THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR $\mathbb{Q}$-CURVES AND ODA' S PERIOD RELATIONS

HENRI DARMON, VICTOR ROTGER AND YU ZHAO

To Takayuki Oda on his 60th birthday.

Contents

1. Introduction

Let E be an elliptic curve over a number field F and let $L(E/F,s)$ denote its Hasse-Weil L-series. It is widely believed that the Shafarevich-Tate group $Ш(E/F)$ is finite and that $L(E/F,s)$ extends to an entire function of the complex variable s. The order of vanishing of this function at $s=1$, denoted by $r_{\mathrm{an}}(E/F)$, is commonly referred to as the *analytic rank* of E over F, a terminology justified by the Birch and Swinnerton-Dyer conjecture which asserts that

$$\mathrm{rank}(E(F)) \stackrel{?}{=} r_{\mathrm{an}}(E/F). \tag{1}$$

The most convincing evidence for the Birch and Swinnerton-Dyer conjecture is the fact that it is proved when $F=\mathbb{Q}$ and $L(E,s):=L(E/\mathbb{Q},s)$ has at most a simple zero at $s=1$:

Theorem 1.1 (Gross-Zagier, Kolyvagin)**.** *If $r_{\mathrm{an}}(E/\mathbb{Q})\leq 1$, then* (1) *holds for $E/\mathbb{Q}$, and $Ш(E/\mathbb{Q})$ is finite.*

The proof of Theorem 1.1, which is briefly recalled in Section 2.1, rests on two key ingredients. The first is the modularity of E, in the strong geometric form which asserts that E is a quotient of the Jacobian of a modular curve over $\mathbb{Q}$. The second is the collection of Heegner points on this modular curve, which satisfies the axioms of an "Euler system" and provides a valuable bridge between the arithmetic of E and the analytic behaviour of its L-series.

Both these ingredients are available in greater generality, most notably when F is a *totally real field*. In this setting, a modular elliptic curve E over F is said to satisfy the *Jacquet-Langlands hypothesis* (JL) if either $[F:\mathbb{Q}]$ is odd, or there is at least one prime of F at which the automorphic form on $\mathrm{GL}_2(\mathbb{A}_F)$ attached to E is not in the principal series. Here, $\mathbb{A}_F$ stands for the ring of adèles of F. The

The research of the second author is financially supported by DGICYT Grant MTM2009-13060-C02-01 and the Grup de recerca consolidat de Catalunya 2009 SGR 1220.

meaning of condition (JL), which only fail to hold for certain elliptic curves of square conductor, is described more concretely in Section 2.1.

Most importantly for the proof of (1), the Jacquet-Langlands hypothesis implies that E is the quotient of the Jacobian of a suitable Shimura curve over F. Shimura curves are equipped with a plentiful supply of CM points, which have been parlayed into the proof of the following number field generalisation of Theorem 1.1.

Theorem 1.2 (Zhang)**.** *Let E be a modular elliptic curve over a totally real field F satisfying (JL). If $r_{\mathrm{an}}(E/F) \leq 1$, then $Ш(E/F)$ is finite and (1) holds for E/F.*

Denote by $\mathfrak{N}$ the conductor of E/F. If either $[F:\mathbb{Q}]$ is odd or there exists a prime $\mathfrak{p}$ of F for which $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{N}) = 1$, this is Theorem A of [Zh]. The full result in which E is only assumed to satisfy (JL) follows from the subsequent strengthening of the Gross-Zagier formula proven in [YZZ]. Both results are discussed further in Section 2.1.

In analytic rank zero, the Jacquet-Langlands hypothesis can be dispensed with:

Theorem 1.3 (Longo)**.** *Let E be a modular elliptic curve over a totally real field F. If $L(E/F,1) \neq 0$, then $E(F)$ and $Ш(E/F)$ are finite.*

Longo's proof [Lo], building on the approach of [BD], exploits the theory of congruences between modular forms to realise the Galois representation $E[p^n]$ in the Jacobian of a Shimura curve X_n whose level may (and indeed does) depend on n. The Euler system of CM points on X_n then gives rise to a collection of p^n-torsion cohomology classes which is used to bound the p^n-Selmer group of E over F independently of n, and thereby obtain the finiteness of $E(F)$ and $Ш(E/F)$.

The problem of removing the Jacquet-Langlands hypothesis from Theorem 1.2—or equivalently, of extending Theorem 1.3 to the case where $L(E/F,s)$ has a simple zero at $s=1$—is still very much open.

To better understand the difficulty which arises, it is instructive to examine the simplest setting where the Jacquet-Langlands hypothesis fails to hold. Assume for the rest of the introduction that F is a real quadratic field, and consider for now the case where E/F is an elliptic curve of conductor 1.

Assuming E is modular, the L-series $L(E/F,s)$ is known to have a functional equation relating its values at s and $2-s$, and the sign $w_E \in \{-1,1\}$ in this functional equation is always equal to 1 in this case.

Let M be any quadratic extension of F, let

$$\chi_M : G_F \longrightarrow \pm 1$$

be its associated Galois character, and denote by E_M the twist of E over F by χ_M, so that the L-series $L(E/M,s)$ factors as

$$L(E/M,s) = L(E/F,s)L(E/F,\chi_M,s) = L(E/F,s)L(E_M/F,s).$$

Since E has conductor 1, the sign w_{E_M} of the twisted L-series is controlled by the local signs attached to the archimedean places ∞_1 and ∞_2 of F, which are equal to $\chi_M(\infty_1)$ and $\chi_M(\infty_2)$ respectively. It follows that $w_{E_M} = 1$ if M is either totally real or CM. In particular, the elliptic curve E is always of *even* analytic rank over such M. Since an Euler system of Heegner points attached to a quadratic CM extension M/F is only expected to be available when E has odd analytic rank over M, this suggests that the mathematical objects so crucial in Kolyvagin's descent method may be unavailable for elliptic curves of conductor 1.

A similar expectation can be derived more generally for all elliptic curves which do not satisfy (JL). Indeed, if E/F is an elliptic curve of square conductor $\mathfrak{N}$ and M is a quadratic extension of F which is unramified at the primes dividing $\mathfrak{N}$, then the same analysis as above reveals that

$$r_{\mathrm{an}}(E/M) \equiv \begin{cases} 0 \pmod 2, & \text{if } M \text{ is CM or totally real;} \\ 1 \pmod 2 & \text{otherwise.} \end{cases} \tag{2}$$

A quadratic extension M of F which is neither CM nor totally real is called an *ATR extension* of F. An ATR extension of F thus has two real places and one complex place. (The acronym "ATR" stands for "Almost Totally Real", and is used more generally in [DL] to designate quadratic extensions of a totally real field having exactly one complex place.)

The present article is motivated by the following specific instance of the Birch and Swinnerton-Dyer conjecture which emerges naturally from the discussion above.

Conjecture 1.4. *Let E be a (modular) elliptic curve over a real quadratic field F of square conductor $\mathfrak{N}$ for which $w_E = 1$, and let M/F be an ATR extension of F of discriminant prime to $\mathfrak{N}$. If $L'(E_M/F, 1) \neq 0$, then $E_M(F)$ has rank one and $Ш(E_M/F)$ is finite.*

Although it seems tantalisingly close to the setting of Theorem 1.2, Conjecture 1.4 presents a real mystery and appears to lie beyond the reach of known methods. The difficulty is that, in the absence of the Jacquet-Langlands hypothesis, no natural "modular" method presents itself in general for constructing the point of infinite order on $E_M(F)$ whose existence is predicted by the Birch and Swinnerton–Dyer conjecture.

One of the original motivations for singling out Conjecture 1.4 for special study lies in the conjectural construction of a so-called *Stark-Heegner point* $P_M^? \in E(M)$ described in [DL]. This construction, which is recalled briefly in Section 2.2, involves the images under a complex Abel-Jacobi map attached to the Hilbert modular form associated to E/F of certain "ATR cycles" indexed by ideals of M. The ATR cycles are null-homologous cycles of real dimension one on the corresponding Hilbert modular surface. It is conjectured in [DL] that the point $P_M^?$ is of infinite order precisely when $L'(E/M, 1) \neq 0$, and that $P_M^?$ is part of a norm-coherent collection of points defined over abelian extensions of M satisfying Euler-System-like properties. However, progress on Conjecture 1.4 through the theory of ATR cycles is thwarted by our inability to provide much theoretical evidence for the conjectures of [DL] at present.

The first aim of this note is to study Conjecture 1.4 for the class of elliptic curves E/F which are isogenous over F to their Galois conjugate. Following a terminology that was first introduced by Ribet in [Ri], these elliptic curves are called $\mathbb{Q}$-*curves*. Their basic properties are reviewed in Section 3. As explained in that section, the case of $\mathbb{Q}$-curves is ultimately made tractable by the existence of a classical elliptic cusp form f (with *non-trivial* nebentypus character in general) satisfying

$$L(E/F, s) = L(f, s)L(\bar{f}, s),$$

leading to a modular parametrisation of E by a classical modular curve $X_1(N)$ for a suitable $N \geq 1$. The main theorem of Section 3 is a proof of Conjecture 1.4 for $\mathbb{Q}$-curves:

Theorem 1.5. *Let E/F be a $\mathbb{Q}$-curve of square conductor $\mathfrak{N}$, and let M/F be an ATR extension of F of discriminant prime to $\mathfrak{N}$. If $L'(E_M/F, 1) \neq 0$, then $E_M(F)$ has rank one and $Ш(E_M/F)$ is finite.*

The key ingredients in the proof of Theorem 1.5 are a strikingly general recent extension of the theorem of Gross-Zagier obtained by Xinyi Yuan, Shouwu Zhang and Wei Zhang [YZZ] covering cusp forms with possibly non-trivial nebentypus characters, and a strengthening of Kolyvagin's descent method to cover abelian variety quotients of $J_1(N)$, as worked out in the forthcoming book of Ye Tian and Shouwu Zhang [TZ]. Section 3 explains how Theorem 1.5 follows from these results and the *Artin formalism* for certain Rankin L-series.

The second part of the article focuses on the special case where the $\mathbb{Q}$-curve E is of conductor 1. Such elliptic curves, which were first systematically studied by Shimura [Shim], are essentially in bijection with newforms f in $S_2(\Gamma_0(N), \varepsilon_N)$ with quadratic Fourier coefficients, where N is the discriminant of the real quadratic field F, and

$$\varepsilon_N : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \pm 1$$

is the corresponding even Dirichlet character.

Section 4 describes the explicit construction, for all quadratic ATR extensions M of F, of a canonical point $P_M \in E(M)$ arising from suitable CM divisors on $X_1(N)$. The trace to $E(F)$ of P_M is shown to vanish, so that P_M can also be viewed as an F-rational point on the twisted curve E_M.

After explaining how the points P_M can be computed complex analytically by integrating the elliptic modular form f, we tabulate these points for a few ATR extensions M of small discriminant. One expects that the height of the point P_M is related in a simple way to $L'(E_M/F, 1)$.

Finally, Conjecture 4.7 spells out a precise conjectural relationship between the *classical* Heegner point P_M and the Stark-Heegner point $P_M^?$ arising from ATR cycles on the Hilbert modular variety. This conjecture, which relates certain complex analytic invariants attached to an elliptic modular form f and its Doi-Naganuma lift, can be viewed as an analogue for Abel-Jacobi maps of Oda's period relations which are formulated in [Oda]. It is therefore a pleasure to dedicate this article to Takayuki

Oda whose work on periods of Hilbert modular surfaces was a major source of inspiration for the conjectures of [DL].

It is also a pleasure to thank Xavier Guitart, Ariel Pacetti and David Rohrlich for their comments on a previous version of this manuscript.

2. Background

2.1. **The Birch and Swinnerton-Dyer conjecture in low analytic rank.** We begin by recalling in greater detail the main ideas behind the proofs of Theorems 1.1 and 1.2. We start with the assumption that F is a number field and write $\mathcal{O}_F$ for its ring of integers. Let $\mathfrak{N} \subset \mathcal{O}_F$ denote the conductor of the elliptic curve E/F.

The proofs of Theorems 1.1 and 1.2 can be broken up into five steps:

(i) *Modularity*: When $F = \mathbb{Q}$, the main results of [Wi] and [TW] (as completed in [BCDT]) imply that there is a normalised newform f of weight 2 on $\Gamma_0(N)$ satisfying $L(E, s) = L(f, s)$. In particular, $L(E, s)$ has an analytic continuation to the left of the half plane $\mathrm{Re}(s) > 3/2$, and its order of vanishing at $s = 1$ is therefore well defined. For general F, the modularity of E/F is just the assertion that $L(E/F, s)$ is the L-series attached to an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$. Such a property is predicted to hold, as a (very special) case of the Langlands functoriality conjectures. In spite of the powerful ideas introduced into the subject building on Wiles' breakthrough, a proof in the general number field setting still seems a long way off. When F is totally real, modularity can be phrased in terms of modular forms much as in the case $F = \mathbb{Q}$. Namely, E/F is modular whenever there is a normalised Hilbert modular eigenform f of parallel weight 2 on the congruence group $\Gamma_0(\mathfrak{N}) \subseteq \mathrm{SL}_2(\mathcal{O}_F)$ satisfying $L(E/F, s) = L(f, s)$. The methods originating from Wiles' work seem well suited to yield a proof of modularity of all elliptic curves over totally real fields. (See for example the works of Skinner-Wiles [SkWi], Fujiwara [Fu], Jarvis-Manoharmayum [JM] and the references therein for an overview of the significant progress that has been achieved in this direction.) Currently, the case which offers most difficulties arises when the residual Galois representation at 3 is *reducible*.

(ii) *Geometric modularity*: Thanks to the geometric construction of Eichler-Shimura and to Faltings' proof of the Tate conjecture for abelian varieties over number fields, the modularity of E in the case where $F = \mathbb{Q}$ can be recast as the statement that E is a quotient of the jacobian $J_0(N)$ of the modular curve $X_0(N)$ over $\mathbb{Q}$, where $\mathfrak{N} = (N)$, $N \geq 1$. A non-constant morphism

$$\pi_E : J_0(N) \longrightarrow E \tag{3}$$

of abelian varieties over $\mathbb{Q}$ is called a *modular parametrisation* attached to E.

When F is a totally real field and E/F is known to be modular, the modular parametrisation arising from Eichler-Shimura theory admits no counterpart in general. However, such a modular parametrisation can be obtained when the Jacquet-Langlands hypothesis formulated in the introduction holds. More precisely, as it is explained in [Zh, §3], hypothesis (JL) implies that E is a quotient of the Jacobian of a suitable Shimura curve X attached to an order in a quaternion algebra over F which splits at exactly one archimedean place of F. That is, there is a non-constant map

$$\pi_E : J(X) \longrightarrow E \tag{4}$$

of abelian varieties over F generalising (3). The condition that the automorphic form $\pi = \otimes \pi_v$ attached to E be a principal series representation at a place v of F is satisfied precisely when E acquires good reduction over an abelian extension of F_v. For $v \nmid 2$, the meanings of various conditions on the local representations π_v in terms of the behaviour of E over F_v are summarised in the table below.

(5)

π_v	E/F_v	$\mathrm{ord}_v(\mathfrak{N})$
Unramified principal series	Good reduction over F_v	0
Principal series	Good reduction over an abelian extension of F_v	even
Steinberg	Potentially multiplicative reduction over F_v	1 or 2
Supercuspidal	Otherwise	≥ 2

We refer the reader to [Ge, p. 73], [Pa], [Ro, Prop. 2], [Ro2, Prop. 2 and 3] for proofs of these statements. (Note that, although in the latter article the ground field is assumed to be $F = \mathbb{Q}$,

the results remain valid for arbitrary F as the questions at issue are purely local). See [Pa] for the behaviour at places v above 2.

In particular, an elliptic curve which fails to satisfy hypothesis (JL) is necessarily of square conductor. The converse is not true, but note that it also follows from the table that all elliptic curves of conductor 1 over a totally real number field of even degree fail to satisfy (JL). We will often restrict our attention to elliptic curves of square conductor, thus encompassing all elliptic curves that do not satisfy hypothesis (JL).

(iii) *Heegner points and L-series*: Suppose first that $F = \mathbb{Q}$ and let K be an imaginary quadratic field of discriminant relatively prime to N and satisfying the

Heegner hypothesis: $\mathcal{O}_K$ has an ideal $\mathcal{N}$ of norm N satisfying $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$.

An ideal $\mathcal{N}$ of K with this property is sometimes called a *cyclic ideal* of norm N. When the Heegner hypothesis is satisfied, it can be shown that the L-function $L(E/K, s)$ has sign -1 in its functional equation, and therefore vanishes at $s = 1$. The CM points on $X_0(N)$ attached to the moduli of elliptic curves with complex multiplication by $\mathcal{O}_K$, and their images under π_E, can be used to construct a canonical point $P_K \in E(K)$: the so-called *Heegner point* on E attached to K. The main result of [GZ] expresses $L'(E/K, 1)$ as a multiple by a simple non-zero scalar of the Néron-Tate height of P_K. In particular, the point P_K is of infinite order if and only if $L'(E/K, 1) \neq 0$.

In the setting where F is a totally real field, the Shimura curve X is equipped with an infinite supply of CM points enjoying properties similar to their counterparts on modular curves. The auxiliary field K is now a totally complex quadratic extension of F satisfying a suitable Heegner hypothesis relative to X. The CM points attached to K can be used to construct a canonical point $P_K \in E(K)$ as in the case $F = \mathbb{Q}$. A general extension of the Gross-Zagier theorem ([Zh, Theorem C]) to this context relates the height of P_K to the derivative $L'(E/K, 1)$. In particular, the point P_K is of infinite order precisely when $L(E/K, s)$ has a simple zero at $s = 1$. We emphasise that this more general Heegner point construction relies crucially on E/F satisfying hypothesis (JL).

(iv) *The Euler system argument*: The Heegner point P_K does not come alone, but can be related to the norms of algebraic points on E defined over abelian extensions of K. Using this fact, it is shown in [Ko] in the case $F = \mathbb{Q}$ that the point P_K, when it is of infinite order, necessarily generates $E(K) \otimes \mathbb{Q}$. Koyvagin's argument extends without essential difficulties to the context of Shimura curves over totally real fields (cf. [KL2], [Zh, §7.2], or the forthcoming book [TZ]).

(v) *Descending from K to F*: Assume first that $F = \mathbb{Q}$. If $\mathrm{ord}_{s=1}(L(E, s)) \leq 1$, the analytic non-vanishing results of [BFH] or [MM] produce an imaginary quadratic field K satisfying the Heegner hypothesis, and for which $L(E/K, s)$ has a simple zero at $s = 1$. By the Gross-Zagier theorem, the Heegner point P_K generates $E(K)$, and its trace therefore generates $E(\mathbb{Q})$. The known properties of the Heegner point P_K imply in particular that its trace to $\mathbb{Q}$ vanishes when $L(E, 1) \neq 0$, and is of infinite order when $L(E, 1) = 0$. Theorem 1.1 for $E/\mathbb{Q}$ follows from this. The proof of Theorem 1.2 is deduced similarly, by noting that the analytic non-vanishing results of [BFH] or [Wa] generalize to any number field and again produce a totally complex imaginary quadratic extension K/F satisfying the Heegner hypothesis for which $\mathrm{ord}_{s=1}(L(E/K, s)) = 1$.

2.2. **Oda's period relations and ATR points.** . This section briefly recalls the main construction of [DL] which to any ATR extension M of F (satisfying a suitable Heegner condition) associates a point $P_M \in E(\mathbb{C})$ belonging conjecturally to $E(M)$. The points P_M arise by considering the images of certain *non-algebraic* cycles on Hilbert modular varieties under a map which is formally analogous to the Griffiths-Weil Abel-Jacobi maps on null-homologous algebraic cycles.

The general setting. We begin by treating a more general context where F is a totally real field of degree $r + 1$. (This extra generality does not unduly complicate the notations, and may even clarify some of the key features of the construction.) Fix an ordering $v_0, v_1, \ldots, v_r$ of the $r+1$ distinct real embeddings of F. Let E be an elliptic curve over F, and let

$$E_j := E \otimes_{v_j} \mathbb{R} \qquad (0 \leq j \leq r)$$

be the $r+1$ elliptic curves over $\mathbb{R}$ obtained by taking the base change of E to $\mathbb{R}$ via the embedding v_j. To ease the exposition, we will make the following inessential assumptions:

(1) The field F has narrow class number one;
(2) the conductor of E/F is equal to 1 (i.e., E has everywhere good reduction).

(For a more general treatment where these assumptions are significantly relaxed, see for instance the forthcoming PhD thesis [Gar].)

The Hilbert modular form G on $\mathrm{SL}_2(\mathcal{O}_F)$ attached to E is a holomorphic function on the product $\mathcal{H}_0\times\mathcal{H}_1\times\cdots\times\mathcal{H}_r$ of $r+1$ copies of the complex upper half plane, which is of parallel weight $(2,2,\dots,2)$ under the action of the Hilbert modular group $\mathrm{SL}_2(\mathcal{O}_F)$. The latter group acts discretely on $\mathcal{H}_0\times\cdots\times\mathcal{H}_r$ by Möbius transformations via the embedding

$$(v_0,\dots,v_r):\mathrm{SL}_2(\mathcal{O}_F)\longrightarrow \mathrm{SL}_2(\mathbb{R})^{r+1}.$$

Because of this transformation property, the Hilbert modular form G can be interpreted geometrically as a holomorphic differential $(r+1)$-form on the complex analytic quotient

$$X(\mathbb{C}):=\mathrm{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}_0\times\mathcal{H}_1\times\cdots\times\mathcal{H}_r), \tag{6}$$

by setting

$$\omega_G^{\mathrm{hol}}:=(2\pi i)^{r+1}G(\tau_0,\dots,\tau_r)d\tau_0\cdots d\tau_r.$$

It is important to replace ω_G^{hol} by a closed, but non-holomorphic differential $(r+1)$-form ω_G on $X(\mathbb{C})$. When $r=1$, the differential ω_G is defined by choosing a unit $\epsilon\in\mathcal{O}_F^\times$ of norm -1 satisfying

$$\epsilon_0:=v_0(\epsilon)>0,\qquad \epsilon_1:=v_1(\epsilon)<0,$$

and setting

$$\omega_G=(2\pi i)^2\left(G(\tau_0,\tau_1)d\tau_0d\tau_1-G(\epsilon_0\tau_0,\epsilon_1\bar\tau_1)d\tau_0d\bar\tau_1\right).$$

For general r, one defines ω_G similarly, but this time summing over the subgroup of $\mathcal{O}_F^\times/(\mathcal{O}_F^+)^\times$ of cardinality 2^r consisting of units ϵ with $v_0(\epsilon)>0$. Note that the closed $(r+1)$-form ω_G is holomorphic in τ_0, but only harmonic in the remaining variables $\tau_1,\dots,\tau_r$. The justification for working with ω_G rather than ω_G^{hol} lies in the following statement which is a reformulation of a conjecture of Oda [Oda] in the special case of modular forms with rational fourier coefficients:

Conjecture 2.1 (Oda)**.** *Let*

$$\Lambda_G:=\left\{\int_\gamma\omega_G,\quad \gamma\in H_{r+1}(X(\mathbb{C}),\mathbb{Z})\right\}.$$

Then Λ_G is a lattice in $\mathbb{C}$ and the elliptic curve $\mathbb{C}/\Lambda_G$ is isogenous to E_0.

In [Oda], this conjecture is shown to hold for Hilbert modular forms which are base change lifts of classical elliptic modular forms, which corresponds to the case where the associated elliptic curve E is a $\mathbb{Q}$-curve. But it should be emphasised that no $\mathbb{Q}$-curve hypothesis on E is necessary in Conjecture 2.1.

Let

$$\mathcal{Z}_r(X(\mathbb{C})):=\left\{\begin{array}{c}\text{Null-homologous cycles}\\ \text{of real dimension } r\\ \text{on } X(\mathbb{C})\end{array}\right\}.$$

Conjecture 2.1 makes it possible to define an "Abel-Jacobi map"

$$\mathrm{AJ}_G:\mathcal{Z}_r(X(\mathbb{C}))\longrightarrow E_0(\mathbb{C}), \tag{7}$$

by choosing an isogeny $\iota:\mathbb{C}/\Lambda_G\longrightarrow E_0(\mathbb{C})$, and setting

$$\mathrm{AJ}_G(\Delta):=\iota\left(\int_{\tilde\Delta}\omega_G\right),\qquad (\text{for any } \tilde\Delta \text{ with } \partial\tilde\Delta=\Delta). \tag{8}$$

Note that the domain $\mathcal{Z}_r(X(\mathbb{C}))$ of AJ_G has no natural algebraic structure, and that the map AJ_G bears no simple relation (beyond an analogy in its definition) with the Griffiths-Weil Abel-Jacobi map on the Hilbert modular variety X.

ATR Cycles. Generalising slightly the definitions given in the Introduction to the case $r>1$, a quadratic extension M of F is called an ATR extension if

$$M\otimes_{F,v_0}\mathbb{R}\simeq\mathbb{C},\qquad M\otimes_{F,v_j}\mathbb{R}\simeq\mathbb{R}\oplus\mathbb{R},\quad (1\le j\le r).$$

The acronym ATR stands for "Almost Totally Real", since an ATR extension of F is "as far as possible" from being a CM extension, without being totally real.

Fix an ATR extension M of F, and let $\Psi : M \longrightarrow M_2(F)$ be an F-algebra embedding. Then

(1) Since $M \otimes_{F,v_0} \mathbb{R} \simeq \mathbb{C}$, the torus $\Psi(M^\times)$ has a unique fixed point $\tau_0 \in \mathcal{H}_0$.
(2) For each $1 \leq j \leq r$, the fact that $M \otimes_{F,v_j} \mathbb{R} \simeq \mathbb{R} \oplus \mathbb{R}$ shows that $\Psi(M^\times)$ has two fixed points τ_j and τ_j' on the boundary of $\mathcal{H}_j$. Let $\Upsilon_j \subset \mathcal{H}_j$ be the hyperbolic geodesic joining τ_j to τ_j'.

An embedding $\Psi : M \longrightarrow M_2(F)$ has a *conductor*, which is defined to be the $\mathcal{O}_F$-ideal c_Ψ for which

$$\Psi(M) \cap M_2(\mathcal{O}_F) = \Psi(\mathcal{O}_F + c_\Psi \mathcal{O}_M).$$

The $\mathcal{O}_F$-order $\mathcal{O}_\Psi := \mathcal{O}_F + c_\Psi \mathcal{O}_M$ is called the *order associated to* Ψ. It can be shown that there are finitely many distinct $\mathrm{SL}_2(\mathcal{O}_F)$-conjugacy classes of embeddings of M into $M_2(F)$ associated to a fixed order $\mathcal{O} \subset \mathcal{O}_M$, and that the Picard group (in a narrow sense) of $\mathcal{O}$ acts simply transitively on the set of such conjugacy classes of embeddings.

By the Dirichlet unit theorem, the group

$$\Gamma_\Psi := \Psi((\mathcal{O}_\Psi^+)^\times) \subset \mathrm{SL}_2(\mathcal{O}_F)$$

is of rank r and preserves the region

$$R_\Psi := \{\tau_0\} \times \Upsilon_1 \times \cdots \times \Upsilon_r.$$

The ATR cycle associated to the embedding Ψ is defined to be the quotient

$$\Delta_\Psi := \Gamma_\Psi \backslash R_\Psi.$$

It is a closed cycle on $X(\mathbb{C})$ which is topologically isomorphic to an r-dimensional real torus. In many cases, one can show that Δ_Ψ is null-homologous, at least after tensoring with $\mathbb{Q}$ to avoid the delicate issues arising from the possible presence of torsion in integral homology. (The homological triviality of Δ_Ψ always holds, for instance, when $r = 1$, and follows from the fact that the group cohomology $H^1(\mathrm{SL}_2(\mathcal{O}_F), \mathbb{C})$ is trivial.) Assume from now on that Δ_Ψ is homologically trivial, and therefore that it belongs to $\mathcal{Z}_r(X(\mathbb{C}))$.

The following conjecture lends arithmetic meaning to the Abel-Jacobi map AJ_G and to the ATR cycles Δ_Ψ.

Conjecture 2.2. *Let $\Psi : M \longrightarrow M_2(F)$ be an F-algebra embedding of an ATR extension M of F. Then the complex point $\mathrm{AJ}_G(\Delta_\Psi) \in E_0(\mathbb{C})$ is algebraic. More precisely, the isogeny ι in the definition (8) of AJ_G can be chosen so that, for all Ψ,*

$$\mathrm{AJ}_G(\Delta_\Psi) \text{ belongs to } E(H_{c_\Psi}),$$

where H_{c_Ψ} is the ring class field of M of conductor c_Ψ. Furthermore, if $\Psi_1, \ldots, \Psi_h$ is a complete system of representatives for the $\mathrm{SL}_2(\mathcal{O}_F)$-conjugacy classes of embeddings of M in $M_2(\mathcal{O}_F)$ of a given conductor c, then the Galois group $\mathrm{Gal}(H_c/M)$ acts (transitively) on the set $\{\mathrm{AJ}_G(\Delta_{\Psi_1}), \ldots, \mathrm{AJ}_G(\Delta_{\psi_h})\}$.

Conjecture 2.2 is poorly understood at present. For instance, it is not clear whether the Tate conjecture sheds any light on it. On the positive side, the ATR points that are produced by Conjecture 2.2 are "genuinely new" and go beyond what can be obtained using only CM points on Shimura curves. Indeed, the former are defined over abelian extensions of ATR extensions of totally real fields, while the latter are defined over abelian extensions of CM fields.

Most germane to the concerns of this paper, Conjecture 2.2 can be used as a basis for the construction of a point $P_M^? \overset{?}{\in} E(M)$, by letting $\Psi_1, \ldots, \Psi_h$ be a complete system of representatives for the $\mathrm{SL}_2(\mathcal{O}_F)$-conjugacy classes of embeddings of M in $M_2(\mathcal{O}_F)$ of conductor 1 and setting

$$P_M^? := \mathrm{AJ}_G(\Delta_{\Psi_1}) + \cdots + \mathrm{AJ}_G(\Delta_{\Psi_h}). \tag{9}$$

3. The Birch and Swinnerton-Dyer conjecture for $\mathbb{Q}$-curves

3.1. **Review of $\mathbb{Q}$-curves.** The first goal of the present work is to study Conjecture 2.2 for $\mathbb{Q}$-curves, which are defined as follows:

Definition 3.1. Let F be a number field and fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ containing F. We say that an elliptic curve E/F is a $\mathbb{Q}$-*curve* if it is *isogenous over F* to all its Galois conjugates over $\mathbb{Q}$.

In the literature, these curves are sometimes referred as $\mathbb{Q}$-curves *completely defined over* F, reserving the term $\mathbb{Q}$-curve for the wider class of elliptic curves over F which are isogenous *over* $\bar{\mathbb{Q}}$ to all their Galois conjugates over $\mathbb{Q}$.

$\mathbb{Q}$-curves are known to be modular, thanks to the work of Ellenberg and Skinner [ES] (who proved (geometric) modularity of $\mathbb{Q}$-curves under local conditions at 3), now vastly superseded by [KW], which implies modularity of all $\mathbb{Q}$-curves as a very particular case. Combining this with the older work of Ribet (cf. [Ri] for a survey), it follows that $\mathbb{Q}$-curves E/F are arithmetically uniformisable *over* $\bar{\mathbb{Q}}$ by the classical modular curves $X_1(N)$. By this, we mean that there exists a non-constant morphism of curves

$$\pi_E : X_1(N)_{\bar{\mathbb{Q}}} \longrightarrow E_{\bar{\mathbb{Q}}} \tag{10}$$

over $\bar{\mathbb{Q}}$, for some $N \geq 1$.

For simplicity, in this article we shall restrict our attention to $\mathbb{Q}$-curves over a *quadratic* field F, which represents the simplest non-trivial scenario. However, we believe that the ideas present in this note should allow, with some more effort, to treat more general cases; see the forthcoming Ph.D thesis [Zhao] of the third author.

Let F be a quadratic field with ring of integers $\mathcal{O}_F$ and write $\mathrm{Gal}\,(F/\mathbb{Q}) = \{1, \tau\}$. Let E be a $\mathbb{Q}$-curve over F of conductor $\mathfrak{N} \subset \mathcal{O}_F$.

Given a Dirichlet character ε of conductor N, let

$$\Gamma_\varepsilon(N) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \,\big|\, N|c,\, \varepsilon(a) = 1\} \subseteq \mathrm{SL}_2(\mathbb{Z})$$

and let $X_\varepsilon(N)$ be the modular curve associated to this congruence subgroup. The curve $X_\varepsilon(N)$ admits a canonical model over $\mathbb{Q}$, and coarsely represents the moduli problem of parametrizing triples (A, C, t) where A is a generalised elliptic curve, C is a cyclic subgroup of order N of $A(\bar{\mathbb{Q}})$ and t is an orbit in $C \setminus \{O\}$ for the action of $\ker(\varepsilon) \subset (\mathbb{Z}/N\mathbb{Z})^\times$. Note that the group $(\mathbb{Z}/N\mathbb{Z})^\times$ acts on $X_\varepsilon(N)$ via the diamond operators, and that the subgroup $\ker(\varepsilon)$ fixes it.

As discussed for example in [GQ] or [Ri], the modular parametrisation (10) is particularly well-behaved when F is quadratic. More precisely, there exists a positive integer $N \geq 1$, an even Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\} \subset \mathbb{C}^\times$, and a pair $f_E, f'_E \in S_2(\Gamma_\varepsilon(N)) \subseteq S_2(\Gamma_0(N), \varepsilon)$ of normalised *newforms* of weight 2, level N and nebentypus ε, such that

$$L(E/F, s) = L(f_E, s) \cdot L(f'_E, s). \tag{11}$$

In this case, the uniformisation in (10) factors through a modular parametrisation

$$\pi_E : X_\varepsilon(N)_F \longrightarrow E_F \tag{12}$$

defined over F.

Let K_f denote the field generated by the Fourier coefficients of f_E. It is either $\mathbb{Q}$ or a quadratic field. When $K_f = \mathbb{Q}$, the elliptic curve E is in fact isogenous to the base change of an elliptic curve defined over $\mathbb{Q}$ and question (1) can rather be tackled with the classical techniques reviewed in §2; we assume throughout that this is not the case. Hence $[K_f : \mathbb{Q}] = 2$ and, letting σ denote the single nontrivial automorphism of K_f, we have

$$f'_E = {}^\sigma f_E.$$

Weil's restriction of scalars $A := \mathrm{Res}_{F/\mathbb{Q}}(E)$ is an abelian surface of GL_2-type over $\mathbb{Q}$ such that

$$\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} \simeq K_f \quad \text{(and thus is simple over } \mathbb{Q}\text{)}, \tag{13}$$

$$A_{/F} \simeq E \times {}^\tau E, \text{ and} \tag{14}$$

$$L(A/\mathbb{Q}, s) = L(E/F, s) = L(f_E, s) \cdot L(f'_E, s). \tag{15}$$

Moreover, for any field extension $L/\mathbb{Q}$, there is a canonical isomorphism

$$A(L) \simeq E(F \otimes_{\mathbb{Q}} L) \tag{16}$$

and in particular $A(\mathbb{Q}) \simeq E(F)$. As shown by Carayol, the conductor of A over $\mathbb{Q}$ is N^2, and it follows from [Mi, Prop. 1] (see also [GG, Remark 9] for a more detailed discussion) that the conductor of E/F is $\mathfrak{N} = N_0 \cdot \mathcal{O}_F$, where $N_0 \in \mathbb{Z}$ satisfies

$$N = N_0 \cdot |\mathrm{disc}(F)|. \tag{17}$$

As we shall now explain, when F is imaginary the problem can be reduced to the classical setting considered by Gross-Zagier and Kolyvagin-Logachev, and presents no mysteries. It is the case of F real that deserves more attention, and to which the main bulk of this note will be devoted.

If ε is trivial, then K_f is real and F can be either real or imaginary (and indeed both cases occur in examples). As a direct consequence of (11), (16) and the generalization [KL] of the work of Kolyvagin to higher dimensional quotients of $J_0(N)$ over $\mathbb{Q}$, (1) also holds for E/F provided $\mathrm{ord}_{s=1}L(f_E,s)\leq 1$.

Assume $\varepsilon\neq 1$ for the rest of this article. Now K_f is an imaginary quadratic field. Besides, it follows from an observation of Serre (cf. [Ri, Proposition 7.2]) that F is necessarily *real*. In fact, F can be computed explicitly from f_E as $F=\bar{\mathbb{Q}}^{\ker(\varepsilon)}$. In particular it follows that ε is the quadratic Dirichlet character associated with F.

Let ω_N denote the Fricke involution of $X_\varepsilon(N)_F$ defined on the underlying Riemann surface by the rule $\tau\mapsto -\frac{1}{N\tau}$. It induces an involution on the jacobian $J_\varepsilon(N)_F$ of $X_\varepsilon(N)_F$ which leaves A_F stable. We have

$$A_F\sim(1+\omega_N)A_F\times(1-\omega_N)A_F, \tag{18}$$

where both factors on the right have dimension 1, are isogenous over F and conjugate one each other over $\mathbb{Q}$ (cf. [Cr, §5]). By replacing E by its conjugate if necessary, we shall assume throughout that $E=(1+\omega_N)A_F$.

It then follows that (12) factors through the following commutative diagram:

$$\begin{array}{ccccc} X_\varepsilon(N)_F & \longrightarrow & J_\varepsilon(N)_F & \longrightarrow & A_F \\ \downarrow \pi_N & & \downarrow & & \downarrow \\ X_\varepsilon^+(N) & \longrightarrow & J_\varepsilon^+(N) & \xrightarrow{\varphi_E} & E, \end{array} \tag{19}$$

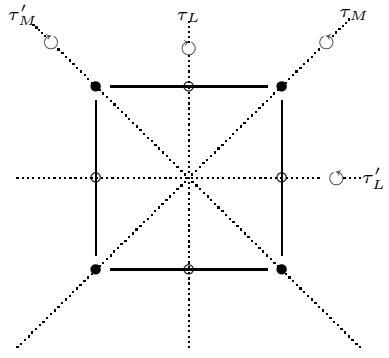
where we set $X_\varepsilon^+(N):=X_\varepsilon(N)_F/\langle\omega_N\rangle$ and $J_\varepsilon^+(N):=(1+\omega_N)J_\varepsilon(N)_F$. The reader should keep in mind that both are varieties over F, not over $\mathbb{Q}$.

3.2. **The main result.** The goal of this section is to prove Theorem 1.5 of the Introduction. Let M be a quadratic ATR extension of F. Since M has two real places and one complex place, it is not Galois over $\mathbb{Q}$. Let M' denote its Galois conjugate over $\mathbb{Q}$, and let $\mathcal{M}$ be the Galois closure of M over $\mathbb{Q}$. It is not hard to see that $\mathcal{M}$ is the compositum over F of M and M' and that $\mathrm{Gal}(\mathcal{M}/\mathbb{Q})$ is isomorphic to the dihedral group of order 8. The subgroup $V_F:=\mathrm{Gal}(\mathcal{M}/F)$ is isomorphic to a Klein 4-group. The dihedral group of order 8 contains two distinct, non-conjugate subgroups which are isomorphic to the Klein 4-group. This is most easily seen by viewing D_8 as the symmetry group of a square, as in the figure below, in which V_F is identified with the subgroup generated by the reflections about the two diagonals. These two reflections can be labeled as τ_M and τ'_M, in such a way that

$$\mathcal{M}^{V_F}=F,\qquad \mathcal{M}^{\tau_M}=M,\qquad \mathcal{M}^{\tau'_M}=M'.$$

The second Klein four-group, which shall be denoted V_K, is generated by the reflections about the vertical and horizontal axes of symmetry of the square. We label these reflections as τ_L and τ'_L, as shown in the figure below.

(20)

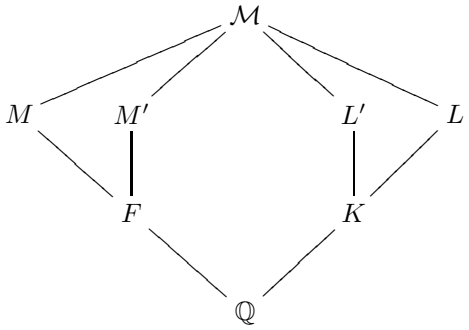


Now let

$$K:=\mathcal{M}^{V_K},\qquad L:=\mathcal{M}^{\tau_L},\qquad L'=\mathcal{M}^{\tau'_L}.$$

These fields fit into the following diagram of field extensions, where each unbroken line indicates an extension of degree 2:

(21)



Let

$$\chi_M, \chi'_M : G_F \longrightarrow \{\pm 1\}$$

denote the Galois characters of the real quadratic field F which cut out the extensions M and M', and let

$$\chi_L, \chi'_L : G_K \longrightarrow \{\pm 1\}$$

be the quadratic characters of the imaginary quadratic field K which cut out the extensions L and L'. We will often view these characters as idèle class characters defined on $\mathbb{A}_F^\times$ and on $\mathbb{A}_K^\times$ respectively. Finally, let ε_F and ε_K denote the quadratic Dirichlet characters attached to F and K, and let $\mathrm{N}_{\mathbb{Q}}^F : \mathbb{A}_F^\times \longrightarrow \mathbb{A}_{\mathbb{Q}}^\times$ and $\mathrm{N}_{\mathbb{Q}}^K : \mathbb{A}_K^\times \longrightarrow \mathbb{A}_{\mathbb{Q}}^\times$ denote the norms on adèles.

Proposition 3.2. (1) *The field K is a quadratic imaginary field.*

(2) *The characters χ_M, χ'_M, χ_L and χ'_L, viewed as idèle class characters of F and K respectively, satisfy*

$$\chi_M \chi'_M = \varepsilon_K \circ N_{\mathbb{Q}}^F; \qquad \chi_L \chi'_L = \varepsilon_F \circ N_{\mathbb{Q}}^K.$$

(3) *The central character of χ_M and χ'_M is ε_K, and the central character of χ_L and χ'_L is ε_F.*

(4) *The following two-dimensional representations of $G_{\mathbb{Q}}$ are isomorphic:*

$$Ind_F^{\mathbb{Q}} \chi_M = Ind_F^{\mathbb{Q}} \chi'_M = Ind_K^{\mathbb{Q}} \chi_L = Ind_K^{\mathbb{Q}} \chi'_L.$$

Proof. The quadratic field K is of the form $\mathbb{Q}(\sqrt{-d})$, where $-d$ is defined (modulo squares in $\mathbb{Q}^\times$) by

$$-d = \mathrm{N}_{F/\mathbb{Q}}(\alpha), \qquad \text{with} \quad M = F(\sqrt{\alpha}).$$

The fact that M is ATR implies that $-d$ is a negative rational number, and therefore that K is an imaginary quadratic field. The second part follows directly from the field diagram (21) above. To prove the third part, note that part (2) implies that the central character of L restricted to the group of norms from K is equal to ε_F. (This is because $\chi_L(x) = \chi'_L(\bar{x})$, where $x \mapsto \bar{x}$ is complex conjugation). Class field theory implies that this central character differs from ε_F by a power of ε_K. But the central character of χ_L cannot be $\varepsilon_F \varepsilon_K$ since this is an odd Dirichlet character and the central character of a finite order Hecke character of an imaginary quadratic field is necessarily even, because the map from the group of components of $\mathbb{R}^\times$ to the group of components of $\mathbb{C}^\times$ is trivial. Finally, the proof of part (4) is a simple exercise in representation theory: the four representations that are listed in (4) are all isomorphic to the unique irreducible two-dimensional representation of $\mathrm{Gal}(\mathcal{M}/\mathbb{Q})$. □

As at the end of the previous section §3.1, let E be a $\mathbb{Q}$-curve over a real quadratic field F and $A = \mathrm{Res}_{F/\mathbb{Q}}(E)$, let $f = f_E \in S_2(\Gamma_\varepsilon(N))$ denote the modular form associated to it and let K_f denote the imaginary quadratic field generated over $\mathbb{Q}$ by the Fourier coefficients of f.

Theorem 3.3 (Tian, Yuan, Zhang and Zhang)**.** *Let K be a quadratic imaginary field satisfying the Heegner hypothesis, and let $\chi : \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ be a finite order Hecke character of K satisfying*

(22)
$$\chi|_{\mathbb{A}_{\mathbb{Q}}^\times} = \varepsilon_f^{-1}.$$

Then

(i) *The L-function $L(f/K, \chi, s)$ vanishes to odd order at $s = 1$;*

(ii) *If* $L'(f/K,\chi,1)\neq 0$*, then* $(A(K^{\mathrm{ab}})\otimes\mathbb{C})^{\chi}$ *has rank one over* $K_f\otimes_{\mathbb{Q}}\mathbb{C}$*, and* $Ш(A/K^{\mathrm{ab}})^{\chi}$ *is finite.*

Proof. The modular form f gives rise to a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ whose central character is $\omega_\pi=\varepsilon_f$, the nebentypus of f. Condition (22) ensures that the tensor product of the motives attached to π and χ is self-dual, and therefore the L-function

$$L(f/K,\chi,s)=L(\pi,\chi,s-\frac{1}{2})$$

satisfies a functional equation whose central critical point is $s=1$; since the discriminant of K is relatively prime to N, the sign of this functional equation is $(-1)^{\sharp\Sigma}$, where

$$\Sigma=\{\text{primes }\ell\text{ inert in }K\text{ such that }\mathrm{ord}_\ell(N)\text{ is odd}\}\cup\{\infty\}.$$

The Heegner hypothesis satisfied by K says that $\Sigma=\{\infty\}$ and thus the sign is -1; this implies (i).

As a consequence of (13), the complex vector space $(A(K^{\mathrm{ab}})\otimes\mathbb{C})^{\chi}$ is naturally a $K_f\otimes_{\mathbb{Q}}\mathbb{C}$-module. Part (ii) is a theorem of Tian-Zhang [TZ] which follows as a corollary of [YZZ, Theorem 1.3.1] by applying Kolyvagin's method. Since [TZ] is not currently available, the reader may consult [YZZ, Theorem 1.4.1] and, for the precise statement quoted here, [Zh2, Theorem 4.3.1]. □

We are now ready to prove Theorem 1.5 of the introduction.

Theorem 3.4. *Let* E *be a* $\mathbb{Q}$*-curve over* F *of square conductor* $\mathfrak{N}$*, and let* M/F *be an ATR extension of* F *of discriminant prime to* $\mathfrak{N}$*. If* $L'(E_M/F,1)\neq 0$*, then* $E_M(F)$ *has rank one and* $Ш(E_M/F)$ *is finite.*

Proof. By (11) and the Artin formalism for L-series,

$$L(E_M/F,s)=L(E,\chi_M,s)=L(f\otimes\chi_M/F,s)=L(f\otimes\mathrm{Ind}_F^{\mathbb{Q}}\chi_M,s). \tag{23}$$

By part 4 of Proposition 3.2,

$$L(f\otimes\mathrm{Ind}_F^{\mathbb{Q}}\chi_M,s)=L(f\otimes\mathrm{Ind}_K^{\mathbb{Q}}\chi_L,s)=L(f\otimes\chi_L/K,s). \tag{24}$$

It follows from (23) and (24) that

$$L'(E_M/F,1)=L'(f\otimes\chi_L/K,1)=L'(f^\sigma\otimes\chi_L/K,1). \tag{25}$$

Therefore the two rightmost expressions in (25) are non-zero by assumption, so that the product

$$L(f\otimes\chi_L/K,s)L(f^\sigma\otimes\chi_L/K,s)=L(A/K,\chi_L,s)$$

vanishes to order exactly $2=[K_f:\mathbb{Q}]$ at $s=1$. By Theorem 3.3, it follows that $A(L)^-$ is of rank two, where $A(L)^-$ denotes the subgroup of the Mordell-Weil group of $A(L)$ of points whose trace to K is trivial. In particular, the Galois representation $\mathrm{Ind}_K^{\mathbb{Q}}\chi_L$ occurs in $A(\overline{\mathbb{Q}})\otimes\mathbb{C}$ with multiplicity 2. Hence, invoking once again part 4 of Proposition 3.2, we find that

$$\mathrm{rank}(A(M)^-)=2.$$

But since M contains F and since A is isogenous over F to $E\times E$, it follows that

$$\mathrm{rank}(E(M)^-)=\mathrm{rank}(E_M(F))=1.$$

The result about the ranks follows. The result about the finiteness of $Ш(E_M/F)$ follows in the same way from part (ii) of Theorem 3.3. □

4. Heegner points on Shimura's elliptic curves

Implicit in the proof of Theorem 3.4 (via the use that is made of it in the proof of Theorem 3.3) is the construction of a Heegner point $P_M\in E_M(F)$ arising from the image of certain CM divisors on $X_\varepsilon(M)$ via the modular parametrisation (10). We now wish to make this construction explicit in the case where the $\mathbb{Q}$-curve E has everywhere good reduction over the real quadratic field F. The $\mathbb{Q}$-curves with this property are sometimes called *Shimura elliptic curves* because they were first systematically considered by Shimura. More precisely, in [Shim] it is shown how to associate a Shimura elliptic curve over $F=\mathbb{Q}(\sqrt{N})$ to any classical elliptic modular form $f\in S_2(\Gamma_0(N),\varepsilon_N)$ with quadratic fourier coefficients. (Cf. also (17).)

It will be assumed throughout this chapter that E/F is a Shimura elliptic curve, and that f is the corresponding elliptic modular form. We also assume for simplicity that N *is odd*, and thus square-free.

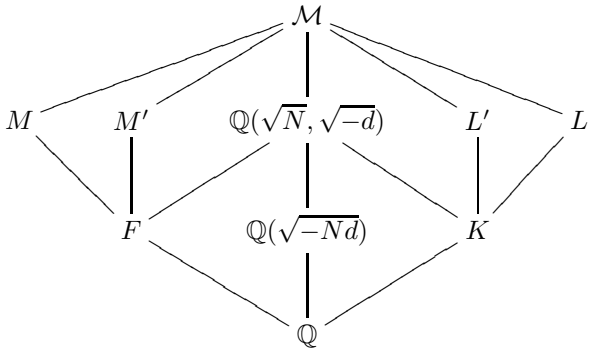
Remark 4.1. According to calculations performed by the third author using PARI [PA] (extending the data gathered in [Cr, §6], [Pi] in the range $N \leq 1000$), there exists an eigenform $f \in S_2(\Gamma_0(N), \varepsilon_N)$ of prime level $1 < N < 5000$, with fourier coefficients in a quadratic imaginary extension $K_f = \mathbb{Q}(\sqrt{-d})$ for precisely the values of N and d listed in the following table.

N	29	37	41	109	157	229	257	337	349	373	397	421
d	5	1	2	3	1	5	2	2	5	1	1	7
N	461	509	877	881	997	1069	1709	1861	2657	4481	4597	
d	5	5	1	2	3	1	5	5	2	11	1	

Associated to each such eigenform there is a Shimura elliptic curve over $F = \mathbb{Q}(\sqrt{N})$. Furthermore, according to computations due to Cremona, Dembelé, Elkies and Pinch, there are only four primes N in the range $[1, 1000]$ for which there exists an elliptic curve with good reduction everywhere over $F = \mathbb{Q}(\sqrt{N})$ which is *not* a $\mathbb{Q}$-curve, namely, $N = 509$, 853, 929 and 997. It is hard to predict whether the preponderance of Shimura elliptic curves among elliptic curves of conductor one will persist or is merely an artefact of the relatively low ranges in which numerical data has been gathered. Note that it is not even known whether there exist infinitely many Shimura elliptic curves over real quadratic fields, while it is a theorem of S. Comalada [Co] that there are infinitely many elliptic curves over real quadratic fields with good reduction everywhere.

4.1. **An explicit Heegner point construction.** Let us recall the diagram of field extensions introduced in (21):

(26)



The following lemma is crucial in constructing the point $P_M \in E(M)^- = E_M(F)$ explicitly.

Lemma 4.2. *Let M be an ATR extension of F and let K be the quadratic imaginary field attached to M as in the diagram* (26)*. Then K has a (canonical) ideal $\mathcal{N}$ of K of norm N. In particular, all the prime divisors of N are either split or ramified in K.*

Proof. The conductor-discriminant formula combined with part 4 of Proposition 3.2 show that

$$\mathrm{disc}(F)\mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{disc}(M/F)) = \mathrm{disc}(K)\mathrm{Nm}_{K/\mathbb{Q}}(\mathrm{disc}(L/K)).$$

Therefore, after setting

$$N_{\mathrm{ram}} = \gcd(N, \mathrm{disc}(K)), \qquad N_{\mathrm{split}} = N/N_{\mathrm{ram}},$$
$$\mathcal{N}_{\mathrm{ram}} = (N_{\mathrm{ram}}, \sqrt{\mathrm{disc}(K)}), \qquad \mathcal{N}_{\mathrm{split}} = (N_{\mathrm{split}}, \mathrm{disc}(L/K)),$$

we find that $\mathcal{N} := \mathcal{N}_{\mathrm{ram}}\mathcal{N}_{\mathrm{split}}$ gives the desired ideal of norm N. □

Let $\mathbb{A}_K$ denote the ring of adèles of K, and let

$$\hat{\mathcal{O}}_K^\times := \prod_v \mathcal{O}_v^\times$$

denote the maximal compact subgroup of the group $\mathbb{A}_{K,\mathrm{fin}}^\times$ of finite idèles of K. Given a rational integer $c \geq 1$, $(c, N) = 1$, we define

$$U_c = \hat{\mathbb{Z}}^\times(1 + c\hat{\mathcal{O}}_K)\mathbb{C}^\times \subset \mathbb{A}_K^\times.$$

By class field theory, the quotient $G_c := \mathbb{A}_K^\times/(K^\times U_c)$ is identified with $\mathrm{Gal}(H_c/K)$, where H_c is the *ring class field* of K of conductor c.

As a piece of notation, we shall write H_c for the ring class field attached to the order in K of conductor $c \geq 1$ and write $K_{\mathfrak{a}}$ for the ray class field of conductor $\mathfrak{a}$.

Define

$$U_c^+ = \{\beta \in U_c \text{ such that } (\beta)_{\mathcal{N}} \in \ker(\varepsilon) \subset (\mathbb{Z}/N\mathbb{Z})^\times\},$$

$$U_c^- = \{\beta \in U_c \text{ such that } (\beta)_{\overline{\mathcal{N}}} \in \ker(\varepsilon) \subset (\mathbb{Z}/N\mathbb{Z})^\times\},$$

and $\tilde{U}_c = U_c^+ \cap U_c^-$. Here $(\beta)_{\mathcal{N}}$ denotes the image of the local term of the idèle β at $\mathcal{N}$ in the quotient $\mathcal{O}_{\mathcal{N}}^\times/(1+\mathcal{N}\cdot\mathcal{O}_{\mathcal{N}}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. Similarly for $\overline{\mathcal{N}}$. This way we can regard the character ε as having source either $\mathcal{O}_{\mathcal{N}}^\times$ or $\mathcal{O}_{\overline{\mathcal{N}}}^\times$.

Set

$$\tilde{G}_c := \mathbb{A}_K^\times/(K^\times \tilde{U}_c) = \mathrm{Gal}(\tilde{H}_c/K),$$

where $\tilde{H}_c$ is a biquadratic extension of the ring class field H_c. It can be written as $\tilde{H}_c = L_c L_c'$, where L_c (resp. L_c') is the class field attached to U_c^+ (resp. U_c^-).

Proposition 4.3. *The relative discriminant of L/K factors as $d(L/K) = c\cdot\mathcal{N}$, where c is a positive integer such that $L \subset L_c$ and $L' \subset L_c'$ and thus $\mathcal{M} \subset \tilde{H}_c$.*

More precisely, we have $c = 2^t \cdot c_0$ where $0 \leq t \leq 3$ and c_0 is odd and square-free. The proof of this proposition is an exercise in class field theory, which we relegate to §4.4 for the convenience of the reader.

We now explain how to construct a degree zero divisor on $X_\varepsilon(N)$ defined over $\tilde{H}_c$. To do this, let A_c be an elliptic curve satisfying

$$\mathrm{End}(A_c) = \mathcal{O}_c,$$

where $\mathcal{O}_c := \mathbb{Z} + c\mathcal{O}_K$ is the order in K of conductor c. Such a curve, along with its endomorphisms, may be defined over the ring class field H_c. The module $A_c[\mathcal{N}]$ of $\mathcal{N}$-torsion points is therefore defined over H_c, yielding a point $P_c := [A_c, A_c[\mathcal{N}]] \in X_0(N)(H_c)$.

The action of $G_{H_c} := \mathrm{Gal}(\overline{\mathbb{Q}}/H_c)$ on the points of this group scheme gives a Galois representation

$$\rho_{\mathcal{N}} : G_{H_c} \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times.$$

The composition of $\rho_{\mathcal{N}}$ with the nebentypus character ε is a quadratic character of G_{H_c}, which cuts out the quadratic extension L_c of H_c. The point P_c lifts to two points P_c^+ and P_c^- in $X_\varepsilon(N)(L_c)$ which are interchanged by the action of $\mathrm{Gal}(L_c/H_c)$; we do not specify the order in which these points are to be taken. Similarly, we can replace the module $A_c[\mathcal{N}]$ by $A_c[\overline{\mathcal{N}}]$, mimic the above construction and obtain points $P_c'^+$ and $P_c'^-$ defined over L_c'.

Definition 4.4. Let

$$\mathrm{CM}(c) = \bigcup\{P_c^+, P_c^-, P_c'^+, P_c'^-\} \subset X_\varepsilon(N)(\tilde{H}_c)$$

be the set of Heegner points on $X_\varepsilon(N)$ obtained by letting A_c run over all isomorphism classes of elliptic curves with CM by $\mathcal{O}_c$.

If we let $h(O_c)$ denote the cardinality of the group $\mathrm{Pic}(\mathcal{O}_c)$ of classes of locally free ideals of $\mathcal{O}_c$, the cardinality of $\mathrm{CM}(c)$ is $4h(\mathcal{O}_c)$. In fact, $\mathrm{CM}(c)$ is naturally the disjoint union of the two subsets $CM(c) \cap X_\varepsilon(N)(L_c)$ and $CM(c) \cap X_\varepsilon(N)(L_c')$, each of cardinality $2h(\mathcal{O}_c)$.

A Heegner point $P \in \mathrm{CM}(c)$ of conductor c may be described by a triple $([\mathfrak{a}], \mathfrak{n}, t)$, where

- $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)$ is the class of an invertible $\mathcal{O}_c$-module of K,
- $\mathfrak{n}$ is an integral ideal of $\mathcal{O}_c$ such that the quotient $\mathcal{O}_c/\mathfrak{n}$ is cyclic of order N,
- t is an orbit for the action of $\ker(\varepsilon)$ of an element of order N in $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$.

Let $\tilde{C}$ be the quotient of the ray class group of K of conductor $c\mathcal{N}$ for which Artin's reciprocity map of global class field theory furnishes a canonical isomorphism

$$\mathrm{rec} : \tilde{C} \xrightarrow{\sim} \mathrm{Gal}(\tilde{H}_c/K).$$

Let $\mathcal{O} = \mathcal{O}_c$ denote the order of conductor c in K. There are natural exact sequences, sitting in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\tilde{H}_c/H_c) & \longrightarrow & \mathrm{Gal}(\tilde{H}_c/K) & \xrightarrow{\mathrm{res}_{\tilde{H}_c/H_c}} & \mathrm{Gal}(H_c/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{rec}} & & \downarrow{\scriptstyle \mathrm{rec}} & & \downarrow{\scriptstyle \mathrm{rec}} & & \\ 1 & \longrightarrow & \langle [\beta_0], [\beta_0'] \rangle & \longrightarrow & \tilde{C} & \longrightarrow & \mathrm{Pic}(\mathcal{O}) & \longrightarrow & 1, \end{array}$$

where the vertical arrows are isomorphisms. Here, $\beta_0 \in \mathcal{O}_{\mathcal{N}}^\times$ and $\beta_0' \in \mathcal{O}_{\overline{\mathcal{N}}}^\times$ are elements such that $\varepsilon(\beta_0) = -1$ and $\varepsilon(\beta_0') = -1$. Artin's reciprocity map induces an isomorphism

$$\mathrm{Gal}(\tilde{H}_c/H_c) \simeq \mathcal{O}_{\mathcal{N}}^\times/\ker(\varepsilon) \times \mathcal{O}_{\overline{\mathcal{N}}}^\times/\ker(\varepsilon) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

We thus can formally write elements of $\tilde{C}$ as classes of *enhanced ideals*, which are defined as elements of the form $\underline{\mathfrak{b}} := \beta_{\mathcal{N}}\beta_{\overline{\mathcal{N}}}\prod_{\wp\nmid N}\wp^{n_\wp}$, taken up to principal ideals (b) with $b \in K^\times$. Here $\beta_{\mathcal{N}}$ and $\beta_{\overline{\mathcal{N}}}$ belong to $K_{\mathcal{N}}^\times/\ker(\varepsilon)$ and $K_{\overline{\mathcal{N}}}^\times/\ker(\varepsilon)$ respectively, $\wp$ runs over all prime invertible ideals of $\mathcal{O}$ not dividing N, and the exponents $n_\wp$ are integers which are almost all zero. We say an enhanced ideal is *integral* if $\beta_{\mathcal{N}}$ and $\beta_{\overline{\mathcal{N}}}$ have representatives in $\mathcal{O}_{\mathcal{N}}^\times$ and $\mathcal{O}_{\overline{\mathcal{N}}}^\times$ respectively, and $n_\wp \geq 0$ for all $\wp$. The image of the class $\underline{\mathfrak{b}}$ in $\mathrm{Pic}(\mathcal{O})$ is simply the class of the ideal $\mathfrak{b} = \mathcal{N}^{\mathrm{ord}_{\mathcal{N}}(\beta_{\mathcal{N}})}\overline{\mathcal{N}}^{\mathrm{ord}_{\overline{\mathcal{N}}}(\beta_{\overline{\mathcal{N}}})}\prod_{\wp\nmid N}\wp^{n_\wp}$ generated by it.

By Shimura's reciprocity law,

$$\mathrm{rec}(\underline{\mathfrak{b}})(D) = \underline{\mathfrak{b}}^{-1} \star D \tag{27}$$

for all $\underline{\mathfrak{b}} \in \tilde{C}$ and all divisors $D \in J_\varepsilon(N)(\tilde{H}_c)$ supported on $\mathrm{CM}(c)$.

On the left hand side we make use of the natural Galois action of $\mathrm{Gal}(\tilde{H}_c/K)$ on $J_\varepsilon(N)(\tilde{H}_c)$, via Artin's reciprocity isomorphism. On the right hand side, a class $[\underline{\mathfrak{b}}] \in \tilde{C}$ acts on $\mathrm{CM}(c)$ by the rule

$$\underline{\mathfrak{b}} \star P = ([\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{n}, \varphi_{\mathfrak{b}}(\beta_{\mathcal{N}} t)), \tag{28}$$

where $P = ([\mathfrak{a}], \mathfrak{n}, t) \in \mathrm{CM}(c)$, $\underline{\mathfrak{b}} = \beta_{\mathcal{N}}\beta_{\overline{\mathcal{N}}}\prod_{\wp\nmid N}\wp^{n_\wp}$ is an integral representative of its class and $\varphi_{\mathfrak{b}} : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}$ is the natural projection map. Writing $P = [\tau] \in X_\varepsilon(N)(\mathbb{C})$ for some $\tau \in \mathcal{H}$, let $\gamma_{\underline{\mathfrak{b}}} \in \mathrm{GL}_2^+(\mathbb{Q})$ be such that $\underline{\mathfrak{b}} \star P = [\gamma_{\underline{\mathfrak{b}}}\tau]$.

Besides this action, there is also the diamond involution W_ε, acting on $P = [\tau] \in X_\varepsilon(N)(\mathbb{C})$ as $W_\varepsilon([\tau]) = [\gamma_\epsilon\tau]$ and on $P = ([\mathfrak{a}], \mathfrak{n}, t) \in \mathrm{CM}(c)$ as

$$W_\varepsilon(P) = ([\mathfrak{a}], \mathfrak{n}, dt), \quad \text{for } \gamma_\epsilon = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N) \setminus \Gamma_\varepsilon(N). \tag{29}$$

The cardinality of $\mathrm{CM}(c)$ is $4h(\mathcal{O})$ and it is acted on freely and transitively by the group $\langle W_N, W_\varepsilon\rangle \times \tilde{C}_{\mathcal{M}}$, where we let $\tilde{C}_{\mathcal{M}} := \mathrm{rec}^{-1}(\mathrm{Gal}(\tilde{H}_c/\mathcal{M})) \subset \tilde{C}_K$. Note that the restriction map $\mathrm{res}_{\tilde{H}_c/H_c}$ induces an isomorphism $\tilde{C}_{\mathcal{M}} \cong \mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(H_c/K)$.

It is our aim now to define a point $P_M \in E(M)$ (and thus also, by conjugation over F, a point $P_{M'} \in E(M')$) on the elliptic curve E, rational over the ATR extension M/F. We shall construct P_M as a suitable linear combination of certain points $P_L \in A(L)$ and $P_{L'} \in A(L')$ on the abelian surface $A = \mathrm{Res}_{F/\mathbb{Q}}(E)$. These points are defined as the trace to L of the projection of $P_c^+ \in X_\varepsilon(N)(L_c)$ (respectively of $P_c^{'+} \in X_\varepsilon(N)(L_c')$) on A.

Before doing so, we first observe that choosing $P_c^- = W_\varepsilon(P_c^+)$ instead of P_c^+ (and similarly $P_c'^-$ instead of $P_c'^+$) is unimportant for our construction, as the next lemma shows that both lead to the same point on A up to sign and torsion. Recall the canonical projection $\pi_f : J_\varepsilon(N) \to A$ defined over $\mathbb{Q}$ and reviewed in (19), which can be composed with the natural embedding of $X_\varepsilon(N)$ into its jacobian $J_\varepsilon(N)$ given by the map $P \mapsto P - i\infty$. By an abuse of notation, we continue to denote by π_f this composition.

Lemma 4.5. *For any $P \in X_\varepsilon(N)(\overline{\mathbb{Q}})$, the point $\pi_f(P) + \pi_f(W_\varepsilon(P))$ belongs to $A(F)_{\mathrm{tors}}$.*

Proof. There is a natural decomposition $S_2(\Gamma_\varepsilon(N)) = S_2(\Gamma_0(N)) \oplus S_2(\Gamma_0(N), \varepsilon)$ corresponding to the eigenspaces of eigenvalue ± 1 with respect to the action of the involution W_ε. The rule $f(z) \mapsto f(z)dz$ yields an identification of $S_2(\Gamma_\varepsilon(N))$ with the space of holomorphic differentials on $X_\varepsilon(N)_{\mathbb{C}}$. Via this

isomorphism, $\pi_f^* H^0(\Omega^1_A)$ is contained in $S_2(\Gamma_0(N),\varepsilon)$. Consequently, $\pi_f(P-i\infty) = -\pi_f(W_\varepsilon(P-i\infty))$ and

$$\pi_f(P) + \pi_f(W_\varepsilon(P)) = \pi_f(P-i\infty) + \pi_f(W_\varepsilon(P) - i\infty)$$
$$= \pi_f(P-i\infty) + \pi_f(W_\varepsilon(P) - W_\varepsilon(i\infty)) + \pi_f(W_\varepsilon(i\infty) - i\infty) = \pi_f(W_\varepsilon(i\infty) - i\infty).$$

This last expression is a torsion point on $A(F)$ by the Manin-Drinfeld theorem which asserts that degree zero cuspidal divisors on a modular curve give rise to torsion elements in its Jacobian. □

We now set

$$P_L = \mathrm{Tr}_{L_c/L}(\pi_f(P_c^+)) \in A(L).$$

Note that $\tau_M(P_L^+)$ is either equal to $\mathrm{Tr}_{L'_c/L'}(\pi_f(P_c'^+))$ or to $\mathrm{Tr}_{L'_c/L'}(\pi_f(P_c'^-))$. Without loss of generality, assume that $\tau_M(P_L^+) = \mathrm{Tr}_{L'_c/L'}(\pi_f(P_c'^+))$ and denote it by P'_L.

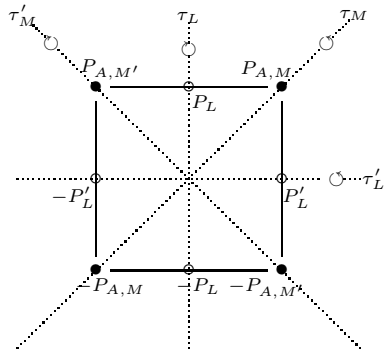
Set

$$u = \begin{cases} 2 & \text{if } K = \mathbb{Q}(\sqrt{-1}) \text{ and } c = 1; \\ 3 & \text{if } K = \mathbb{Q}(\sqrt{-3}) \text{ and } c = 1; \\ 1 & \text{otherwise,} \end{cases}$$

and define

$$P_{A,M} := \frac{1}{u}(P_L + P'_L), \qquad P_{A,M'} := \frac{1}{u}(P_L - P'_L).$$

The construction of the point $P_{A,M}$ is illustrated in the figure below.



This figure suggests–and it is indeed easy to check–that

$$P_{A,M} \in A(M), \qquad P_{A,M'} \in A(M').$$

Recall that the morphism $\varphi_F : A_F \longrightarrow E$ introduced in (19) is defined over $F \subset M$, and therefore that the point

$$P_M := \varphi_F(P_{A,M})$$

belongs to $E(M)$. As a by-product of our explicit construction we obtain the following analytic formula for calculating the point P_M.

Theorem 4.6. *Let $\tau_c, \tau'_c \in \mathcal{H}$ be elements representing the Heegner points $P_c^+, P_c'^+ \in X_\varepsilon(N)(\tilde{H}_c)$. Set*

$$z_M = \sum_{\underline{\mathfrak{b}} \in \tilde{C}_{\mathcal{M}}} \left[\int_{i\infty}^{\gamma_{\underline{\mathfrak{b}}}\tau_c} (f_E(\tau) + f_E\big|_{W_N}(\tau))\, d\tau + \int_{i\infty}^{\gamma_{\underline{\mathfrak{b}}}\tau'_c} (f_E(\tau) + f_E\big|_{W_N}(\tau))\, d\tau \right]. \tag{30}$$

Then $P_M = \eta(z_M)$ where η is the Weierstrass parametrization

$$\eta : \mathbb{C}/\Lambda_E \longrightarrow E(\mathbb{C}), \quad \eta(z) = (\wp(z), \wp'(z)). \tag{31}$$

Here, $\wp$ is the Weierstrass function associated with the lattice of periods

$$\Lambda_E := \left\{ \int_\delta (f_E + f_E\big|_{W_N}) d\tau \right\}$$

where $\delta \in H_1(X_\varepsilon(\mathbb{C}), \mathbb{Z})$ runs over the cycles of $X_\varepsilon(\mathbb{C})$ such that $\int_\delta (f_E - f_E\big|_{W_N}) d\tau = 0$.

4.2. **Heegner points and ATR cycles.** The main conjecture that will be formulated in this section relates the Heegner point P_M with the Stark Heegner point $P_M^?$ arising from ATR cycles. Recall that $\mathrm{Gal}(F/\mathbb{Q}) = \{1, \tau\}$ and $D_F = \mathrm{disc}(F)$. Let also $c_{E/F}$ (resp. $c_{E^\tau/F}$) denote either the real period or twice the real period of $E/\mathbb{R}$ (resp. of $E^\tau/\mathbb{R}$) depending on whether $E(\mathbb{R})$ (resp. $E^\tau(\mathbb{R})$) is connected or not.

Conjecture 4.7. *The ATR point $P_M^?$ is of infinite order if and only if P_M is of infinite order and $L(E/F, 1) \neq 0$. More precisely,*

$$P_M^? = 2^s \ell \cdot P_M \tag{32}$$

where $\ell \in \mathbb{Q}^\times$, which depends only on (E, F) and not on M, satisfies

$$\ell^2 = \frac{L(E/F, 1)}{\Omega_{E/F}}, \qquad \text{with } \Omega_{E/F} = \frac{c_{E/F} \cdot c_{E^\tau/F}}{D_F^{1/2} \cdot |E_{\mathrm{tor}}(F)|^2},$$

and $s \in \mathbb{Z}$ depends on M.

Below we collect some numerical data in support of conjecture 4.7. Besides the numerical evidence, Conjecture 4.7 is also motivated by the equality

$$L'(E/M, 1) = L(E/F, 1) L'(E/F, \chi_M, 1)$$

as recalled in the proof of Theorem 3.4, and by the facts that

(1) the Néron-Tate height of the Stark-Heegner point $P_M^?$ is expected (cf. [DL]) to be related in a simple way to $L'(E/M, 1)$.
(2) the extension of the Gross-Zagier formula proved in [YZZ] should in principle lead to an analogous relationship between the Heegner point P_M and the derivative $L'(f/K, \chi_L, 1) = L'(f/F, \chi_M, 1) = L'(E/F, \chi_M, 1)$.

It would be interesting to formulate a precise recipe predicting the power of 2 that arises as a fudge factor in (32). The authors have not made a serious attempt to do this.

4.3. **Numerical examples.** For $N = 29, 37, 41$ it is known (cf. [Shio] and [Cr, § 6]) that there is a unique Shimura elliptic curve defined over $F = \mathbb{Q}(\sqrt{N})$ up to isogeny over F.

The aim of this section is to provide numerical evidence for conjecture 4.7, which we have gathered by explicitly computing the points P_M and $P_M^?$ for several ATR extensions M/F on each of these three elliptic curves. The computation of the Heegner point P_M was performed with the software package PARI [PA] by exploiting formula (30) and the material in [Shio] and [Cr, § 6] to produce a complex invariant $z_M \in \mathbb{C}/\Lambda_E$ mapping to P_M under the Weierstrass uniformisation. Similarly, the ATR point $P_M^?$ was computed by following the method explained in [DL].

In fact, for our experiments it was sufficient to compute the element $z_M^? \in \mathbb{C}/\Lambda_E$ mapping to $P_M^?$ under the Weierstrass uniformisation. For several values of M, the invariants z_M and $z_M^?$ were calculated to roughly 50 digits of decimal accuracy, and the constants s and ℓ in (32) could then be obtained by picking a basis (e_1, e_2) for Λ_E and searching for a linear dependence relation with small integer coefficients between the four complex numbers z_M, $z_M^?$, e_1 and e_2, using Pari's `lindep` command.

This approach represents a dramatic improvement over the one that had to be followed in [DL], in which only the point $P_M^?$ was computed. In practice, recognizing $P_M^?$ as an algebraic point using standard rational recognition programs is difficult once the height of $P_M^?$ becomes large. The authors of [DL] were forced instead to perform an independent search for a generator of $E(M)$–a computationally difficult and time-consuming task–in order to check that $P_M^?$ indeed agreed with a point of small height on $E(M)$ to within the calculated decimal accuracy. The new approach based on the Heegner point P_M makes the experimental verifications of [DL] much more systematic and efficient, and allows them to be carried out for much further ranges.

In the tables below, we have followed almost the same notations as in [DL, §3]. In particular, we have written $M = F(\beta)$ with $\beta^2 \in F$, and denoted by $D_M = \mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{disc}(M/F))$ the absolute discriminant. (Note that K is used in [DL] to denote the field that we call M in the present work.) As before, L/K denotes the quadratic extension sitting in the Galois closure of M as in the field diagram (26), and we denote $D_K = \mathrm{disc}(K/\mathbb{Q})$ and $D_L = \mathrm{Nm}_{K/\mathbb{Q}}(\mathrm{disc}(L/K))$ and $\ell^2 \in \mathbb{Q}^\times$ is the value we

found numerically for the constant alluded to in Conjecture 4.7. Finally note that ℓ and s uniquely determine P_M up to sign and $E(M)_{\mathrm{tor}}$.

The case $N = 29$**.** Let $\delta = 2 + \omega = (5 + \sqrt{29})/2$. Shiota's Weierstrass equation for E_N is given by

$$E_{29} : y^2 + xy + \delta^2 y = x^3,$$

whose discriminant is $\Delta_{29} = -\delta^{10}$. Our calculations convincingly suggest that

$$\ell^2 = \frac{L(E_{29}/F, 1)}{\Omega_{E_{29}/F}} = 1$$

and that the point $P_M^?$ and s are given in the following table. The table suggests that $s = -2$ in all cases that have been calculated for this particular curve.

$D_M = D_K \cdot c^2$	β^2	D_L	$\lvert\mathrm{Pic}(\mathcal{O}_c)\rvert$	$P_M^?$	s
$-7 = -7 \cdot 1$	$-1+\omega$	29	1	$(\beta^2+3,\ -\frac{5}{2}\beta^3 - 3\beta^2 - 8\beta - \frac{19}{2})$	-2
$-16 = -4 \cdot 2^2$	$2+\omega$	$2^2 \cdot 29$	1	$(\frac{\beta^2}{2},\ -\frac{5}{4}\beta^3 - \frac{11}{4}\beta^2 - \frac{\beta}{4} - \frac{1}{2})$	-2
$-23 = -23 \cdot 1$	$17+8\omega$	29	3	$(\frac{1}{8}(11\beta^2+5),\ -\frac{13}{8}\beta^3 - \beta^2 - \frac{7}{8}\beta - \frac{1}{2})$	-2
$-35_1 = -35 \cdot 1$	$19+9\omega$	29	2	$(\frac{1}{5}(2\beta^2+1),\ -\frac{59}{225}\beta^3 - \frac{43}{90}\beta^2 - \frac{89}{450}\beta - \frac{29}{90})$	-2
$-35_2 = -35 \cdot 1$	$4+3\omega$	29	2	$(-\frac{1}{15}(4\beta^2+11),\ -\frac{1}{150}(17\beta^3+105\beta^2+43\beta+270))$	-2
$-59 = -59 \cdot 1$	$61+28\omega$	29	3	$(-\frac{1}{9},\ -\frac{11}{1512}\beta^3 - \frac{5}{56}\beta^2 - \frac{1}{1512}\beta + \frac{1}{504})$	-2
$-63 = -7 \cdot 3^2$	3ω	$3^2 \cdot 29$	4	$(\frac{7}{9}\beta^2+5,\ \frac{26}{27}\beta^3 - \frac{11}{9}\beta^2 + \frac{57}{9}\beta - 8)$	-2
$-64 = -4 \cdot 4^2$	$4+2\omega$	$2^4 \cdot 29$	2	$(-\frac{1}{4},\ -\frac{3}{8}\beta^3 - \frac{5}{4}\beta^2 - \frac{\beta}{4} - \frac{3}{8})$	-2
$-80 = -20 \cdot 2^2$	$1+\omega$	$2^2 \cdot 29$	4	$(\frac{1}{10}(43\beta^2+51),\ -\frac{517}{50}\beta^3 - \frac{93}{20}\beta^2 - \frac{1233}{100}\beta - \frac{111}{20})$	-2
$-91 = -91 \cdot 1$	$7+5\omega$	29	2	$(\frac{1}{13}(98\beta^2+387),\ -\frac{18939}{845}\beta^3 - \frac{111}{26}\beta^2 - \frac{150109}{1690}\beta - \frac{439}{26})$	-2
$-175 = -7 \cdot 5^2$	$-5+5\omega$	$5^2 \cdot 29$	6	$(-\frac{6}{50}\beta^2 - 2,\ \frac{1}{10}\beta^3 - \frac{11}{25}\beta^2 + \frac{98}{100}\beta - \frac{45}{10})$	-2

Table 2: ATR extensions of $\mathbb{Q}(\sqrt{29})$ and ATR points on E_{29}

The case $N = 37$. Letting $\omega = \frac{1+\sqrt{37}}{2}$, Shiota's Weierstrass equation for E_{37} is given by

$$E_{37} : y^2 + y = x^3 + 2x^2 - (19 + 8\omega)x + (28 + 11\omega),$$

and its discriminant is $\Delta_{37} = (5+2\omega)^6$. Note that $5+2\omega$ is a fundamental unit of F. Our calculations are consistent with the fact that

$$\ell^2 = \frac{L(E_{37}/F, 1)}{\Omega_{E_{37}/F}} = 1.$$

More precisely, the Stark-Heegner point $P_M^?$ and s are given in the tables below.

$D_M = D_K \cdot c^2$	β^2	D_L	$\lvert\mathrm{Pic}(\mathcal{O}_c)\rvert$	$P_M^?$	s
$-3 = -3 \cdot 1$	$-3+\omega$	37	1	$(-\frac{2}{3}\beta - \frac{13}{3},\ -\frac{61}{18}\beta^3 - \frac{169}{9}\beta - \frac{1}{2})$	-1
$-7 = -7 \cdot 1$	$1+\omega$	37	1	$(\frac{3}{7}\beta - \frac{3}{7},\ -\frac{57}{98}\beta^3 - \frac{44}{49}\beta - \frac{1}{2})$	-1
$-11 = -11 \cdot 1$	$38+15\omega$	37	1	$(-\frac{2}{165}\beta^2 - \frac{104}{165},\ -\frac{17}{1210}\beta^3 - \frac{2}{605}\beta - \frac{1}{2})$	-1
$-16 = -4 \cdot 2^2$	$5+2\omega$	$2^2 \cdot 37$	1	$(\frac{\beta^2}{8} - \frac{5}{8},\ \frac{\beta^3}{8} - \frac{1}{2})$	-2
$-48 = -3 \cdot 4^2$	$2+\omega$	$4^2 \cdot 37$	3	$(\frac{115}{588}\beta^2 - \frac{80}{147},\ -\frac{12225}{24696}\beta^3 - \frac{1529}{6174}\beta - \frac{1}{2})$	-1
$-64 = -4 \cdot 4^2$	$10+4\omega$	$4^2 \cdot 37$	2	$(-\frac{\beta^2}{8} - \frac{3}{4},\ -\frac{\beta^3}{8} - \frac{1}{2})$	-2
$-67 = -67 \cdot 1$	$193+76\omega$	67	1	$(-1,\ -\frac{1}{2} + \frac{1}{2}\beta)$	-2
$-75 = -3 \cdot 5^2$	$-15+5\omega$	$5^2 \cdot 37$	3	$(\frac{196}{775}\beta^2 + \frac{136}{27},\ -\frac{1555}{12150}\beta^3 - \frac{25732}{60075}\beta - 1/2)$	-1
$-192 = -3 \cdot 8^2$	$18+8\omega$	$8^2 \cdot 37$	6	$(\frac{7}{3} + \frac{7}{6}\omega,\ -\frac{1}{2} + \frac{1}{36}(\frac{85}{3} + \frac{14}{3}\sqrt{37})\beta)$	-2
$-275 = -11 \cdot 5^2$	$445+180\omega$	$5^2 \cdot 37$	4	$(\frac{2}{11} + \frac{4}{11}\omega,\ -\frac{1}{2} + \frac{1}{242}(\frac{62}{7} + \frac{9}{7}\sqrt{37})\beta)$	-2
$-448 = -7 \cdot 8^2$	$2+2\omega$	$8^2 \cdot 37$	4	$(\frac{45}{7} + \frac{39}{14}\omega,\ -\frac{1}{2} + \frac{1}{196}(\frac{989}{2}\sqrt{37} + \frac{4191}{2})\beta)$	-2

Table 3: ATR extensions of $\mathbb{Q}(\sqrt{37})$ and ATR points on E_{37}

The case $N = 41$. Shiota's Weierstrass equation for E_{41} is

$$E_{41} : y^2 = x^3 - \frac{17}{48}x + \left(-\frac{5}{32} + \frac{1}{27}\sqrt{41}\right)$$

In their computations, Darmon and Logan used instead curve $E'_{41} : y^2 + xy = x^3 - (32 + 5\sqrt{41})x$. This Weierstrass equation was first found by Oort, and there is an explicit isogeny $\psi : E'_{41} \to E_{41}$ of degree 2. Following Darmon-Logan's approach, points $P_M^?$ listed below are points on E'_{41}. Since the isogeny ψ is explicit, it is an easy task to transfer them to points on E_{41}, and this is what we did in

order to compare the Heegner points $P_M \in E_{41}(M)$ with the Stark-Heegner points $\psi(P_M^?) \in E_{41}(\mathbb{C})$. In this case, calculations suggest once again that

$$\ell^2 = \frac{L(E_{41}/F,1)}{\Omega_{E_{41}/F}} = 1,$$

while the values of the exponent s also appear in the table below.

$D_M = D_K \cdot c^2$	β^2	D_L	$\lvert\mathrm{Pic}(\mathcal{O}_c)\rvert$	$P_M^?$	s
$-4 = -4 \cdot 1$	$27 + 10\omega$	41	1	$(-\frac{1}{4},\ -\frac{\beta}{2} + \frac{1}{8})$	1
$-8 = -8 \cdot 1$	$-248 + 67\omega$	41	1	$(-\frac{1}{268}(3\beta^2 + 1481),\ \frac{1}{536}(-254\beta^3 + 3\beta^2 - 108954\beta + 1481))$	0
$-20 = -20 \cdot 1$	$697 + 258\omega$	41	2	$(\frac{1}{43}(\beta^2 - 9),\ \frac{1}{258}(-\beta^3 - 3\beta^2 + 181\beta + 27))$	0
$-23 = -23 \cdot 1$	$398 + 144\omega$	41	3	$(\frac{-71027\beta^2 - 1271153}{9884736},\ \frac{-1095348\beta^3 + 9304537\beta^2 + 16459332\beta + 166521043}{2589800832})$	0
$-32 = -8 \cdot 2^2$	$1 + \omega$	$2^2 \cdot 41$	2	$(\frac{29\beta^2 + 49}{4},\ \frac{1}{16}(-359\beta^3 - 58\beta^2 - 611\beta - 98))$	0
$-36 = -4 \cdot 3^2$	$6 + 3\omega$	$3^2 \cdot 41$	4	$(-8 + 2\omega, (\frac{7}{2} - \frac{1}{2}\sqrt{41})(1 + 5\beta))$	-1
$-40 = -40 \cdot 1$	$35 + 13\omega$	41	2	$(9 + \frac{27}{8}\omega, -\frac{171}{32} - \frac{27}{32}\sqrt{41} + \frac{3}{32}(\frac{109}{2} + \frac{17}{2}\sqrt{41})\beta)$	-1
$-100 = -4 \cdot 5^2$	$10 + 5\omega$	$5^2 \cdot 41$	2	$(\frac{9}{2} + \frac{7}{4}\omega, -\frac{43}{16} - \frac{7}{16}\sqrt{41} + (\frac{3}{8}\sqrt{41} + \frac{19}{8})\beta)$	-2
$-115 = -115 \cdot 1$	$177 + 68\omega$	41	2	$(-\frac{31}{9} - \frac{11}{9}\omega, \frac{73}{36} + \frac{11}{36}\sqrt{41} + \frac{1}{108}(\frac{59}{5} + \frac{9}{5}\sqrt{41})\beta)$	-1
$-160 = -40 \cdot 2^2$	4ω	$2^2 \cdot 41$	4	$(32 + 12\omega, -19 - 3\sqrt{41} + (\frac{173}{2} + \frac{27}{2}\sqrt{41})\beta)$	-2
$-368 = -23 \cdot 4^2$	$43 + 16\omega$	$4^2 \cdot 41$	6	$(\frac{29}{4} + \frac{11}{4}\omega, -\frac{69}{16} - \frac{11}{16}\sqrt{41} + (\frac{13}{4} + \frac{1}{2}\sqrt{41})\beta)$	-2

Table 4: ATR extensions of $\mathbb{Q}(\sqrt{41})$ and ATR points on E'_{41}

4.4. **Proof of Proposition 4.3.** The aim of this section is proving Proposition 4.3, which was left unproved in §4.1 and asserts that the relative discriminant of L/K factors as $d(L/K) = c \cdot \mathcal{N}$, where c is a positive integer such that $L \subset L_c$ (and similarly $L' \subset L'_c$).

Recall our assumption on $N = \mathrm{disc}(F)$ to be odd, and thus square-free. Here we shall assume for notational simplicity that $K \neq \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, so that $\mathcal{O}_K^\times = \{\pm 1\}$; we leave to the reader the task of filling the details for the two excluded fields.

Let us recall first the following classical lemma on Kummer extensions of local fields, which applies in particular to our quadratic extension L/K.

Lemma 4.8. [Hec, §38-39], [Dab] *Let k be a local field containing all p-th roots of unity for some prime p and let $v_k : k^\times \to \mathbb{Z}$ denote the valuation map of k, normalized so that $v_k(k^\times) = \mathbb{Z}$. Let K/k be a Kummer extension of degree p with discriminant $\mathfrak{d}_{K/k}$. Then $K = k(\sqrt[p]{\vartheta})$ for some $\vartheta \in k$ such that $v_k(\vartheta) \in \{0, 1\}$. Moreover,*

(i) *If $v_k(\vartheta) = 1$, $v_k(\mathfrak{d}_{K/k}) = pv_k(p) + (p-1)$.*
(ii) *Assume $v_k(\vartheta) = 0$. If $v_k(p) = 0$, then $v_k(\mathfrak{d}_{K/k}) = 0$. Otherwise, write $\mathfrak{p}_k$ for the unique maximal ideal in k. We have:*
  (a) *If equation $x^p \equiv \vartheta (mod\ \mathfrak{p}_k^{pv_k(p)/(p-1)})$ can be solved in k, then $v_k(\mathfrak{d}_{K/k}) = 0$.*
  (b) *If not, $v_k(\mathfrak{d}_{K/k}) = pv_k(p) + (p-1)(1-\eta)$, where $\eta = \max_\ell\{0 \leq \ell < pv_k(p)/(p-1) \,\big|\, x^p \equiv \vartheta (mod\ \mathfrak{p}_k^\ell)$ can be solved in $\mathcal{O}_k\}$.*

We use the above result in order to deduce several lemmas which shall allow us to reduce the proof of Proposition 4.3 to the case in which L/K is unramified at dyadic primes.

Lemma 4.9. *Let $p \nmid \mathrm{disc}(K)$ be a prime and put $p^* = 8$ if $p = 2$, $p^* = p$ if $p \equiv 1 (mod\ 4)$ and $p^* = -p$ if $p \equiv -1 (mod\ 4)$. Then $K(\sqrt{p^*})$ is contained in the* ring class field *H_c of K associated to the order $\mathcal{O}_c$ of conductor $c = |p^*|$.*

Proof. Suppose first that p is split in K and fix a prime $\mathfrak{p}|p$ in K. Let

$$U = K_\mathfrak{p}^\times \bigcap K^\times \prod_v \mathcal{O}_{c,v}^\times,$$

where the intersection is computed by regarding $K_\mathfrak{p}^\times$ as a subgroup of $\prod_v K_v^\times$ by means of the usual embedding $x_\mathfrak{p} \mapsto (1, ..., 1, x_\mathfrak{p}, 1, ..., 1)$.

Since the map $K_\mathfrak{p}^\times / U \to \mathbb{I}_K / \left(K^\times \prod_v \mathcal{O}_{c,v}^\times\right)$ is injective by [Mi2, p. 173, Prop. 5.2], it follows that $U \subset K_\mathfrak{p}^\times \simeq \mathbb{Q}_p^\times$ corresponds to $H_{c,\mathfrak{P}}/K_\mathfrak{p}$ by local class field theory for any prime $\mathfrak{P}$ of H_c above $\mathfrak{p}$.

Write $c = p^r$ with $r = 3$ if $p = 2$, $r = 1$ if p is odd. Since $1 + p^r\mathbb{Z}_p \subseteq U$, $1 + p^{r-1}\mathbb{Z}_p \not\subset U$ by [Cox, p. 197], an easy calculation shows that

$$U = \{\frac{\alpha}{\overline{\alpha}} \,\big|\, \alpha \in V\} \cdot (1 + \mathfrak{p}^r),$$

where $V = \{\alpha \in K^\times \,\big|\, \mathrm{ord}_v(\alpha) = 0 \ \forall v \neq \mathfrak{p}\}$. Note that $V = \{\pm\alpha_0^n, n \in \mathbb{Z}\}$ for some $\alpha_0 \in K^\times$ such that $\mathrm{ord}_v(\alpha_0) = 0$ for all $v \neq \mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha_0) = n_0 \geq 1$ is minimal. With this notation we have

$$U = \{\big(\frac{\alpha_0}{\overline{\alpha}_0}\big)^n, n \in \mathbb{Z}\} \cdot (1 + \mathfrak{p}^r). \tag{33}$$

Suppose now that p remains inert in $\mathcal{O}_K$. Arguing similarly as before we obtain that the open subgroup $U \subset K_p^\times$ corresponding to $H_{p^r,\mathfrak{P}}/K_p$ by local class field theory is $U = K_p^\times \cap \big(K^\times \prod_v \mathcal{O}_{p^r,v}^\times\big)$, i.e.

$$U = \{\alpha \,\big|\, \alpha \in K^\times, \mathrm{ord}_v(\alpha) = 0, \forall v \neq p\} \cdot (1 + p^r\mathcal{O}_{K_p}) = \{(\pm\alpha_0)^n \,\big|\, n \in \mathbb{Z}\} \cdot (1 + p^r\mathcal{O}_{K_p}), \tag{34}$$

where $\alpha_0 \in K^\times$ is chosen such that $\mathrm{ord}_v(\alpha_0) = 0$ for all $v \neq p$ and $\mathrm{ord}_p(\alpha_0) \geq 1$ is minimal. We can thus take $\alpha_0 = p^{n_0}$ for some $n_0 \geq 1$.

Put $K' = K(\sqrt{p^*})$. Any prime $\mathfrak{p}$ in K above p ramifies in K'. Fix one such prime $\mathfrak{p}$ and put $\mathfrak{p} = \wp^2$ in K' so that $K'_\wp = K_\mathfrak{p}(\sqrt{p^*})$. By class field theory, in order to prove that $K' \subset H_c$ it is enough to show that $U \subset \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K_\mathfrak{p}^{'\times})$. Since $d(K'/K) = p^*$ by Lemma 4.8, K' is contained in the *ray class field* K_c of conductor c of K and it thus suffices to verify that $\alpha_0\overline{\alpha}_0$ (resp. $\pm\alpha_0$) lies in $\mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K_\mathfrak{p}^{'\times})$ if p splits (resp. remains inert) in K.

Assume $p = 2$. Then $\pm1, \pm2 \in \mathrm{Nm}_{K'_\wp/K_\mathfrak{p}}(K_\wp^{'\times})$ because $-1 = \mathrm{Nm}(1 + \sqrt{2})$ and $-2 = \mathrm{Nm}(\sqrt{2})$. The lemma thus follows automatically if 2 is inert in K, while if 2 splits, it follows because $\alpha_0\overline{\alpha}_0$ is a power of 2, hence $\alpha_0\overline{\alpha}_0$ lies in either $\pm\mathbb{Q}_2^{\times^2}$ or $\pm2\mathbb{Q}_2^{\times^2}$.

Assume p is odd. Then $-p^* = \mathrm{Nm}(\sqrt{p^*}) \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K_\mathfrak{p}^{'\times})$. Suppose first p splits in K: as before, it is enough to show that $p \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K^{'\times})$, which we already did if $p^* = -p$. That the same holds when $p^* = p$ follows because $p \equiv 1 (\mathrm{mod}\ 4)$ implies that $-1 \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K_\mathfrak{p}^{'\times})$. Suppose now p remains inert in K; we must show that $\pm p \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K_\mathfrak{p}^{'\times})$. If $p^* = p$ this follows by the same reason as above; if $p^* = -p$, then $p \equiv 3 (\mathrm{mod}\ 4)$, $K_p = \mathbb{Q}_p(\sqrt{-1})$ and thus $-1 \in K_p^{\times^2}$, which allows us to conclude. □

Note that a direct consequence of the previous lemma is that for any odd square free integer m relatively coprime with $\mathrm{disc}(K)$ either $K(\sqrt{m})$ or $K(\sqrt{-m})$ is contained in H_m.

Lemma 4.10. *$d(L/K) = 2^t c_0\mathcal{N}$ for some integer $0 \leq t \leq 3$ and some positive integer $c_0 \geq 1$ relatively coprime to 2 and $\mathcal{N}$. If further 2 is ramified in K, $0 \leq t \leq 2$.*

Proof. Write $K = \mathbb{Q}(\sqrt{-d_0})$ for some square free integer $d_0 > 0$ and $L = K(\sqrt{\beta})$ for some $\beta \in \mathbb{Z} + \mathbb{Z}\sqrt{-d_0}$ and square free in K. Without loss of generality, N can be written as $\mathcal{N}\overline{\mathcal{N}}$ where $\mathcal{N}$ divides the square free part $\mathfrak{B}$ of (β) in K and $\overline{\mathcal{N}}$ is relatively coprime to $\mathfrak{B}$.

Write $\mathfrak{B}_2$ for the largest ideal which divides $\mathfrak{B}$ and is relatively coprime to any prime of K above 2. Since $v_{K_{\mathfrak{p}'}}(2) = 0$ and $v_{K_{\mathfrak{p}'}}(\mathfrak{B}_2) = 1$ for any prime $\mathfrak{p}' \mid \mathfrak{B}_2$, Lemma 4.8 shows that $v_{K_{\mathfrak{p}'}}(\mathfrak{d}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}'}}) = 1$, where $\mathfrak{P}'$ is the prime in L above $\mathfrak{p}'$, thus the prime-to-2 part of $d(L/K)$ is $\mathfrak{B}_2$. Besides, $\mathfrak{B}_2 = \mathcal{N} \cdot \mathfrak{C}$ with $(\mathfrak{C}, \mathcal{N}) = 1$. Since $\mathrm{Nm}_{K/\mathbb{Q}}(\beta)/N$ is a perfect square in $\mathbb{Z}$, $\mathfrak{C}$ is principal and can be written as $\mathfrak{C} = (c_0)$ for some integer $c_0 > 0$. Hence $\mathcal{N}c_0 \mid d(L/K) \mid 2^t\mathcal{N}c_0$ for some integer $t \geq 0$.

If 2 is unramified in K we have $v_{K_\mathfrak{p}}(2) = 1$ for any prime $\mathfrak{p} \mid 2$ in K and it follows from Lemma 4.8 that $d(L/K) = \mathcal{N}c_0 2^t$ with $0 \leq t \leq 3$.

Suppose now that 2 ramifies in K with $(2) = \mathfrak{p}^2$ in K. Then, since $v_{K_\mathfrak{p}}(2) = 2$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\beta)/N$ is a perfect square in $\mathbb{Z}$, we fall into case (ii) of Lemma 4.8: for any prime $\mathfrak{P}$ in L above $\mathfrak{p}$, $L_\mathfrak{P}$ can be written as $K_\mathfrak{p}(\sqrt{\vartheta})$ for some $\vartheta \in K_\mathfrak{p}^\times$ such that $v_{k_\mathfrak{p}}(\vartheta) = 0$. Suppose $v_{K_\mathfrak{p}}(\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}}) \neq 0$. Then Lemma 4.8 (b) asserts that

$$v_{K_\mathfrak{p}}(\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}}) = 5 - \eta,$$

where

$$\eta = \max\{0 \leq \ell < 4 \,\big|\, \exists \iota \in \mathcal{O}_{K_\mathfrak{p}},\, \iota^2 \equiv \vartheta (\mathrm{mod}\ \mathfrak{p}^\ell)\}.$$

A classical result of Hilbert (cf. [HSW], [Hil]) implies that $v_{K_\mathfrak{p}}(\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}})$ is even. Hence $d(L/K) = \mathcal{N}2^t c_0$ with $0 \leq t \leq 2$. □

Lemma 4.11. *It is enough to prove Proposition* 4.3 *when* $d(L/K) = 2^t\mathcal{N}$ *and* $0 \leq t \leq 2$.

Proof. Lemma 4.10 shows in general $d(L/K) = 2^t c_0\mathcal{N}$, where $0 \leq t \leq 3$ and $c_0 \geq 1$. Suppose first that $t = 3$, then 2 is unramified in K by the same lemma. Let $\mathfrak{P}$ and $\mathfrak{p}$ be prime ideals in L and K respectively such that $\mathfrak{P}|\mathfrak{p}|2$. Then $L_\mathfrak{P}$ can be written as $K_\mathfrak{p}(\sqrt{\vartheta})$ for some $\vartheta \in K$ with $v_{K_\mathfrak{p}}(\vartheta) \in \{0, 1\}$. Define $L' = K(\sqrt{\vartheta'})$, where ϑ' is defined as

$$\vartheta' = \begin{cases} \vartheta/2 & \text{if } v_{K_\mathfrak{p}}(\vartheta) = 1; \\ \vartheta & \text{if } v_{K_\mathfrak{p}}(\vartheta) = 0. \end{cases}$$

Hence $v_{K_\mathfrak{p}}(\vartheta') = 0$. Let $\mathfrak{P}'$ be a prime in L' above $\mathfrak{p}$. Then either case (a) or (b) of Lemma 4.8 applies. In case (a), $v_{K_\mathfrak{p}}(\mathfrak{d}_{L'_{\mathfrak{P}'}/K_\mathfrak{p}}) = 0$. In case (b), $v_{K_\mathfrak{p}}(\mathfrak{d}_{L'_{\mathfrak{P}'}/K_\mathfrak{p}}) = 3-\eta$, where $0 \leq \eta \leq 2$, hence $\mathfrak{p}$ is ramified in L', so residue field of $L'_{\mathfrak{P}'}$ is equal to that of $K_\mathfrak{p}$ and consequently $\eta \geq 1$. We conclude that $v_{K_\mathfrak{p}}(\mathfrak{d}_{L'_{\mathfrak{P}'}/K_\mathfrak{p}}) \leq 2$. By Lemma 4.9, $L \subset K(\sqrt{2})L' \subset H_8L'$ with $d(L'/K) = 2^{t'}c_0\mathcal{N}$ for some integer $0 \leq t' \leq 2$.

Suppose now $c_0 > 1$. Setting $L'' = K(\sqrt{\delta\vartheta'/c_0})$ we have $d(L''/K) = 2^{t'}\mathcal{N}$, where $\delta \in \{\pm 1\}$ such that $K(\sqrt{\delta c_0}) \subset H_{c_0}$ as described in Lemma 4.9. By the same lemma, $L' \subset K(\sqrt{\delta c_0})L'' \subset H_{c_0}L''$.

So $L \subset H_8L' \subset H_8H_{c_0}L'' = H_{8c_0}L''$ such that L''/K is a quadratic extension and $d(L''/K) = 2^{t'}\mathcal{N}$ for some integer $0 \leq t' \leq 2$. This justifies we only need to prove proposition 4.3 when $0 \leq t \leq 2$ and $d(L/K) = 2^t\mathcal{N}$. □

Thanks to Lemma 4.11 we can assume in what follows that $c_0 = 1$ and $0 \leq t \leq 2$.

Lemma 4.12. *There is a unique quadratic extension* $\mathcal{L}_{2^t}/K_{2^t}$ *contained in* $K_{2^t\mathcal{N}}$ *such that the set of primes in* K_{2^t} *which ramify in* $\mathcal{L}_{2^t}$ *is the set of primes above* $\mathcal{N}$. *We have* $L \subset \mathcal{L}_{2^t}$.

Proof. Assume first $t = 0$ or 1. Then $\mathrm{Gal}(K_{2^t\mathcal{N}}/K_{2^t}) \cong (\prod_{\mathfrak{p}|\mathcal{N}}(\mathcal{O}_K/\mathfrak{p})^\times)/\{\pm 1\} \cong (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. This is obvious for $t = 0$, and holds for $t = 1$ because $K_2K_\mathcal{N} = K_{2\mathcal{N}}$. Extension $\mathcal{L}_{2^t}/K_{2^t}$ corresponds by Galois theory to the unique primitive even quadratic Dirichlet character ε of conductor N.

Suppose now $t = 2$. Then

$$\mathrm{Gal}(K_{2^t\mathcal{N}}/K_{2^t}) \cong G := \big(\{\pm 1\} \times (\mathbb{Z}/N\mathbb{Z})^\times\big)/\{\pm \mathbb{1}\},$$

where $\mathbb{1} = (1, \mathbf{1})$ is the identity element of $\{\pm 1\} \times (\mathbb{Z}/N\mathbb{Z})^\times$. Again, any extension $\mathcal{L}_{2^t}/K_{2^t}$ as in the statement corresponds to a non-trivial character $\varepsilon' : G \to \{\pm 1\}$ which is trivial on $\{\pm 1\} \times \{\mathbf{1}\}$ and is even and primitive on $\{1\} \times (\mathbb{Z}/N\mathbb{Z})^\times$. As above, the only such character is $\varepsilon' = 1 \times \varepsilon$.

Finally, note that LK_{2^t}/K_{2^t} is a quadratic extension contained in $K_{2^t\mathcal{N}}$. Since $\mathrm{disc}(LK_{2^t}/K_{2^t}) = \mathcal{N}$ it follows that $\mathcal{L}_{2^t} = LK_{2^t}$ and thus $L \subset \mathcal{L}_{2^t}$. □

Recall the quadratic extension L_c of the ring class field H_c introduced in §4.1, over which the Heegner points P_c^+ and $P_c^- \in \mathrm{CM}(c)$ are rational. Lemma 4.12 reduces the proof of Proposition 4.3 to showing that $L_c = \mathcal{L}_c$. Since L_c was defined as the quadratic extension of H_c cut out by the kernel of the single even primitive character ε of conductor N, it suffices to show that $H_{2^t} = K_{2^t}$ for $0 \leq t \leq 2$.

When $t=0$ and we obviously have $H_1=K_1$. If $t=1$ or 2, the ratio of the ray class number h_{2^t} by the ring class number $h(\mathcal{O}_{2^t})$ is (cf. [Mi2, p.154] for this and the remaining notations):

$$\begin{aligned}\frac{h_{2^t}}{h(\mathcal{O}_{2^t})} &= \frac{[U:U_{2^t,1}]^{-1}\mathrm{Nm}(2^t)\prod_{\mathfrak{p}|2^t}(1-\frac{1}{\mathrm{Nm}(\mathfrak{p})})}{\frac{2^t}{[\mathcal{O}_K^\times:\mathcal{O}_{2^t}^\times]}\prod_{p|2^t}(1-\left(\frac{d_K}{p}\right)\frac{1}{p})} \\ &= \begin{cases} \frac{[\mathcal{O}_K^\times:\mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]}\cdot\frac{2^{2t}\left(1-\frac{1}{4}\right)}{2^t\left(1-\left(\frac{d_K}{2}\right)\frac{1}{2}\right)} & \text{if 2 is inert in } K, \\ \frac{[\mathcal{O}_K^\times:\mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]}\cdot\frac{2^{2t}\left(1-\frac{1}{2}\right)^2}{2^t\left(1-\left(\frac{d_K}{2}\right)\frac{1}{2}\right)} & \text{if 2 is split in } K, \\ \frac{[\mathcal{O}_K^\times:\mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]}\cdot\frac{2^{2t}\left(1-\frac{1}{2}\right)}{2^t} & \text{if 2 is ramified in } K. \end{cases} \\ &= \frac{[\mathcal{O}_K^\times:\mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]}\cdot 2^{t-1}. \end{aligned} \tag{35}$$

Since $K\neq\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, $[\mathcal{O}_K^\times:\mathcal{O}_{2^t}^\times]=1$. If $t=1$, then $U=U_{2^t,1}$, so $K_2=H_2$. If $t=2$, then $[U:U_{2^t,1}]=2$, and therefore $K_{2^2}=H_{2^2}$.

References

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*. J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[BD] M. Bertolini and H. Darmon. *Iwasawa's main conjecture for elliptic curves over anticyclotomic* $\mathbb{Z}_p$*-extensions*. Ann. of Math. (2) **162** (2005), no. 1, 1–64.

[BFH] D. Bump, S. Friedberg, and J. Hoffstein. *Nonvanishing theorems for L-functions of modular forms and their derivatives*. Invent. Math. **102** (1990), no. 3, 543–618.

[Cox] D. A. Cox. *Primes of the form* x^2+ny^2*: Fermat, class field theory, and complex multiplication*. John Wiley & Sons (1989).

[Co] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990), 237-258.

[Cr] J. E. Cremona. *Modular symbols for* $\Gamma_1(N)$ *and elliptic curves with everywhere good reduction*. Math. Proc. Camb. Phil. Soc. (1992), **111**, 199–218.

[Dab] M. Daberkow. *On computations in Kummer extensions*. J. Symbolic Computation **31** (2001), 113–131.

[DL] H. Darmon and A. Logan. *Periods of Hilbert modular forms and rational points on elliptic curves*. International Math. Res. Not. **40** (2003), 2153–2180.

[ES] J. S. Ellenberg and C. Skinner. *On the modularity of* $\mathbb{Q}$*-curves*. Duke Math. J. **109** (2001), no. 1, 97–122.

[Fu] K. Fujiwara. *Deformation rings and Hecke algebras in the totally real case*. Preprint 1996, revised 2004, 2006.

[Gar] J. Gärtner. *Points de Darmon et variétés de Shimura*. Thèse de Doctorat, Université Paris 7 (Jussieu) (2010).

[Ge] S. Gelbart. *Automorphic forms on adèle groups*. Ann. of Math. Studies **83**, Princeton Univ. Press, Princeton, NJ (1975).

[GG] E. González and X. Guitart. *On the modularity level of modular abelian varieties over number fields*. J. Number Theory **130** (2010), no. 7, 1560-1570.

[GQ] X. Guitart and J. Quer. *Modular abelian varieties over number fields*. Preprint available at http://arxiv.org/abs/0905.2550.

[GZ] B.H. Gross and D.B. Zagier. *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), no. 2, 225–320.

[Hec] E. Hecke. *Lectures on the theory of algebraic numbers*. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. Graduate Texts in Mathematics, 77. Springer-Verlag, New York-Berlin (1981).

[Hil] D. Hilbert. *Über die Theories des relativquadratischen Zahlkörpers*. Math. Ann. **51** (1899), 1–127.

[HSW] J.G. Huard, B.K. Spearman, and K.S. Williams. *Integral bases for quartic fields with quadratic subfields*. J. Number Theory **51** (1995), no. 1, 87–102.

[JM] F. Jarvis and J. Manoharmayum. *On the modularity of supersingular elliptic curves over certain totally real number fields*. J. Number Theory **128** (2008), no. 3, 589–618.

[Ko] V.A. Kolyvagin. *Finiteness of* $E(\mathbf{Q})$ *and* $Ш(E,\mathbf{Q})$ *for a subclass of Weil curves*. Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 670–671; translation in Math. USSR-Izv. 32 (1989), no. 3, 523–541.

[KL] V. A. Kolyvagin and D. Yu. Logachev. *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*. Leningrad Math. J., **1** (1990), no. 5, 1229–1253.

[KL2] V. A. Kolyvagin and D. Yu. Logachev. *Finiteness of Ш over totally real fields*. Math. USSR Izvestiya **39** (1992), no. 1, 829–853.

[KW] C. Khare and J.-P. Wintenberger. *Serre's modularity conjecture I, II*. Invent. Math. **178** (2009), no. 3, 485–504 and 505–586.

[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.

[Mi] J. S. Milne. *On the arithmetic of abelian varieties*. Invent. Math. **17** (1972), 177–190.

[Mi2] J. S. Milne. *Class field theory*. Available at http://www.jmilne.org/math.

[MM] M.R. Murty and V.K. Murty. *Mean values of derivatives of modular L-series*. Ann. of Math. (2) **133** (1991), no. 3, 447–475.
[Oda] T. Oda. *Periods of Hilbert modular surfaces*. Progress in Mathematics, **19**. Birkhäuser, Boston, Mass. (1982).
[PA] PARI/GP, version `2.3.4`, Bordeaux (2008). Available at http://pari.math.u-bordeaux.fr/.
[Pa] A. Pacetti, On the change of root number under twisting and applications, available at arXiv:1010.3781.
[Pi] R.G.E. Pinch. *Elliptic curves over number fields*. D. Phil thesis, Oxford University (1982).
[Ri] K. A. Ribet. *Abelian varieties over $\mathbb{Q}$ and modular forms*, in *Modular curves and abelian varieties*. J. Cremona, J.-C. Lario, J. Quer, K. Ribet (eds.), Progress in Mathematics **224**, Birkhäuser (2004), 241–261.
[Ro] D.E. Rohrlich. *Nonvanishing of L-functions and structure of Mordell-Weil groups*. Journal für di Reine und Angewand. Math. **417** (1991), 1–26.
[Ro2] D.E. Rohrlich. *Variation of the root number in families of elliptic curves*. Compositio Math. **87** (1993) 119–151.
[Shim] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton Univ. Press, Princeton, NJ (1994).
[Shio] K. Shiota. *On the explicit models of Shimura's elliptic curves*. J. Math. Soc. Japan **38** (1986), no. 4, 649–659.
[SkWi] C. Skinner and A. Wiles. *Nearly ordinary deformations of irreducible residual representations*. Ann. Fac. Sci. Toulouse Math. (6) **10** (2001), 185–215.
[TW] R. Taylor and A. Wiles. *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) **141** (1995), no. 3, 553–572.
[TZ] Y. Tian and S. Zhang. Book, in progress.
[Wa] J.-L. Waldspurger. *Sur les valeurs de certaines fonctions L automorphes en leur centre de symmétrie*. Compositio Math. **54** (1985), 173–242.
[Wi] A. Wiles. *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) **141** (1995), no. 3, 443–551.
[YZZ] X. Yuan, W. Zhang, and S. Zhang. *Heights of CM points I: Gross–Zagier formula*. Preprint.
[Zh] S. Zhang. *Heights of Heegner points on Shimura curves*. Ann. of Math. (2) **153** (2001), no. 1, 27–147.
[Zh2] S. Zhang. *Arithmetic of Shimura curves*. Science China Mathematics **53** (2010), 573–592.
[Zhao] Y. Zhao. McGill Univ. Ph. D Thesis. In progress.

H. D.: Department of Mathematics and Statistics, McGill University, 805 Sherbooke Street West, H3A-2K6 Montreal, Canada
E-mail address: `darmon@math.mcgill.ca`

V. R.: Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, C. Jordi Girona 1-3, 08034 Barcelona, Spain
E-mail address: `victor.rotger@upc.edu`

Y. Z.: Department of Mathematics and Statistics, McGill University, 805 Sherbooke Street West, H3A-2K6 Montreal, Canada
E-mail address: `zhao@math.mcgill.ca`