 2^{-([F:\mathbb{Q}]+1)} \sqrt{\mathrm{N}(d_{K/F})} \frac{L(E/K, 1)}{(f, f)} \langle \phi', \phi' \rangle, \tag{1.6}$$

where $d_{K/F}$ is the relative discriminant of K/F and $\mathrm{N}(d_{K/F})$ is its absolute norm. The quantity (f, f) is the period of the Hilbert modular form f, as defined in Theorem 6.1 of [Zh3]. As will be explained in Section 2 below, the quantity $\mathbb{L}(E/K, 1)$ is an integer. We make the following conjecture:

Conjecture 1.7 *Let p be a prime that does not divide the absolute norm of N. Assume that p does not divide the Tamagawa numbers of E/K, and that the mod p Galois representation $E[p]$ is absolutely irreducible. If $\mathrm{Sel}_p(E/K)$ is trivial, then p does not divide $\mathbb{L}(E/K, 1)$.*

We can now state the main result.

Theorem 1.8 *Let p and q be two odd primes such that q generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Let E be an elliptic curve defined over $\mathbb{Q}$, and let $L_n = \mathbb{Q}(\mu_{p^n}, q^{1/p^n})$. Assume that*

(i) *E has good ordinary reduction at p and $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$;*
(ii) *E has multiplicative reduction at q;*
(iii) $\mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^\infty})) = 0$.
(iv) *Conjecture 1.7 holds for E and the extensions $F = \mathbb{Q}(\mu_{p^n})^+$ and $K = \mathbb{Q}(\mu_{p^n})$ for all n.*

Then $r_E(L_n) = p^n - 1$ and $r_E(\mathbb{Q}(q^{1/p^n})) = n$.

Concerning the behaviour of the Hasse–Weil L-series and the Shafarevich–Tate groups, our proof of Theorem 1.8 leads to the following information.

Theorem 1.9 *Under the assumptions of Theorem 1.8, we have*

$$\mathrm{ord}_{s=1} L(E/L_n, s) = p^n - 1, \quad \mathrm{ord}_{s=1} L(E/\mathbb{Q}(q^{1/p^n}), s) = n.$$

Furthermore, the Shafarevich–Tate groups of E over L_n and $\mathbb{Q}(q^{1/p^n})$ are finite.

The next two sections are devoted to a discussion of the two critical hypotheses (iii) and (iv) that are made in Theorem 1.8.

2 Conjecture 1.7 and Zhang's formula

The formulation of Conjecture 1.7 is justified by an explicit formula of Zhang for $\mathbb{L}(E/K, 1)$ (generalising a formula of Gross [Gr]) which shows that this quantity is always an integer.

The article [Zh3] associates with X' and K a canonical element Δ'_K of $\mathbb{Q}[X']$. This element is obtained by considering the conjugacy classes of optimal embeddings of $\mathcal{O}_K$ into Eichler orders in B' which are locally conjugate to R'. Such an optimal embedding is defined to be a pair

$$(\Psi, \alpha) \in G'(F) \backslash \big(\hom(K, B') \times G'(\mathbb{A}_f) \big) / U'$$

satisfying

$$\alpha_v^{-1}\Psi(\mathcal{O}_{K,v})\alpha_v \subset R'_v, \qquad \text{for all places } v \text{ of } F. \tag{2.1}$$

The class group $K^\times\backslash\hat{K}^\times/\prod_v \mathcal{O}_{K,v}^\times$ acts naturally on the optimal embeddings by the rule

$$\xi \star (\Psi, \alpha) := (\Psi, \Psi(\xi)\alpha).$$

Let $(\Psi_1, \alpha_1), \ldots, (\Psi_h, \alpha_h)$ be a full orbit for this action, and let w_j be the cardinality of the automorphism group of (Ψ_j, α_j). Then we define

$$\Delta'_K := \sum_{j=1}^{h} w_j^{-1}\alpha_j \in \mathbb{Q}[X']. \tag{2.2}$$

It can be shown that Δ'_K belongs to the dual lattice $\mathbb{Z}[X']^\vee$ of $\mathbb{Z}[X']$ under the pairing (1.5).

Zhang's formula (*cf.* [Zh3, Theorem 7.1]) relates the position of the vector Δ'_K in $\mathbb{Z}[X']^\vee$ to the special value of $L(E/K, 1)$:

$$\frac{\langle\phi', \Delta'_K\rangle^2}{\langle\phi', \phi'\rangle} = 2^{-([F:\mathbb{Q}]+1)}\sqrt{\mathrm{N}(d_{K/F})}\frac{L(E/K, 1)}{(f, f)}.$$

(Note that the expression on the left is unchanged when ϕ' is rescaled.) This formula shows that

$$\mathbb{L}(E/K, 1) = \langle\phi', \Delta'_K\rangle^2$$

is an integer. Moreover, as Δ ranges over all the elements of $\mathbb{Z}[X']^\vee$, the fact that ϕ' is not divisible by any integer greater than 1 in $\mathbb{Z}[X']$ implies that the quantities $\langle\phi', \Delta\rangle$ have no common prime divisor. This is why we expect that if a prime p does not arise in the extraneous factors of the Birch and Swinnerton-Dyer conjecture (namely, the Tamagawa numbers of E/K and the cardinality of $E(K)_{\mathrm{tors}}$), it should only divide $\mathbb{L}(E/K, 1)$ when the Selmer group $\mathrm{Sel}_p(E/K)$ is non-trivial.

A proof of conjecture 1.7 has been announced in [Sk] in the case where $F = \mathbb{Q}$. The approach of [Sk] is to assume that p divides $\mathbb{L}(E/K, 1)$ and to relate this quantity to the constant term of an Eisenstein series on $U(2, 2)$ arising from a lift of f_0. A mod p congruence between this Eisenstein series and a cusp form leads to an irreducible but residually reducible p-adic Galois representation from which the sought-for non-trivial element of $\mathrm{Sel}_p(E/K)$ can be constructed. It is the authors' hope that Conjecture 1.7 might eventually yield to similar methods. While the technical obstacles may be considerable, it is fair to say that Conjecture 1.7 presents less mystery than either the Birch–Swinnerton-Dyer or the Shafarevich–Tate conjectures, thanks to the ideas introduced in [Sk].

We also remark that the converse of Conjecture 1.7 is proved, in the case where $F = \mathbb{Q}$ and under certain extra hypotheses, in [BD4]. The approach described there,

just like the methods of [Sk], admits a generalization to totally real fields. (See for example [Lo] and [TZ].)

The proof of Theorem 1.8 involves certain imprimitive versions of the invariants Δ'_K and $\mathbb{L}(E/K,1)$. More precisely, given an ideal λ of $\mathcal{O}_F$, we let $\mathcal{O}_K[\lambda] := \mathcal{O}_F + \lambda\mathcal{O}_K$ be the $\mathcal{O}_F$-order of K of conductor λ. An optimal embedding of K into B' of conductor λ is defined in the obvious way, by replacing $\mathcal{O}_K$ by $\mathcal{O}_K[\lambda]$ in the definition (2.1) of an optimal embedding of conductor 1. The invariant $\Delta'_{K,\lambda}$ is then defined as in (2.2), but summing this time over an orbit of optimal embeddings of conductor λ under the action of the class group $K^\times\backslash\hat{K}^\times/\hat{\mathcal{O}}_K[\lambda]^\times$. Finally we set

$$\mathbb{L}(E/K,1)_{(\lambda)} := \langle\phi', \Delta'_{K,\lambda}\rangle^2. \tag{2.3}$$

Let us return now to the specific setting where $F = \mathbb{Q}(\mu_{p^n})^+$ and where $K = \mathbb{Q}(\mu_{p^n})$. Let $\mathfrak{p}$ be the unique prime of F above p, and let

$$a_p := p + 1 - \#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - \#E(\mathcal{O}_F/\mathfrak{p}).$$

Lemma 2.1 *For all integers $t \geq 1$,*

$$\mathbb{L}(E/K,1)_{(\mathfrak{p}^t)} \equiv (a_p - 1)a_p^{t-1}\mathbb{L}(E/K,1) \pmod{p}.$$

Proof The elements $\Delta_{K,\mathfrak{p}^t}$ are related to the images of Δ'_K under powers of the Hecke operator $\mathrm{T}_\mathfrak{p}$ via the following recursive formulae:

$$\Delta'_{K,\mathfrak{p}} = (\mathrm{T}_\mathfrak{p} - 1)\Delta'_K, \qquad \Delta'_{K,\mathfrak{p}^{t+1}} = \mathrm{T}_\mathfrak{p}\Delta'_{K,\mathfrak{p}^t} - p\Delta'_{K,\mathfrak{p}^{t-1}}, \quad \text{for } t \geq 1.$$

Recall that $\mathrm{T}_\mathfrak{p}$ acting on $\mathbb{Q}[X']$ is self-adjoint, and that $\mathrm{T}_\mathfrak{p}\phi' = a_p\phi'$. It follows that

$$\mathbb{L}(E/K_n,1)_{(\mathfrak{p})} = \langle\phi', (\mathrm{T}_\mathfrak{p} - 1)\Delta'_K\rangle = (a_p - 1)\langle\phi', \Delta'_K\rangle = (a_p - 1)\mathbb{L}(E/K,1)_{(\mathfrak{p})}.$$

Likewise, we have, for all $t \geq 1$:

$$\begin{aligned}\mathbb{L}(E/K_n,1)_{(\mathfrak{p}^{t+1})} &= a_p\mathbb{L}(E/K_n,1)_{(\mathfrak{p}^t)} - p\mathbb{L}(E/K_n,1)_{(\mathfrak{p}^{t-1})} \\ &\equiv a_p\mathbb{L}(E/K_n,1)_{(\mathfrak{p}^t)} \pmod{p}.\end{aligned}$$

■

3 Regular Primes

We now make some remarks on hypothesis (iii) that occurs in Theorem 1.8. Assume, as in the statement of Theorem 1.8, that E has good ordinary reduction at p. Let $K_\infty = \mathbb{Q}(\mu_{p^\infty})$ and $k = \mathbb{Q}(\mu_p)$, and let $\Gamma = \mathrm{Gal}(K_\infty/k) \simeq \mathbb{Z}_p$ be the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of k. Let $X(E/K_\infty)$ denote the Pontryagin dual of $\mathrm{Sel}_p(E/K_\infty)$. We call p a *regular prime for E* if the following equivalent conditions are satisfied:

(i) $\mathrm{Sel}_p(E/K_\infty) = 0$;
(ii) $\mathrm{Sel}_p(E/K_\infty)$ is finite;
(iii) the characteristic ideal of $X(E/K_\infty)$ is trivial;

(iv) the Euler characteristic $\chi(E/K_\infty) := \dfrac{|H_0(\Gamma, X(E/K_\infty))|}{|H_1(\Gamma, X(E/K_\infty))|}$ is a p-adic unit;

(v) the number $\dfrac{|Ш(E/k)| \cdot |\widetilde{E}(\mathbb{F}_p)|^2 \cdot \prod_v c_v}{|E(k)|^2}$ is a p-adic unit, where $\widetilde{E}$ is the reduction of E at the unique prime of k above p, and c_v denotes the Tamagawa number of E at a finite place v of k.

The equivalence between (i) and (ii) is given by Matsuno's Theorem [Mat] that $X(E/K_\infty)$ is p-torsion-free. The remaining equivalences are well known.
The terminology of regular primes follows from the obvious analogy with the notion of regular prime in the theory of cyclotomic fields. We expect that if $r_E(\mathbb{Q}) = 0$, then there are infinitely many regular primes for E. Although this appears hard to prove, there is a readily computable criterion that allows one to test whether a given prime is regular, which is analogous to Kummer's criterion for regularity in terms of Bernoulli numbers, and rests on the notion of *modular symbols*.

Write $2\pi i f_0(z)dz$ for the holomorphic differential form on $\Gamma_0(N)\backslash\mathcal{H}$ attached to f_0. The modular symbol $[r]$ attached to $r \in \mathbb{Q}$ is the complex number defined by the formula

$$[r] := \int_r^{i\infty} 2\pi i f_0(z)dz.$$

The fact that the weight two modular form f_0 is periodic with period 1 implies that $[r]$ depends only on the value of r in $\mathbb{Q}/\mathbb{Z}$. The set of values taken on by $[r]$ as $r \in \mathbb{Q}/\mathbb{Z}$ generates a rank two lattice $\Pi_E \subset \mathbb{C}$, which is commensurable with the Néron lattice of E. This makes it possible to view $[r]$ as taking values in Π_E.

For $0 \leq j \leq p-2$, define the "j-th Bernoulli number attached to E" by the formula

$$B_E(j) = \sum_{r=1}^{p-1} \left[\frac{r}{p}\right] r^j \in \Pi_E.$$

Let $\Gamma = \mathrm{Gal}(K_\infty/k)$ and let $\Lambda(\Gamma)$ be its Iwasawa algebra. A construction originally due to Mazur and Swinnerton-Dyer attaches a p-adic L-function $\mathcal{G}_k \in \Lambda(\Gamma)$ to E and the cyclotomic $\mathbb{Z}_p$-extension K_∞/k. This p-adic L-function is defined in terms of modular symbols, and it follows directly from its definition that the following conditions are equivalent.

(i) $\mathcal{G}_k$ is a unit in the Iwasawa algebra $\Lambda(\Gamma)$;
(ii) under the isomorphism $\Lambda(\Gamma) \cong \mathbb{Z}_p[[T]]$, the constant term $\mathcal{G}_k(0)$ is p-adic unit;
(iii) p does not divide $B_E(j)$ for all $0 \leq j \leq p-2$.

We will say that a prime p is *analytically regular* for E if these equivalent conditions are satisfied.

Theorem 3.1 **(Kato)** *Let E be an elliptic curve defined over $\mathbb{Q}$ and p a good ordinary prime for E. Assume that $E[p]$ is an irreducible $G_\mathbb{Q}$-module. Then the characteristic ideal of $X(E/K_\infty)$ divides $\mathcal{G}_k\Lambda(\Gamma)$. In particular, if p is analytically regular for E, then p is regular for E.*

A computer program can be used to find the first few analytically regular primes for E by computing the numbers $B_E(j)$, much as Kummer's criterion can be used

to generate tables of regular primes. The following list gives some regular primes for the first few elliptic curves in Cremona's tables, and indicates the proportion of the primes $< 20,000$ that are analytically regular. (The authors are grateful to Jack Fearnley for performing these calculations.)

E	Analytically regular $p < 100$	Percentage $< 20,000$
$11A$	$3, 23, 31, 59, 67, 89, 97.$	27.5
$14A$	$3, 5, 13, 59, 61, 83.$	27.0
$15A$	$17, 23, 31, 79.$	27.0
$17A$	$3, 7, 11, 13, 23, 31, 53, 79.$	27.8
$19A$	$5, 7, 11, 17, 47, 61.$	28.0

Of course, it is expected that the converse to Theorem 3.1 holds, *i.e.*, that a prime p is analytically regular if and only if it is regular. The ongoing work of Skinner and Urban alluded to in the discussion of Conjecture 1.7 may shed some light on this converse.

Theorem 3.1 and the above table yield plenty of instances where the hypotheses made on E, p, and q in Theorem 1.8 are satisfied, proving that Theorem 1.8 is not vacuous. For the sake of illustration, we mention the following result.

Corollary 3.2 *Let $E\colon y^2 - y = x^3 - x^2$ be the (unique, up to isogeny) elliptic curve of conductor* 11*, and let p be one of the primes* $3, 23, 31, 59, 67, 89,$ *or* 97*. If Conjecture* 1.7 *is true, then*

$$r_E(\mathbb{Q}(\mu_{p^n}, 11^{1/p^n})) = p^n - 1, \quad r_E(\mathbb{Q}(11^{1/p^n})) = n.$$

The remainder of this article is devoted to explaining the proof of Theorem 1.8.

4 The Basic Strategy

We maintain the notations of the previous section and the assumptions in the statement of Theorem 1.8. Let us begin by listing a few facts about E and its behaviour over L_n that will be needed in the course of our study.

Lemma 4.1 *With notations and assumptions of Theorem* 1.8*, we have the following:*

(i) $E(L)[p^\infty] = 0$ *for any subfield L of L_∞.*
(ii) *The Shafarevich–Tate group $Ш(E/k)$ has trivial p-primary part.*
(iii) *The prime q is inert in K_∞ and $p \nmid \mathrm{ord}_q(q_{\mathrm{Tate}})$, where q_{Tate} denotes the period of the Tate curve E over the completion of k at the unique prime above q.*
(iv) $a_p \not\equiv 1 \pmod{p}$.
(v) $\mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^n})) = 0$ *for each $n \geq 0$.*
(vi) *The functional equation of the L-function $L(E/\mathbb{Q}(\mu_{p^n}), s)$ has sign $+1$.*
(vii) *Any elliptic curve isogenous to E still satisfies conditions* (i)–(iii) *in Theorem* 1.8.

Proof Part (i) of this lemma follows directly from the fact that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$ and that G has no quotient isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. Parts

(ii)–(iv) then follow from the characterisation (v) in the definition of a regular prime for E. To prove (v), let $\Gamma_n = \mathrm{Gal}(K_\infty/\mathbb{Q}(\mu_{p^n}))$. The kernel of the restriction map

$$\mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^n})) \longrightarrow \mathrm{Sel}_p(E/K_\infty)^{\Gamma_n}$$

is contained in $H^1(\Gamma_n, E_{p^\infty}(K_\infty))$ which is zero by (1), *i.e.*, this restriction map is injective. But $\mathrm{Sel}_p(E/K_\infty) = 0$ by assumption, and (v) follows. Now (vi) follows from (v) and the parity theorem in [Ne1, Prop. 12.5.9.5(iv)]. (See also [Do-TV2, Theorem 1.1] and [Ne2]; alternately, (vi) is also a consequence of Conjecture 1.7.) Part (vii) follows from the fact that $E[p]$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, in light of the fact that properties (i)–(iii) in Theorem 1.8 are preserved under isogenies of degree prime to p. ∎

For each integer $n \geq 1$, recall that $G_n = \mathrm{Gal}(L_n/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z}) \rtimes (\mathbb{Z}/p^n\mathbb{Z})^\times$ and that $K_n = \mathbb{Q}(\mu_{p^n})$. Let χ_n be any *faithful* character of $\mathrm{Gal}(L_n/K_n) \cong \mathbb{Z}/p^n\mathbb{Z}$ (*i.e.*, a surjective homomorphism to the group of p^n-th roots of unity). The induced representation $\rho_n := \mathrm{Ind}_{K_n}^{\mathbb{Q}} \chi_n$ is an absolutely irreducible rational representation of G_n of dimension $p^n - p^{n-1}$ which is faithful and does not depend on the choice of χ_n.

Lemma 4.2 *The representation ρ_n is the unique faithful irreducible representation of G_n. Any other irreducible representation of G_n factors through the group* $\mathrm{Gal}(L_{n-1}K_n/\mathbb{Q})$.

Theorem 1.8 is now a consequence of the following more precise statement.

Theorem 4.3 *Assume all the hypotheses of Theorem* 1.8. *Then for each $n \geq 0$,*

$$E(L_n) \otimes \mathbb{Q} \cong \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_n. \tag{4.1}$$

Our strategy to prove Theorem 4.3 is to proceed by induction on n. For $n = 0$, we have $L_n = F_n = \mathbb{Q}$, and there is nothing to show. So assume that

$$E(L_{n-1}) \otimes \mathbb{Q} = \rho_1 \oplus \cdots \oplus \rho_{n-1}.$$

In particular, $r_E(L_{n-1}) = p^{n-1} - 1$. Proposition 1.5 implies that $r_E(L_n) \leq p^n - 1$. To show that equality is attained, it is enough to prove that

$$\mathrm{Hom}_{G_n}(\rho_n, E(L_n) \otimes \mathbb{Q}) \neq 0, \tag{4.2}$$

which implies that $E(L_n) \otimes \mathbb{Q}$ contains exactly one copy of ρ_n, and therefore that (4.1) holds.

Note that (by Lemma 4.1(iii)) the prime q is inert in $K_n/\mathbb{Q}$. Denote by $\mathfrak{q}_n$ the unique prime of K_n above q. The prime $\mathfrak{q}_n$ is totally ramified in L_n/K_n, with ramification degree p^n. Let $\mathfrak{q}_n'$ denote the unique prime of L_n above $\mathfrak{q}_n$, and let $\mathcal{L}_n$ denote the completion of L_n at this prime. Finally let $\mathcal{O}_n$ denote the ring of integers of $\mathcal{L}_n$, and let $\mathcal{E}_n$ denote the Néron model of E over $\mathrm{Spec}(\mathcal{O}_n)$. By assumption, the elliptic

curve E has split multiplicative reduction at $\mathfrak{q}_n$. Thus E is a Tate curve over $\mathcal{L}_n$, and the group of connected components of $\mathcal{E}_n$ is isomorphic to

$$\mathcal{L}_n^\times / q_{\mathrm{Tate}}^{\mathbb{Z}} \mathcal{O}_{\mathcal{L}_n}^\times \simeq \mathbb{Z}/\operatorname{ord}_q(q_{\mathrm{Tate}})p^n\mathbb{Z}.$$

Let Φ_n denote the p-primary part of this group of connected components. By Lemma 4.1(iii), we know that $p \nmid \operatorname{ord}_q(q_{\mathrm{Tate}})$, and hence Φ_n is (canonically) isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. Write $\partial\colon \mathcal{E}_n(\mathcal{O}_n) \to \Phi_n$ for the specialization map to the group of connected components. We can also view ∂ as a map on $E(L_n)$ by the universal property of the Néron model.

The following proposition gives a useful criterion in terms of the specialisation map ∂ for equation (4.2) to be satisfied.

Proposition 4.4 *Let y be a point in $E(L_n)$ and let $V_y \subset E(L_n) \otimes \mathbb{Q}$ be the rational representation of G_n generated by y. If $\partial(y)$ has order p^n, then* $\operatorname{Hom}_{G_n}(\rho_n, V_y) \neq 0$.

Proof By Lemma 4.2, we only need to show that y does not belong to

$$E(L_n)_{\mathrm{tors}} + E(L'_{n-1}), \quad \text{where} \quad L'_{n-1} := L_{n-1}K_n.$$

Lemma 4.1(i) implies that $\partial(E(L_n)_{\mathrm{tors}}) = 0$, while the fact that $\mathfrak{q}$ has ramification degree p^{n-1} in L'_n implies that

$$\partial(E(L'_{n-1})) \subset p\Phi \simeq \mathbb{Z}/p^{n-1}\mathbb{Z}. \qquad \blacksquare$$

Proposition 4.4 reduces the proof of Theorem 1.8 to the problem of producing for each $n = 1, 2, \ldots$, an algebraic point $y_n \in E(L_n)$ such that $\partial(y_n)$ has order p^n in Φ_n. We will construct the point y_n as a Heegner point arising from an appropriate Shimura curve parametrisation of E.

5 Shimura Curves

In this section and the next, the integer $n \geq 1$ will be fixed. In order to lighten the notations, we will therefore supress it from the subscripts and write

$$F = \mathbb{Q}(\mu_{p^n})^+, \quad K = \mathbb{Q}(\mu_{p^n}), \quad \text{and} \quad L = L_n = \mathbb{Q}(\mu_{p^n}, q^{1/p^n}).$$

Let $\mathfrak{q}$ denote the unique prime of F above q, and let $F_\mathfrak{q}$ denote the completion of F at this prime. We will denote by $\mathcal{O}_{F_\mathfrak{q}}$ the ring of integers of $F_\mathfrak{q}$, and choose a uniformising element $\pi_\mathfrak{q}$ of $\mathcal{O}_{F_\mathfrak{q}}$. Finally, let $\mathbb{F}_\mathfrak{q} = \mathcal{O}_{F_\mathfrak{q}}/\pi_\mathfrak{q}$ denote the residue field of $F_\mathfrak{q}$ at $\mathfrak{q}$.

Let f be the Hilbert modular form obtained by abelian base change of f_0 to F so that $L(f, s) = L(E/F, s)$, $L(f_K, s) = L(E/K, s)$. Let ω be the quadratic Hecke character over F associated with the extension K/F. By Lemma 4.1(vi), the sign of the functional equation for $L(f_K, s)$ is $+1$. It follows that the set Σ' introduced in (1.3) has even cardinality.

Fix an infinite place τ of F, and let

$$\Sigma := \Sigma' \setminus \{\tau, \mathfrak{q}\}.$$

Let B be the quaternion algebra over F ramified exactly at the places of Σ. Let $\mathcal{O}_B$ be a maximal order of B and fix an isomorphism $\mathcal{O}_{B,\mathfrak{q}} \cong M_2(\mathcal{O}_{F_\mathfrak{q}})$. Let $R \subset \mathcal{O}_B$ be an Eichler order of B of discriminant prime to q. Let $g \in \widehat{\mathcal{O}}_B$ be an element whose component at $\mathfrak{q}$ is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi_\mathfrak{q} \end{smallmatrix}\right)$ and whose other components are 1. Let $R_0(\mathfrak{q})$ be the order of B defined by $B \cap (\widehat{R} \cap g\widehat{R}g^{-1})$. Let G be the algebraic group over F representing the functor on F-algebras $A \to (B \otimes_F A)^\times$. Consider the following two open compact subgroups of $G(\mathbb{A}_f)$: $U = \widehat{R}^\times$, $U_0(\mathfrak{q}) = \widehat{R_0(\mathfrak{q})}^\times$. Let $\mathcal{H} = \mathbb{C} - \mathbb{R}$ and let X and $X_0(\mathfrak{q})$ be the Shimura curves over F associated with $(G, \mathcal{H})$ of level U and $U_0(\mathfrak{q})$ respectively. They have complex points

$$X(\mathbb{C}) = G(F)\backslash \mathcal{H} \times G(\mathbb{A}_f)/U,$$
$$X_0(\mathfrak{q})(\mathbb{C}) = G(F)\backslash \mathcal{H} \times G(\mathbb{A}_f)/U_0(\mathfrak{q}).$$

These two (not necessarily connected) curves are equipped with two natural "degeneracy maps" $X_0(\mathfrak{q}) \to X$, denoted π_1 and π_2, respectively. These two maps satisfy $\pi_1 = \pi_2 \circ w_\mathfrak{q}$, where $w_\mathfrak{q}$ is the Atkin–Lehner involution at $\mathfrak{q}$. Let J and $J_0(\mathfrak{q})$ denote the Jacobians of X and $X_0(q)$, respectively.

Let Π be the automorphic representation for G such that the automorphic representation for $\mathrm{GL}_{2,F}$ corresponding to f is the Jacquet-Langlands lift of Π. Let ϕ be a new vector in Π. It is unique up to multiplication by a non-zero scalar and is an eigenvector of the Hecke algebra $\mathbb{T}_{U_0(\mathfrak{q})}$ of level $U_0(\mathfrak{q})$. The annihilator of the new line $\mathbb{C}\phi$ in $\mathbb{T}_{U_0(\mathfrak{q})}$ cuts out a quotient of $J_0(\mathfrak{q})$ which is isogenous to E over F.

Theorem 5.1 *The elliptic curve E is isogenous over F to a quotient of $J_0(\mathfrak{q})$.*

By eventually replacing E with another elliptic curve in its isogeny class, we will assume without loss of generality (by Lemma 4.1(vii)) that E is an *optimal* quotient of $J_0(\mathfrak{q})$, so that the modular parametrization

$$\eta\colon J_0(\mathfrak{q}) \longrightarrow E \tag{5.1}$$

has connected kernel.

The curves X and $X_0(\mathfrak{q})$ have canonical nodal models (in the sense of [Ed, Section 1]) over $\mathrm{Spec}(\mathcal{O}_{F_\mathfrak{q}})$, which will be denoted by $\mathcal{X}$ and $\mathcal{X}_0(\mathfrak{q})$ respectively. The special fiber of $\mathcal{X}_0(\mathfrak{q})$ is the union $C_0 \cup C_\infty$ of two copies of $\mathcal{X}_{/\mathbb{F}_\mathfrak{q}}$ intersecting transversally at the set X_{SS} of supersingular points of $\mathcal{X}_{/\mathbb{F}_\mathfrak{q}}$. A local equation in a neighbourhood of a supersingular point $\mathfrak{s} \in X_{SS}$ is given by $t_1 t_2 = \pi_\mathfrak{q}^{m_\mathfrak{s}}$, where $m_\mathfrak{s} = \#\,\mathrm{Aut}(\mathfrak{s})$. Assume for simplicity that $m_\mathfrak{s} = 1$ for all $\mathfrak{s} \in X_{SS}$. This can always be achieved at the cost of replacing the level structure U by a subgroup of finite index. It will simplify our subsequent discussion without altering any of its essential features to assume that this condition is satisfied.

The generic fiber of $\mathcal{X}_0(\mathfrak{q})$, viewed as a q-adic rigid analytic space, can be expressed as the union of two wide open spaces (in the terminology of Coleman [Cole]), denoted W_0 and W_∞, intersecting in a disjoint union of open annuli $A_\mathfrak{s}$ indexed by the elements of X_{SS}:

$$W_0 \cap W_\infty = \bigcup_{\mathfrak{s} \in X_{SS}} A_\mathfrak{s}.$$

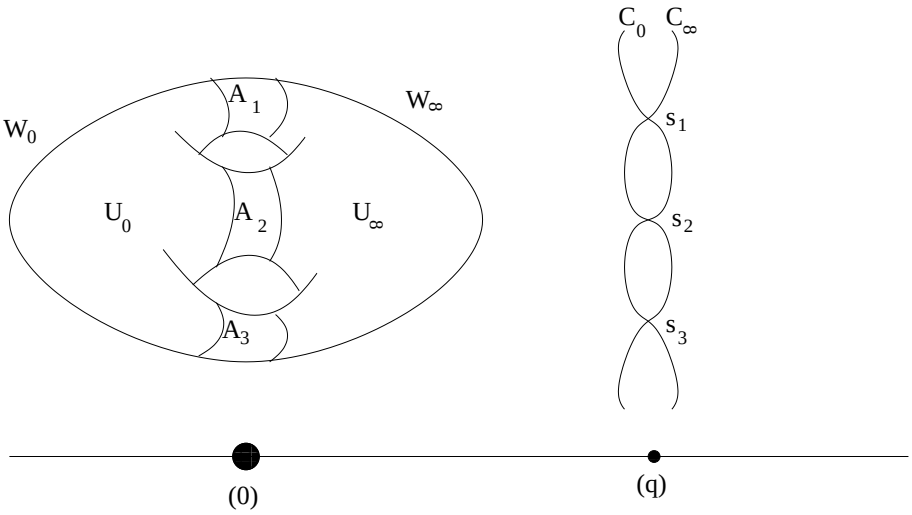

Figure 1: The nodal model of $X_0(\mathfrak{q})$ over $\mathrm{Spec}(\mathcal{O}_{F_\mathfrak{q}})$.

Let U_0 and U_∞ denote the largest affinoid subregions contained in W_0 and W_∞ respectively, so that $X_0(\mathfrak{q})(\bar{F}_\mathfrak{q})$ can be expressed as a disjoint union:

$$X_0(\mathfrak{q})(\bar{F}_\mathfrak{q}) = U_0 \cup U_\infty \cup \bigcup_{\mathfrak{s}\in X_{SS}} A_\mathfrak{s}.$$

Any point in $\mathcal{X}_0(\mathfrak{q})(F_\mathfrak{q})$ is contained in one of the affinoids U_0 and U_∞, and the Cartier divisor associated with such a point meets the special fiber at a smooth point, belonging to either C_0 or C_∞ (but not to both). The same also holds if $F_\mathfrak{q}$ is replaced by any unramified extension. For each $\mathfrak{s} \in X_{SS}$, choose a local parameter $j_\mathfrak{s}$ of $\mathcal{O}_{A_\mathfrak{s}}$ which identifies the annulus $A_\mathfrak{s}$ with the standard annulus in $\mathbb{C}_q$ defined by $\{|\pi_\mathfrak{q}| < |z| < 1\}$. We choose these local parameters in such a way that they give rise to compatible orientations in the sense of [Cole] on each of the annuli $A_\mathfrak{s}$. The situation (in the case where X has genus 0 and three supersingular points, labelled 1, 2, and 3, so that $X_0(\mathfrak{q})$ has genus two) is depicted in Figure 1.

Let $K_\mathfrak{q}$ be any unramified extension of $F_\mathfrak{q}$ and let $\mathcal{L}$ be a totally ramified extension of $K_\mathfrak{q}$ of degree d. We will write $\pi_\mathcal{L}$ for a uniformizing element of the ring of integers $\mathcal{O}_\mathcal{L}$ of $\mathcal{L}$, so that $(\pi_\mathcal{L}^d) = (\pi_\mathfrak{q})$.

Over the ramified base $\mathrm{Spec}(\mathcal{O}_\mathcal{L})$, the nodal model of $X_0(\mathfrak{q})$ is obtained by resolving the singularities of the special fiber by a sequence of blowups, so that the singular points of the two irreducible components C_0 and C_∞ of $\mathcal{X}_{\mathbb{F}_\mathfrak{q}}$ are now connected at each supersingular point by a chain of $d-1$ rational curves intersecting transversally at ordinary double points. Let $\ell_{\mathfrak{s},1}, \ldots, \ell_{\mathfrak{s},d-1}$ denote this chain of projective lines ordered in such a way that

(i) the line $\ell_{\mathfrak{s},1}$ intersects C_0 at the singular point $s_{\mathfrak{s},1}$ on C_0 attached to $\mathfrak{s}$;
(ii) the lines $\ell_{\mathfrak{s},j-1}$ and $\ell_{\mathfrak{s},j}$ intersect transversally in a singular point $s_{\mathfrak{s},j}$, for $j = 2, \ldots, d-1$; and

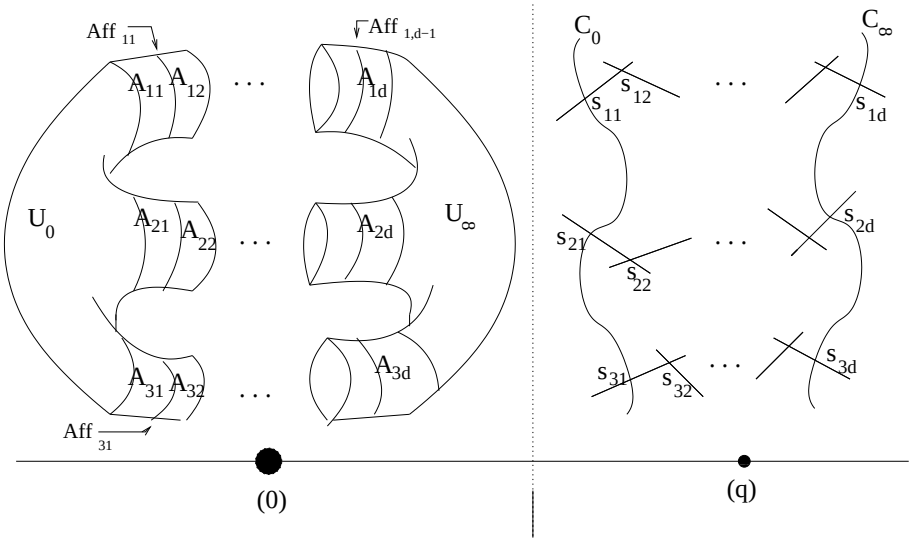

Figure 2: The nodal model of $X_0(\mathfrak{q})$ over $\mathrm{Spec}(\mathcal{O}_{\mathcal{L}})$.

(iii) the line $\ell_{\mathfrak{s},d-1}$ intersects C_∞ in the singular point $s_{\mathfrak{s},d}$ on C_∞ attached to $\mathfrak{s}$.

The reduction map from the $\mathcal{O}_{\mathcal{L}}$-points of the generic fiber to the smooth points of the special fiber can be described by introducing, for each $\mathfrak{s} \in X_{SS}$, the affinoid regions

$$\mathrm{Aff}_{\mathfrak{s},j} = \{\alpha \in A_{\mathfrak{s}} \text{ such that } |j_{\mathfrak{s}}(\alpha)| = |\pi_{\mathcal{L}}^j|\}, \qquad j = 1, \ldots, d-1.$$

The open annulus $A_{\mathfrak{s}}$ is a disjoint union of the $d-1$ affinoids $\mathrm{Aff}_{\mathfrak{s},j}$ with the open annuli of the form

$$A_{\mathfrak{s},j} = \{\alpha \in A_{\mathfrak{s}} \text{ such that } |\pi_{\mathcal{L}}^j| < j_{\mathfrak{s}}(\alpha)| < |\pi_{\mathcal{L}}^{j-1}|\}, \quad j = 1, \ldots, d.$$

On the level of $\mathcal{L}$-rational points, we have

$$A_{\mathfrak{s}}(\mathcal{L}) = \mathrm{Aff}_{\mathfrak{s},1}(\mathcal{L}) \cup \cdots \cup \mathrm{Aff}_{\mathfrak{s},d-1}(\mathcal{L}).$$

A point $P \in \mathcal{X}(\mathcal{L})$ on the ordinary locus reduces to a smooth point on one of the components C_0 or C_∞. If P belongs to the supersingular locus, its image under the reduction map is a smooth point on the unique irreducible component $\ell_{\mathfrak{s},j}$ such that P belongs to $\mathrm{Aff}_{\mathfrak{s},j}$. The nodal model of $X_0(\mathfrak{q})$ over $\mathrm{Spec}(\mathcal{O}_{\mathcal{L}})$ is represented schematically in Figure 2.

Let $\mathcal{G}$ denote the dual graph of the special fiber of $\mathcal{X}_0(\mathfrak{q})$ over $\mathrm{Spec}(\mathcal{O}_{\mathcal{L}})$. Its vertices are indexed by the irreducible components of this special fiber, and we will denote this set of vertices by

$$\mathcal{V}(\mathcal{G}) = \{v_0, v_\infty\} \cup \{v_{\mathfrak{s},j}, \text{ where } \mathfrak{s} \in X_{SS},\ j = 1, \ldots, d-1\}.$$

Figure 3: The dual graph $\mathcal{G}$ of the special fiber of $\mathcal{X}_0(\mathfrak{q})$ over $\mathrm{Spec}(\mathcal{O}_{\mathcal{L}})$.

Two vertices are joined by an edge if they intersect. The set $\mathcal{E}(\mathcal{G})$ of (ordered) edges of $\mathcal{G}$ is therefore in bijection with the singular points of the special fiber, and we write

$$\mathcal{E}(\mathcal{G}) = \{e_{\mathfrak{s},j},\ \text{where } \mathfrak{s} \in X_{SS},\ j = 1, \ldots, d.\}.$$

The dual graph of $\mathcal{X}_0(\mathfrak{q})$ over $\mathrm{Spec}(\mathcal{O}_{\mathcal{L}})$ is depicted in Figure 3. Note that it need not be connected, because $X_0(\mathfrak{q})$ may have several distinct components.

By reduction, a divisor on $\mathcal{X}_0(\mathfrak{q})(\mathcal{O}_{\mathcal{L}})$ gives rise to a formal integral linear combination of elements of $\mathcal{V}(\mathcal{G})$. Let

$$\mathrm{red}\colon\ \mathrm{Div}(\mathcal{X}_0(\mathfrak{q})) \longrightarrow \mathbb{Z}[\mathcal{V}(\mathcal{G})]$$

denote this reduction map. Let $\mathrm{Div}^0(X_0(\mathfrak{q}))$ denote the group of divisors which are homologically trivial (*i.e.*, whose restrictions to each component of the generic fiber are of degree zero). Given any $\Delta \in \mathrm{Div}^0(X_0(\mathfrak{q})(\mathcal{L}))$, write γ_Δ for any path in $\mathcal{G}$ (*i.e.*, element of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$) satisfying

$$\mathrm{boundary}(\gamma_\Delta) = \mathrm{red}(\Delta).$$

Note that the path γ_Δ is determined by this equation only up to elements of $H_1(\mathcal{G}, \mathbb{Z})$.

Assume now for simplicity of exposition that $\mathrm{ord}_{\pi_{\mathfrak{q}}}(q_{\mathrm{Tate}}) = 1$, so that $\mathcal{E}_{/F_{\mathfrak{q}}}$ has trivial group of connected components. This implies that the group Φ of connected components in the special fiber of $\mathcal{E}_{/\mathcal{O}_{\mathcal{L}}}$ is isomorphic to $\mathbb{Z}/d\mathbb{Z}$.

We now recall the description of the specialisation map

$$\partial \circ \eta\colon\ \mathrm{Div}^0(X_0(\mathfrak{q})(\mathcal{L})) \longrightarrow \mathbb{Z}/d\mathbb{Z}$$

that follows from the discussion in [Ed].

Let $\mathbf{1}_E$ be a generator of the character group of the torus attached to E, and let

$$\xi_E := \eta^*(\mathbf{1}_E)$$

denote its pullback under the modular parametrisation η. The element ξ_E can be viewed as an element of $\mathbb{Z}[X_{SS}]$. The set X_{SS} is identified with the double coset space

X' associated to the quaternion algebra B' introduced in (1.4). By the argument explained in [Rib], which adapts to the more general setting of Shimura curves over totally real fields, the fact that $\mathcal{E}_{/F_\mathfrak{q}}$ has a trivial group of connected components implies that the element ξ_E is indivisible. Since it belongs to the eigenspace for the Hecke algebra associated to f, it follows that

$$\xi_E = \pm\phi',$$

where ϕ' is the element introduced just before (1.6). After eventually adjusting the sign of ϕ', we can assume that $\xi_E = \phi'$.

To give a concrete description of the specialisation map to connected components, it is useful to view ξ_E as a function on the set $\mathcal{E}(\mathcal{G})$ of ordered edges of $\mathcal{G}$, by setting, for all $\mathfrak{s} \in X_{SS}$:

$$\langle \xi_E, e_{\mathfrak{s},1} \rangle = \cdots = \langle \xi_E, e_{\mathfrak{s},d} \rangle := \langle \xi_E, \mathfrak{s} \rangle.$$

We may extend ξ_E to $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ by $\mathbb{Z}$-linearity. Note then that $\langle \xi_E, \gamma \rangle := \xi_E(\gamma)$ belongs to $d\mathbb{Z}$, for all $\gamma \in H_1(\mathcal{G}, \mathbb{Z})$. In particular, if Δ is a degree 0 divisor on $X_0(\mathfrak{q})(\mathcal{L})$, the expression $\langle \xi_E, \gamma_\Delta \rangle$ is well defined in $\mathbb{Z}/d\mathbb{Z}$.

The following proposition is a reformulation of the main result of [Ed].

Proposition 5.2 *For all Δ in $\mathrm{Div}^0(X_0(\mathfrak{q})(\mathcal{L}))$, we have*

$$\partial \circ \eta(\Delta) = \langle \xi_E, \gamma_\Delta \rangle = \langle \phi', \gamma_\Delta \rangle.$$

6 Heegner Points

Fix an embedding $\rho\colon K \to B$. Assume that the maximal order $\mathcal{O}_B$ of B has been chosen to contain $\mathcal{O}_K$ and fix an isomorphism $\mathcal{O}_{B,\mathfrak{q}} \cong M_2(\mathcal{O}_{F_\mathfrak{q}})$. Finally, let $R \subset \mathcal{O}_B$ be an order of B containing $\mathcal{O}_K$ with relative discriminant $N/\mathfrak{q}$.

Let T be the algebraic group over F representing the functor $A \to (K \otimes_F A)^\times$ for any F-algebra A. We may regard T as a torus in G via the fixed embedding $\rho\colon K \to B$. Then $T(F) \hookrightarrow G(F)_+$ acts on $\mathcal{H}$. Let h_0 be the unique fixed point of $T(F)$ in the upper half plane $\mathcal{H}^+$. Then $X(\mathbb{C})$ is equipped with the set of CM points:

$$\begin{aligned} \mathbb{C}_U :&= G(F)_+ \backslash G(F)_+ h_0 \times G(\mathbb{A}_f)/U \\ &\simeq T(F) \backslash G(\mathbb{A}_f)/U, \end{aligned}$$

where the last identification is given by $[(h_0, g)] \to [g]$. By Shimura's theory, these CM points by K are defined over abelian extensions of K. More precisely, there is an action of $T(\mathbb{A}_f) \simeq \widehat{K}^\times$ on $\mathbb{C}_U$, given by the left multiplication on $G(\mathbb{A}_f)$. Shimura's reciprocity law asserts that this action factors through the reciprocity map $T(\mathbb{A}_f) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ and corresponds to the Galois action on $\mathbb{C}_U$. For a CM point $z = [g]$ in $\mathbb{C}_U$ with $g \in G(\mathbb{A}_f)$, the stabilizer of z in $T(\mathbb{A}_f)$ equals

$$U_z := T(F) \cdot (T(\mathbb{A}_f) \cap gUg^{-1}).$$

There exists a unique order $\mathcal{O}_c = \mathcal{O}_F + c\mathcal{O}_K$ of $\mathcal{O}_K$, with c a nonzero ideal of $\mathcal{O}_F$, such that $\widehat{\mathcal{O}}_c^\times = T(\mathbb{A}_f) \cap gUg^{-1}$. We say that the conductor of z is c.

Let λ be a prime of $\mathcal{O}_F$ which is relatively prime to $\mathfrak{q}$, and let $z_0 \in \mathbb{C}_U$ be a CM point by K of conductor λ. This point is defined over the ring class field $H[\lambda]$ of K of conductor λ. This ring class field is characterized by the reciprocity law isomorphism

$$\mathrm{Gal}(H[\lambda]/K) \simeq K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_K[\lambda]^\times$$

of class field theory, where we recall that $\mathcal{O}_K[\lambda] = \mathcal{O}_F + \lambda\mathcal{O}_K$ is the $\mathcal{O}_F$-order of K of conductor λ.

The fibers of z_0 under the maps $\pi_i \colon X_0(\mathfrak{q}) \to X$, $i = 1, 2$ are isomorphic to $\mathrm{Spec}\, H[\lambda\mathfrak{q}]$. The field $H[\lambda\mathfrak{q}]$ is a cyclic extension of $H[\lambda]$ which is totally ramified at all the primes of $H[\lambda]$ above $\mathfrak{q}$. Let $d_\lambda := [H[\lambda\mathfrak{q}] : H[\lambda]]$ denote the degree of $H[\lambda\mathfrak{q}]$ over $H[\lambda]$.

Choose any two closed points $z_1, z_2 \in X_0(\mathfrak{q})(H[\lambda\mathfrak{q}])$ satisfying

$$\pi_1(z_1) = z_0, \quad \pi_2(z_2) = z_0. \tag{6.1}$$

For each $\sigma \in \mathrm{Gal}(H[\lambda]/K)$, choose a lift $\tilde{\sigma} \in \mathrm{Gal}(H[\lambda\mathfrak{q}]/K)$ of σ to this group, and write

$$\Delta_{\lambda,\mathfrak{q}} = \sum_{\sigma \in \mathrm{Gal}(H[\lambda]/K)} (z_1 - z_2)^{\tilde{\sigma}} \in \mathrm{Div}^0(X_0(\mathfrak{q})(H[\lambda\mathfrak{q}])),$$

$$y_{\lambda,\mathfrak{q}} = \eta(\Delta_{\lambda,\mathfrak{q}}) \in E(H[\lambda\mathfrak{q}]),$$

where we recall that η is the modular parametrization of (5.1). Because the prime $\mathfrak{q}$ is inert in K/F, it splits completely in $H[\lambda]/K$. Choose a prime of $H[\lambda]$ above $\mathfrak{q}$ and write $\partial \colon E(H[\lambda\mathfrak{q}]) \to \mathbb{Z}/d_\lambda\mathbb{Z}$ for the associated projection onto the group Φ of connected components of E over $H[\lambda\mathfrak{q}]$ at this prime.

We remark that the lifts z_1 and z_2 are well defined by (6.1) up to translation by an element of $\mathrm{Gal}(H[\lambda\mathfrak{q}]/H[\lambda])$. Since this extension is totally ramified at the primes above $\mathfrak{q}$, and since the inertia groups at these primes act trivially on the connected components, the expression $\partial(y_{\lambda,\mathfrak{q}})$ does not depend on the choice of points z_1 and z_2 satisfying (6.1). For the same reason, it does not depend on the choice of lifts $\tilde{\sigma}$, which are well defined up to multiplication by elements in the inertia group at $\mathfrak{q}$. Finally, because the group $\mathrm{Gal}(H[\lambda]/K)$ acts transitively on the primes of $H[\lambda]$ above $\mathfrak{q}$, the expression $\partial(y_{\lambda,\mathfrak{q}})$ obtained through summing over the $\mathrm{Gal}(H[\lambda]/K)$-translates of the divisor $(z_1 - z_2)$ is also independent of the choice of this prime.

Theorem 6.1 *We have* $\partial(y_{\lambda,\mathfrak{q}})^2 = 4\mathbb{L}(E/K, 1)_{(\lambda)} \pmod{d_\lambda}$.

Proof Let

$$\Delta'_{K,\lambda} = \sum_{\mathfrak{s} \in X_{SS}} m(\mathfrak{s})\mathfrak{s} \in \mathbb{Z}[X']$$

denote the Heegner vector introduced in Section 2. It follows from [BD3, Appendix(2.3)] and Gross' work on quasi-canonical liftings of formal groups that (after eventually permuting z_1 and z_2 if necessary) we have

$$\mathrm{red}\Big(\sum_{\sigma \in \mathrm{Gal}(H[\lambda]/K)} z_1^{\tilde{\sigma}}\Big) = \sum_{\mathfrak{s} \in X_{SS}} m(\mathfrak{s})v_{\mathfrak{s},d_\lambda - 1},$$

$$\mathrm{red}\Big(\sum_{\sigma \in \mathrm{Gal}(H[\lambda]/K)} z_2^{\tilde{\sigma}}\Big) = \sum_{\mathfrak{s} \in X_{SS}} m(\mathfrak{s})v_{\mathfrak{s},1}.$$

Therefore we can choose

$$\gamma_{\Delta_{\lambda,\mathfrak{q}}} = \sum_{\mathfrak{s}\in X_{SS}} m(\mathfrak{s})(e_{\mathfrak{s},2} + \cdots + e_{\mathfrak{s},d_\lambda - 1}). \tag{6.2}$$

By Proposition 5.2,

$$\partial(y_{\lambda,\mathfrak{q}}) = \partial \circ \eta(\Delta_{\lambda,\mathfrak{q}}) = \langle \phi', \gamma_{\Delta_{\lambda,\mathfrak{q}}} \rangle. \tag{6.3}$$

Combining (6.2) and (6.3) gives

$$\partial(y_{\lambda,\mathfrak{q}}) = (d_\lambda - 2)\langle \phi', \Delta'_{K,\lambda} \rangle.$$

The theorem now follows after squaring both sides, in light of the definition of $\mathbb{L}(E/K,1)_{(\lambda)}$ given in (2.3). ∎

Let $L \subset H[\lambda\mathfrak{q}]$ be a cyclic extension of K of degree d which is totally ramified at $\mathfrak{q}$, and write

$$\Delta_L = \sum_{\sigma\in \mathrm{Gal}(H[\lambda\mathfrak{q}]/L)} (z_1 - z_2)^\sigma \in \mathrm{Div}^0(X_0(\mathfrak{q}))(L),$$

$$y_L = \eta(\Delta_L) \in E(L). \tag{6.4}$$

Theorem 6.2 *We have*

$$\partial(y_L)^2 = 4\mathbb{L}(E/K,1)_{(\lambda)} \pmod{d}.$$

Proof Since $\mathfrak{q}$ splits completely in $H[\lambda]/K$ and is totally ramified in L/K, the extensions L and $H[\lambda]$ are linearly disjoint over K. Therefore the natural homomorphism $\mathrm{Gal}(H[\lambda\mathfrak{q}]/L) \longrightarrow \mathrm{Gal}(H[\lambda]/K)$ is surjective. We may therefore choose the lifts $\tilde{\sigma}$ of σ in such a way that $\tilde{\sigma}$ belongs to $\mathrm{Gal}(H[\lambda\mathfrak{q}]/L)$. After defining $y_{\lambda,\mathfrak{q}}$ with this choice of lifts, we have

$$y_L = \mathrm{Norm}_{H[\lambda\mathfrak{q}]/LH[\lambda]}(y_{\lambda,\mathfrak{q}}),$$

where $LH[\lambda]$ is the compositum of L and $H[\lambda]$ and $\mathrm{Norm}_{H[\lambda\mathfrak{q}]/LH[\lambda]}$ is the norm to this field. Since all the primes of $LH[\lambda]$ above $\mathfrak{q}$ are totally ramified in $H[\lambda\mathfrak{q}]$, it follows that this norm element induces the natural projection map $\mathbb{Z}/d_\lambda\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$ from the group of connected components of E over $H[\lambda\mathfrak{q}]$ to the group of connected components over L. It follows from Theorem 6.1 that

$$\partial(y_L)^2 \equiv 4\mathbb{L}(E/K,1)_{(\lambda)} \pmod{d},$$

as was to be shown. ∎

7 Conclusion of the Proof

We can now prove Theorems 1.8 and 1.9.

Proof of Theorem 1.8. The extension $L = L_n = \mathbb{Q}(\mu_{p^n}, q^{1/p})$ is an abelian extension of $K = \mathbb{Q}(\mu_{p^n})$ which is unramfied outside $\mathfrak{p}$ and $\mathfrak{q}$ and is tamely ramified at $\mathfrak{q}$. This extension is also Galois over the totally real subfield $F = \mathbb{Q}(\mu_{p^n})^+$, and $\mathrm{Gal}(L/F)$ is a dihedral group. It follows from class field theory that L is contained in a ring class field of the form $H[\mathfrak{p}^t\mathfrak{q}]$ for a suitable $t \geq 1$. Let $y_n = y_L \in E(L)$ denote the Heegner point that was constructed in (6.4). By Theorem 6.2 and Lemma 2.1, we have

$$\begin{aligned}\partial(y_n)^2 &\equiv 4\mathbb{L}(E/K,1)_{(\mathfrak{p}^t)} \pmod{p^n}\\ &= 4(a_p-1)a_p^{t-1}\mathbb{L}(E/K,1) \pmod{p}.\end{aligned}$$

Recall that by Lemma 4.1 the Selmer group $\mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^n}))$ is trivial. Conjecture 1.7 for E and the quadratic extension K/F implies that the special value $\mathbb{L}(E/K,1)$ is a p-adic unit. Hence the same is true of $\partial(y_n)^2$, in light of Lemma 4.1(iv). Therefore $\partial(y_n)$ has order p^n, and Theorem 1.8 follows (by induction on n) from Proposition 4.4. ■

Proof of Theorem 1.9 The L-series $L(E/L)$ factors as a product of abelian L-series of E/K:

$$L(E/L,s) = \prod_{\chi\in\widehat{\mathrm{Gal}(L/K)}} L(E/K,\chi,s).$$

The factor $L(E/K,1)$ associated with the trivial character is non-vanishing by assumption, while the remaining p^n-1 factors each have a zero of odd order because of the sign in the functional equation of $L(E/K,\chi,s)$. Our proof that $\mathrm{rank}(E(L)) \geq p^n-1$ exhibited a Heegner point whose natural image in the χ-component $(E(L)\otimes\mathbb{C})^\chi$ is non-zero. It follows from Zhang's generalisation of the Gross–Zagier formula that each factor associated to a non-trivial χ has non-vanishing derivative. The method of Euler systems, as generalised to the setting of totally real fields in [KL] and [TZ] (and suitably adapted to non-trivial ring class characters, as in [BD1]) implies the second statement in Theorem 1.9. ■

Remark Theorem 4.3 completely determines the structure of $E(L_n)\otimes\mathbb{Q}$ as a representation for $\mathrm{Gal}(L_n/\mathbb{Q})$. One can therefore compute $r_E(L)$ for any subfield L of L_∞ finite over $\mathbb{Q}$ from this theorem. Let L be an arbitrary finite extension of $\mathbb{Q}$ contained in L_∞, let $K = L\cap K_\infty$. Define integers m,n,d by

$$[L:K] = p^n, \quad [K:\mathbb{Q}] = dp^{m-1} \quad \text{with} \quad d \mid p-1.$$

One can show that if $d \neq p-1$, then $L = K(q^{1/p^n})$ for some p^n-th root q^{1/p^n} of q, and if $d = p-1$, then $L = K(\zeta^{p^\ell}q^{1/p^n})$ with $0 \leq \ell \leq n-1$, where ζ is a primitive p^{n+m}-th root of unity.

Theorem 7.1 *Assume the hypotheses of Theorem* 1.8. *Then*

$$r_E(L) = \begin{cases} p^{\ell-1} - 1, & \text{if } d = p-1 \text{ and } 0 \le \ell < m, \\ d \cdot \frac{p^n-1}{p-1}, & \text{if } d \ne p-1 \text{ and } n \le m, \\ d \cdot \left(\frac{p^m-1}{p-1} + p^{m-1}(n-m) \right), & \text{otherwise.} \end{cases}$$

In particular, $r_E(L)$ *is equal to* $0, n$, *and* $p^n - 1$ *for* $L = \mathbb{Q}(\mu_{p^n})$, $\mathbb{Q}(q^{1/p^n})$, *and* L_n, *respectively.*

Acknowledgements The authors are grateful to John Coates for asking the question which motivated this work, and for his continued encouragement. They also thank Tim Dokchitser, Vladimir Dokchitser, and Shouwu Zhang for several helpful exchanges.

References

[BD1] M. Bertolini and H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields.* J. Reine Angew. Math. **412**(1990), 63–74. doi=10.1007/s002220050105

[BD2] _____, *Heegner points on Mumford–Tate curves.* Invent. Math. **126**(1996), no. 3, 413–456. doi:10.1007/s002220050105

[BD3] _____, *A rigid analytic Gross–Zagier formula and arithmetic applications.* Ann. of Math. **146**(1997), no. 1, 111–147. doi:10.2307/2951833

[BD4] _____, *Iwasawa's main conjecture for elliptic curves over anticyclotomic* $\mathbb{Z}_p$*-extensions.* Ann. of Math. (2) **162**(2005), no. 1, 1–64. doi:10.4007/annals.2005.162.1

[CFKS] J. Coates, T. Fukaya, K. Kato, and R. Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory.* J. Algebraic Geom. **19**(2010), no. 1, 19–97.

[Cole] R. F. Coleman, *A p-adic Shimura isomorphism and p-adic periods of modular forms.* In: *p*-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), Contemp. Math. 165, American Mathematical Society, Providence, RI, 1994, pp. 21–51.

[Cor] C. Cornut, *Mazur's conjecture on higher Heegner points.* Invent. Math. **148**(2002), no. 3, 495–523. doi:10.1007/s002220100199

[Do-TV1] T. Dokchitser and V. Dokchitser, *Computations in Non-commutative Iwasawa theory.* With an appendix by J. Coates and R. Sujatha. Proc. London Math. Soc. (3) **94**(2007), no. 1, 211–272. doi:10.1112/plms/pdl014

[Do-TV2] _____, *Self-duality of Selmer groups.* Math. Proc. Cambridge Philos. Soc. **146**(2009), no. 2, 257–267. doi:10.1017/S0305004108001989

[Do-V] V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves.* With an appendix by Tom Fisher. Proc. London Math. Soc. (3) **91**(2005), no. 2, 300–324. doi:10.1112/S0024611505015261

[Ed] Edixhoven, B., Appendix to [BD3].

[Gr] B. H. Gross. *Heights and the special values of L-series.* In: Number theory, CMS Conf. Proc. 7, American Mathematical Society, Providence, RI, 1987, pp. 115–187.

[Har] M. Harris. *Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields.* Invent. Math. **51** (1979), no. 2, 123–141. doi:10.1007/BF01390224

[HV] Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions.* Kazuya Kato's fiftieth birthday. Doc. Math. **2003**, Extra Vol., 443–478.

[Ka] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms.* In: Cohomologies *p*-adiques et applications arithmétiques. III. Astérisque **295**(2004), 117–290.

[Ko1] V. A. Kolyvagin, *The Mordell–Weil and Shafarevich–Tate groups for Weil elliptic curves.* Izv. Akad. Nauk SSSR Ser. Mat. **52**(1988), no. 6, 1154–1180, 1327; translation in Math. USSR-Izv. **33**(1989), no. 3, 473–499.

[Ko2] _____, *Euler systems.* In: The Grothendieck Festschrift, Vol. II, Prog. Math., 87, Birkhäuser, Boston, 1990, pp. 453–483.

[KL] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of* Ш *over totally real fields.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **55**(1991), no. 4, 851–876; translation in Math. USSR-Izv. **39**(1992), no. 1, 829–853.

[Lo] M. Longo, *On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields.* Ann. Inst. Fourier (Grenoble) **56**(2006), no. 3, 689–733.
[Ma] B. Mazur, *Rational points of abelian varieties with values in towers of number fields.* Invent. Math. **18**(1972), 183–266. doi:10.1007/BF01389815
[Mat] K. Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions.* J. Number Theory **99**(2003), no. 2, 415–443. doi:10.1016/S0022-314X(02)00078-1
[Ne1] J. Nekovar, *Selmer complexes.* Astérisque **310**(2006).
[Ne2] ———, *On the parity of ranks of Selmer groups IV.* Compositio Math. **145**(2009), no. 6, 1351–1359. doi:10.1112/S0010437X09003959
[Rib] K. Ribet. Letter to J-F. Mestre. in arXiv:math.AG/0105124.
[Ro] D.E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers.* Invent. Math. **75**(1984), no. 3, 409–423. doi:10.1007/BF01388636
[Sk] Christopher Skinner, *Main conjectures and modular forms*, Current Developments in Mathematics **2004**(2006), 141–161.
[TZ] Y. Tian and S. Zhang, *Kolyvagin systems of Heegner points on Shimura curves*. Forthcoming, Higher Education Press, Beijing, 2011.
[Va1] V. Vatsal, *Uniform distribution of Heegner points.* Invent. Math. **148**(2002), no. 1, 1–46. doi:10.1007/s002220100183
[Va2] ———, *Special values of anticyclotomic L-functions.* Duke Math. J. **116**(2003), no. 2, 219–261. doi:10.1215/S0012-7094-03-11622-1
[Zh1] S. Zhang, *Height of Heegner points on Shimura curves.* Ann. of Math. (2) **153**(2001), no. 1, 27–147. doi:10.2307/2661372
[Zh2] ———, *Gross–Zagier formula for* GL_2. Asian J. Math. **5**(2001), no. 2, 183–290.
[Zh3] ———, *Gross–Zagier formula for* $\mathrm{GL}(2)$. *II.* In: Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 191–214.

Department of Mathematics, McGill University, Montréal, PQ H3A 2T5
e-mail: darmon@math.mcgill.ca

Academy of Mathematics and System Science, Chinese Academy of Sciences, Beijing100190, P.R.China
e-mail: ytian@math.ac.cn