An Algorithm for Modular Elliptic Curves over Real Quadratic Fields

Lassina Dembélé

CONTENTS

Let F be a real quadratic field with narrow class number one, and f a Hilbert newform of weight 2 and level $\mathfrak{n}$ with rational Fourier coefficients, where $\mathfrak{n}$ is an integral ideal of F. By the Eichler–Shimura construction, which is still a conjecture in many cases when $[F:\mathbb{Q}]>1$, there exists an elliptic curve E_f over F attached to f. In this paper, we develop an algorithm that computes the (candidate) elliptic curve E_f under the assumption that the Eichler–Shimura conjecture is true. We give several illustrative examples that explain among other things how to compute modular elliptic curves with everywhere good reduction. Over real quadratic fields, such curves do not admit any parameterization by Shimura curves, and so the Eichler–Shimura construction is still conjectural in this case.

1. INTRODUCTION

Let F be a totally real number field of degree n, $\mathcal{O}_F$ its ring of integers, and $\mathfrak{n} \subseteq \mathcal{O}_F$ an integral ideal. Let f be a Hilbert newform of weight 2 and level $\mathfrak{n}$. The differential form attached to f is given by $\omega_f = (2\pi i)^n f(z_1,\dots,z_n)\,dz_1\cdots dz_n$, and for each prime $\mathfrak{p}$, we let $a_{\mathfrak{p}}(f)$ be the Fourier coefficient of f at $\mathfrak{p}$. Let E be an elliptic curve defined over F. The trace of the Frobenius endomorphism acting on E at the prime $\mathfrak{p}$ is denoted by $a_{\mathfrak{p}}(E)$. We recall that for $\mathfrak{p}\nmid\mathfrak{n}$, $a_{\mathfrak{p}}(E) = \mathrm{N}(\mathfrak{p})+1-\#\tilde{E}(\mathbb{F}_{\mathfrak{p}})$, where $\mathbb{F}_{\mathfrak{p}}=\mathcal{O}_F/\mathfrak{p}$ is the residue field at $\mathfrak{p}$ and $\tilde{E}$ the reduction of E modulo $\mathfrak{p}$; and $\mathrm{N}(\mathfrak{p})$ is the norm of $\mathfrak{p}$. The L-series of f is given by

$$L(f,s) := \sum_{\mathfrak{m}\subseteq\mathcal{O}_F} \frac{a_{\mathfrak{m}}(f)}{\mathrm{N}(\mathfrak{m})^s},$$

2000 AMS Subject Classification: Primary 11-xx; Secondary 11Gxx

Keywords: Hilbert modular forms, elliptic curves, elliptic curves with everywhere good reduction, Oda conjecture

1058-6458/2008 $0.50 per page
Experimental Mathematics **17**:4, page 427

where $a_{\mathfrak{m}}(f)$ is the Fourier coefficient of f at the integral ideal $\mathfrak{m}$; and the L-series of the curve E is given by

$$L(E,s) := \prod_{\mathfrak{p}|\mathrm{cond}(E)} \left(1 - \frac{a_{\mathfrak{p}}(E)}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1} \times \prod_{\mathfrak{p}\nmid\mathrm{cond}(E)} \left(1 - \frac{a_{\mathfrak{p}}(E)}{\mathrm{N}(\mathfrak{p})^s} + \frac{1}{\mathrm{N}(\mathfrak{p})^{2s-1}}\right)^{-1}.$$

This is an analytic function that converges for $\Re(s) > \frac{3}{2}$, and we have the following conjecture.

Conjecture 1.1. *Let f be a Hilbert eigenform with integer Fourier coefficients. Then there exists an elliptic curve E_f such that $L(E_f, s) = L(f, s)$.*

This conjecture is known for $F = \mathbb{Q}$ as the Eichler–Shimura construction, and its proof uses the arithmetic theory of the modular curve $X_0(\mathfrak{n})$ and its Jacobian $\mathrm{Jac}(X_0(\mathfrak{n}))$. In fact, using the theory of modular symbols, one can make this construction very explicit. This is used in a very systematic way by Cremona [Cremona 97] in order to build his database of (modular) elliptic curves over the rationals. Unfortunately, when $[F : \mathbb{Q}] > 1$, the theory of modular Jacobians does not generalize very well, because Hilbert–Blumenthal modular varieties prove not to be good substitutes for modular curves, since they do not provide any uniformization for elliptic curves. As an alternative, the theory of Shimura curves has been exploited to prove many cases of the conjecture. This approach, however, needs to assume in this case that the form f satisfies certain restrictive conditions imposed by the use of the Jacquet–Langlands correspondence. Furthermore, it is very hard to use this method in practice to effectively compute the curve E_f. (Examples of such results can be found in [Zhang 01] and references therein.)

Although Hilbert–Blumenthal varieties are not good substitutes for modular curves, they provide the most natural approach to Conjecture 1.1. Indeed, the Eichler–Shimura construction can be phrased in the language of cohomology or motives, which is better suited for working in higher dimensions. This was observed by Oda in the early 1980s. In [Oda 82], he formulated a cohomological version of Conjecture 1.1 when F is a real quadratic field. He later generalized this to totally real fields of arbitrary degree in [Oda 83]. From now on, we will restrict ourselves to the case that F is a real quadratic field and recall the reformulation of Conjecture 1.1 by Oda. In order to do so, we need to introduce some notation. Let $X_0(\mathfrak{n})/\mathbb{Q}$ be a compact arithmetic Hilbert modular surface of level $\mathfrak{n}$. (We recall that such compactifications exist thanks to [Dimitrov 04].) Let $H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})$ be the middle-degree cuspidal cohomology of the surface $X_0(\mathfrak{n})$. The space $H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})$ comes equipped with a Hecke action provided by algebraic correspondences. Let $H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f$ be the isotypic component that corresponds to f. This has a Hodge structure of type $\{(2,0),(1,1),(0,2)\}$. Then Oda's conjecture can be stated as follows.

Conjecture 1.2. (Oda.) *Let f be a Hilbert newform of weight 2 and level $\mathfrak{n}$ with integer Fourier coefficients. There exists an elliptic curve E_f defined over F with good reduction outside $\mathfrak{n}$, and an isomorphism of Hodge structures*

$$\phi : H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f \cong H^1(E_f, \mathbb{Q}) \otimes H^1(\bar{E}_f, \mathbb{Q}),$$

where $\bar{E}_f$ is the Galois conjugate of E_f.

In [Oda 82], Oda was able to construct the elliptic curve E_f as a complex curve. However, he was able to prove that E_f is defined over F only when the newform f is a base-change lift from $\mathbb{Q}$. In this paper, we propose an algorithm that explicitly constructs an integral model for the curve E_f assuming that we know its discriminant. Not only does this provide some numerical evidence for Conjecture 1.1, but we think that it is the first algorithm that gives a way to systematically construct modular elliptic curves over real quadratic fields. Our algorithm may be of special interest when the newform f corresponds to an elliptic curve E_f with everywhere good reduction. In that case, the approach via Shimura curves is not applicable. However, our algorithm will still produce the curve E_f. We illustrate this with several examples, including the curve $y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + 71 + 34\omega$, where $\omega = \frac{1+\sqrt{509}}{2}$, constructed by Pinch [Pinch 82]. This curve is not a $\mathbb{Q}$-curve and so cannot be obtained by the method in [Cremona 92].

The paper is organized as follows. In Section 2, we present the strategy of our algorithm. In Sections 3 and 4, we explain how to compute the periods of the curve E_f. In Section 5, we present the algorithm, which is followed by several illustrative examples. As a final application of our algorithm, we explain in Section 6 how to construct modular elliptic curves with everywhere good reduction.

2. THE STRATEGY OF THE ALGORITHM

For simplicity, we will assume throughout this paper that F has narrow class number one. We let v_1 and v_2 be

the two archimedean places, and we assume that there is a fundamental unit $\varepsilon \in F$ such that $\varepsilon_1 = v_1(\varepsilon) > 0$ and $\varepsilon_2 = v_2(\varepsilon) < 0$. We denote the discriminant of F by D. We intend to combine the analytic construction of Oda in [Oda 82] and the Weierstrass uniformization theorem in order to find an equation for E_f over F. (See [Cremona 97, Chapter 1] or [Silverman 86, Chapter 5] for background material on elliptic curves.)

Before we do so, we need to refine Oda's conjecture. To this end, let $\omega_f = (2\pi i)^2\sqrt{D}^{-1} f(z_1, z_2)\, dz_1 dz_2$ be the *normalized* differential form attached to f. Also, let ω_E be the Néron differential form of E, and Λ_E the Néron lattice attached to ω_E. We let Ω_E^+ (respectively $\Omega_{\bar{E}}^+$) be the real period of E (respectively $\bar{E}$), and Ω_E^- (respectively $\Omega_{\bar{E}}^-$) the imaginary period of E (respectively $\bar{E}$). We then define the period lattices $\Lambda_E^{\pm} = \Omega_{\bar{E}}^{\pm}\Lambda_E$. Let $\mathfrak{H}$ be the Poincaré upper half-plane. We recall that the two involutions

$$\begin{aligned} \mathfrak{H}^2 &\to \mathfrak{H}^2, \\ (z_1, z_2) &\overset{\eta_1}{\mapsto} (\varepsilon_2\bar{z}_1, \varepsilon_1 z_2), \\ (z_1, z_2) &\overset{\eta_2}{\mapsto} (\varepsilon_1 z_1, \varepsilon_2\bar{z}_2), \end{aligned}$$

descend to the modular surface $X_0(\mathfrak{n})$ and give the Hodge type decomposition

$$\begin{aligned} &H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f \\ &\quad = H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f^{++} \oplus H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f^{-+} \\ &\qquad \oplus H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f^{+-} \oplus H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f^{--}. \end{aligned}$$

Now let $\Lambda_f \subset H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{Q})_f$ be an integral Hodge structure. This is a lattice in $H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{R})_f$. By Poincaré duality, we have an isomorphism of complex spaces $H^2_{\mathrm{cusps}}(X_0(\mathfrak{n}), \mathbb{R})_f \cong \mathbb{C}^2$ by which we identify Λ_f with its image

$$\Lambda_f = \mathbb{Z}\Omega_f^{++} \oplus \mathbb{Z}\Omega_f^{-+} \oplus \mathbb{Z}\Omega_f^{+-} \oplus \mathbb{Z}\Omega_f^{--},$$

where Ω_f^{++} and Ω_f^{--} are positive real numbers and Ω_f^{-+} and Ω_f^{+-} are purely imaginary with positive imaginary parts.

Concretely put, the Oda conjecture asserts that there are nonzero rational numbers $c_{ss'} \in \mathbb{Q}$ such that

$$c_{ss'}\Omega_f^{ss'} = \Omega_E^s \Omega_{\bar{E}}^{s'}, \text{for all} s, s' \in \{-, +\}.$$

This phenomenon illustrates the fact that the periods of the form f are actually mixtures of the periods of E_f and its Galois conjugate $\bar{E}_f$. Unfortunately, there is no known method to separate them, since we do not know the curve a priori. So we must find a way to overcome this problem. The first step in that direction is provided by the following lemma.

Lemma 2.1. *Assume Conjecture 1.2, and let Λ_f^+ (respectively Λ_f^-) be the lattice given by $\Lambda_f^+ = \langle \Omega_f^{++}, \Omega_f^{-+} \rangle$ or $\langle 2\Omega_f^{++}, \Omega_f^{++} + \Omega_f^{-+} \rangle$ (respectively $\Lambda_f^- = \langle \Omega_f^{+-}, \Omega_f^{--} \rangle$ or $\langle 2\Omega_f^{+-}, \Omega_f^{+-} + \Omega_f^{--} \rangle$) depending on whether the real locus of E_f has one or two connected components. Then the complex curves $\mathbb{C}/\Lambda_f^+$ and $\mathbb{C}/\Lambda_f^-$ are isomorphic and belong to the same isogeny class as the complex curve $E_f(\mathbb{C})$.*

Proof: The fact that $\mathbb{C}/\Lambda_f^+$ and $\mathbb{C}/\Lambda_f^-$ are isomorphic complex curves depends only on the modular form f. Indeed, this is a consequence of the Riemann–Hodge relations (see [Oda 82, Theorem 4.4]). The rest of the lemma follows by observing that the lattice Λ_f^+ is homothetic to a lattice contained in Λ_E. □

From Lemma 2.1, it is now easy to compute the j-invariant of the curve E_f. The j-invariant of E_f as a modular function is given by $j(\tau)$, where

$$\tau = \frac{\Omega_f^{-+}}{\Omega_f^{++}} \quad \text{or} \quad \tau = \frac{1}{2}\left(1 + \frac{\Omega_f^{-+}}{\Omega_f^{++}}\right),$$

depending on whether the real locus of E_f has one or two connected components. We can assume without loss of generality that the curve $E = E_f$ is given by a global minimal Weierstrass equation, with $j(\tau) = j(E) = \frac{c_4^3}{\Delta_E}$. Since we assume that we know the discriminant Δ_E, we can obtain c_4 if we know $j(\tau)$ to sufficient precision. Then we can compute c_6 from the relation $c_4^3 - c_6^2 = 1728\Delta_E$ and reconstruct our minimal Weierstrass equation for E from its invariants c_4 and c_6, using Kraus and Laska's algorithm.

3. COMPUTING THE PERIOD LATTICE: THE ODA APPROACH

In this section, we recall some results about the periods constructed by Oda in [Oda 82, Section 16.2]. His construction uses certain explicit 2-cycles that are reminiscent of the classical modular symbols. Let $\chi : (\mathcal{O}_F/\mathfrak{c})^\times \to \mathbb{C}^\times$ be a primitive quadratic character of conductor $\mathfrak{c} = (\nu)$ that is prime to $\mathfrak{n}$, where $\nu \gg 0$. Also, let $V \subseteq \mathcal{O}_F^{\times +}$ be a subgroup of finite index such that $V \subseteq 1 + \mathfrak{c}$. We extend the character χ to nonunits in the obvious way. The twisted L-series of f by χ is given by

$$L(f, \chi, s) := \sum_{\mathfrak{m} \subseteq \mathcal{O}_F} \frac{\chi(\mathfrak{m}) a_{\mathfrak{m}}(f)}{\mathrm{N}(\mathfrak{m})^s},$$

where $a_{\mathfrak{m}}(f)$ is the Fourier coefficient of f at the ideal $\mathfrak{m}$. For the trivial character $\mathbf{1}$, we have $L(f,\mathbf{1},s) = L(f,s)$.

Proposition 3.1. (Oda.) *Let Λ_f be a period lattice in the isotypic component of f and let*

$$\Omega^{ss'}_{f,\chi,V} = -4\pi^2 \mathrm{disc}(F)^{1/2}[\mathcal{O}_F^{\times +} : V]G(\overline{\chi})L(f,\chi,1),$$

where $G(\chi)$ is the Gauss sum of the character χ, and $\chi(\bar{\varepsilon}) = s$, $\chi(\varepsilon) = s'$ with $s, s' \in \{\pm 1\}$. Then $\Omega^{ss'}_{f,\chi,V}$ is a rational multiple of $\Omega^{ss'}_f$ when $\chi(-1) = ss'$.

Remark 3.2. We note that Proposition 3.1 is slightly different from [Oda 82, Theorem 16.3] because of the fact that the differential form we use is normalized.

By making use of Proposition 3.1, it is possible to compute the period lattice Λ_f up to (rational) homothety. But in analogy with the classical setting, one expects a stronger statement to be true. The following conjecture can be found in [Bertolini et al. 04].

Conjecture 3.3. *Let $\chi : (\mathcal{O}_F/\mathfrak{c})^{\times} \to \mathbb{C}^{\times}$ be a primitive quadratic character of conductor $\mathfrak{c} = (\nu)$ that is prime to $\mathfrak{n}$, where $\nu \gg 0$. Let*

$$\Omega^{ss'}_{f,\chi} = -4\pi^2 \mathrm{disc}(F)^{1/2} G(\overline{\chi}) L(f,\chi,1),$$

where $G(\chi)$ is the Gauss sum of the character χ, and $\chi(\bar{\varepsilon}) = s$ and $\chi(\varepsilon) = s'$. Assume that Conjecture 1.2 is true. Then $\Omega^{ss'}_{f,\chi}$ is an integer multiple of $\Omega^{s}_{E}\Omega^{s'}_{\bar{E}}$ when $\chi(-1) = ss'$.

We need to find a way to efficiently compute the periods we have just described. This amounts to finding an effective way to compute good approximations of the special values $L(f,\chi,1)$. In the rest of this section, we explain how this can be done. (The method is closely related to the one used in [Cremona 97, Propositions 2.11.1 and 2.11.2].)

Let W_N be the Atkin–Lehner involution given by

$$W_N : z = (z_1, z_2) \mapsto \left(-\frac{1}{Nz_1}, -\frac{1}{\overline{N} z_2} \right),$$

where N is a totally positive generator of $\mathfrak{n}$, and let

$$\begin{aligned} f(z_1,z_2) &= \sum_{\mu \in \mathcal{O}_F^+} c((\mu)) \exp\left[2\pi i \mathrm{Tr}\left(\frac{\varepsilon \mu z}{\sqrt{D}} \right) \right] \\ &= \sum_{\mu \in \mathcal{O}_F^+/\mathcal{O}_F^{\times +}} c((\mu)) \\ &\quad \times \sum_{u \in\, \mathcal{O}_F^{\times +}} \exp\left[2\pi i \mathrm{Tr}\left(\frac{\varepsilon \mu u z}{\sqrt{D}} \right) \right] \end{aligned}$$

be the Fourier expansion of f. Then $f_\chi = f \otimes \chi \in S_2(\mathfrak{n}\mathfrak{c}^2)$, and its Fourier expansion is given by

$$\begin{aligned} f_\chi(z_1,z_2) &= \sum_{\mu \in \mathcal{O}_F^+} c((\mu))\chi(\mu) \exp\left[2\pi i \mathrm{Tr}\left(\frac{\varepsilon \mu z}{\sqrt{D}} \right) \right] \\ &= \sum_{\mu \in \mathcal{O}_F^+/\mathcal{O}_F^{\times +}} c((\mu))\chi(\mu) \\ &\quad \times \sum_{u \in \mathcal{O}_F^{\times +}} \exp\left[2\pi i \mathrm{Tr}\left(\frac{\varepsilon \mu u z}{\sqrt{D}} \right) \right]. \end{aligned}$$

The following lemma gives an optimized way of computing the special value $L(f,1)$, which in turn tells us how to efficiently compute $L(f,\chi,1)$ for a given character χ.

Lemma 3.4. *Let $f \in S_2(\mathfrak{n})$ be an eigenform, with $W_N f = f \,\|\, W_N = \varepsilon_N f$ ($\varepsilon_N = \pm 1$). If $\varepsilon_N = 1$, then $L(f,1) = 0$; otherwise,*

$$\begin{aligned} L(f,1) = -\frac{D}{2\pi^2} \sum_{\mu \in \mathcal{O}_F^+} \frac{c((\mu))}{\mathrm{N}(\mu)} \left[1 - \exp\left(-\frac{2\pi\mu\varepsilon}{\sqrt{DN}} \right) \right] \\ \times \exp\left[\frac{2\pi}{\sqrt{D}} \left(\frac{\bar{\mu}\bar{\varepsilon}}{\sqrt{\overline{N}}} - \frac{\mu}{\sqrt{N}} \right) \right]. \end{aligned}$$

Proof: By definition,

$$\begin{aligned} L(f,1) &= \int \int_{\mathcal{O}_F^{\times +} \backslash \mathbb{R}_+^2} f(iy_1, iy_2) dy_1 dy_2 \\ &= \int_{\tau_0}^{\varepsilon^2 \tau_0} \int_0^{i\infty} f(z_1,z_2)\, dz_1 dz_2, \end{aligned}$$

with τ_0 arbitrarily chosen on the imaginary axis. But choosing $\tau_0 = i/\varepsilon\sqrt{N}$ and making the change of variable $z \mapsto W_N(z)$, we get

$$\begin{aligned} L(f,1) &= \int_{\tau_0}^{\varepsilon^2 \tau_0} \int_0^{i\infty} f \,\|\, W_N(z_1,z_2)\, dz_1 dz_2 \\ &= (f \| W_N, 1) = \varepsilon_N L(f,1). \end{aligned}$$

This gives the first part of the lemma.

To get the second part, keeping the same choice of τ_0 as before, we choose C on the imaginary axis and split the integral as

$$L(f,1) = \int_{\tau_0}^{\varepsilon^2\tau_0}\int_0^C f(z_1,z_2)dz_1dz_2 + \int_{\tau_0}^{\varepsilon^2\tau_0}\int_C^{i\infty} f(z_1,z_2)\,dz_1dz_2.$$

Again choosing $C = i/\sqrt{\overline{N}}$ and making the change of variable $z \mapsto W_N(z)$ in the first integral of the sum, we get that

$$L(f,1) = (1+\varepsilon_N)\int_{\tau_0}^{\varepsilon^2\tau_0}\int_C^{i\infty} f(z_1,z_2)\,dz_1dz_2.$$

We then complete the proof by integrating the series term by term. The splitting of the integral gives an optimal convergence rate because the choices of τ_0 and C preserve the convergence rate under Atkin–Lehner involution and also ensure that both integrals have the same convergence rate. □

Remark 3.5. Let χ be a quadratic character of conductor $\mathfrak{c}$. Then by Atkin–Lehner, we know that $f_\chi \in S_2(\mathfrak{n}\mathfrak{c}^2)$ and $W_{N\nu^2}f_\chi = \varepsilon_N\chi(-N)f_\chi$. Therefore, by Lemma 3.4, when $\varepsilon_N\chi(-N) = 1$,

$$L(f,\chi,1) = -\frac{D}{2\pi^2}\sum_{\mu\in\mathcal{O}_F^+}\frac{c((\mu))}{\mathrm{N}(\mu)}\chi(\mu) \times\left[1-\exp\left(-\frac{2\pi\mu\varepsilon}{\nu\sqrt{DN}}\right)\right] \times\exp\left[\frac{2\pi}{\sqrt{D}}\left(\frac{\bar\mu\bar\varepsilon}{\bar\nu\sqrt{\overline{N}}}-\frac{\mu}{\nu\sqrt{N}}\right)\right].$$

Using the fact that every totally positive unit is of the form ε^{2k}, $k\in\mathbb{Z}$, this series can be rearranged as

$$L(f,\chi,1) = -\frac{D}{2\pi^2}\sum_{\mu\in\mathcal{O}_F^+/\mathcal{O}_F^{+\times}}\frac{c((\mu))}{\mathrm{N}(\mu)}\chi(\mu) \times\left(\sum_{k\in\mathbb{Z}}\left[1-\exp\left(-\frac{2\pi\mu\varepsilon^{2k+1}}{\nu\sqrt{DN}}\right)\right] \times\exp\left[\frac{2\pi}{\sqrt{D}}\left(\frac{\bar\mu\bar\varepsilon^{2k+1}}{\bar\nu\sqrt{\overline{N}}}-\frac{\mu\varepsilon^{2k}}{\nu\sqrt{N}}\right)\right]\right).$$

4. COMPUTING THE PERIOD LATTICE: THE DARMON APPROACH

The Oda cycles provide a very efficient way to compute a period lattice Λ_f associated to the modular form f. Unfortunately, in a way that is reminiscent of the classical setting, this method gives only the components Ω_f^{++} and Ω_f^{--}, or Ω_f^{-+} and Ω_f^{+-}, depending on whether $\varepsilon_N = 1$ or $\varepsilon_N = -1$, when the level $\mathfrak{n}$ is a square. In order to circumvent this problem, we present a second approach, which is based on a construction of Darmon [Darmon 04, Chapter 8]. His construction is a more down-to-earth reformulation of the Oda conjecture in the language of group cohomology. Although the primary goal of [Darmon 04] was to construct generalizations of so-called Stark–Heegner points to elliptic curves over real quadratic fields, we will see that their results actually give a way to compute the period lattices Λ_f^+ and Λ_f^-. We recall this construction along the lines of [Darmon and Logan 03].

First, we define the differential forms

$$\omega_f^{\pm} := -4\pi^2\sqrt{D}^{-1}\big\{f(z_1,z_2)dz_1dz_2 \pm f(-\varepsilon_1\bar z_1,-\varepsilon_2 z_2)d(\varepsilon_1\bar z_1)d(\varepsilon_2 z_2)\big\}.$$

The differential forms $\omega_f^{\pm}$ are Γ-invariant, where $\Gamma = \Gamma_0(\mathfrak{n})$, and so we have

$$\int_{\gamma\tau_1}^{\gamma\tau_2}\int_{\gamma\tau_3}^{\gamma\tau_4}\omega_f^{\pm} = \int_{\tau_1}^{\tau_2}\int_{\tau_3}^{\tau_4}\omega_f^{\pm}, \quad \text{for all } \gamma\in\Gamma.$$

Let $\mathbb{Z}[\Gamma]$ be the group ring of Γ and I_Γ its augmentation ideal. We tensor the exact sequence

$$0\to I_\Gamma\to\mathbb{Z}[\Gamma]\to\mathbb{Z}\to 0$$

with I_Γ and take the module of coinvariants. This gives the exact sequence

$$0\to K_\Gamma\to(I_\Gamma\otimes I_\Gamma)_\Gamma\xrightarrow{r}(\mathbb{Z}[\Gamma]\otimes I_\Gamma)_\Gamma\to\Gamma_{ab}\to 0,$$

where K_Γ is the kernel of the natural homomorphism r and we use the canonical identification of I_Γ/I_Γ^2 with the abelianization Γ_{ab} of Γ.

We choose $\tau_1,\tau_2\in\mathfrak{H}$ and put

$$I^{\pm}_{\tau_1,\tau_2}((\gamma_1-\gamma_1')\otimes(\gamma_2-\gamma_2')) := \int_{\gamma_1\tau_1}^{\gamma_1'\tau_1}\int_{\gamma_2\tau_2}^{\gamma_2'\tau_2}\omega_f^{\pm},$$

for all $\gamma_i,\gamma_i'\in\Gamma$, and extend it linearly to $(I_\Gamma\otimes I_\Gamma)_\Gamma$. This is possible because of the Γ-invariance of the forms $\omega_f^{\pm}$. The maps $I^{\pm}_{\tau_1,\tau_2}:(I_\Gamma\otimes I_\Gamma)_\Gamma\to\mathbb{C}$ are group homomorphisms whose restrictions to K_Γ do not depend on the choices of τ_1 and τ_2, and so the subgroups $\Lambda_f^{\pm} := I^{\pm}_{\tau_1,\tau_2}(K_\Gamma)$ depend only on the form f. The following conjecture is a combination of Conjectures 1.1. and 2.1 in [Darmon and Logan 03], and it is easy to see that it is a reformulation of Conjecture 1.2.

Conjecture 4.1. [Darmon and Logan 03] *Let f be a Hilbert newform with integer Fourier coefficients. The subgroup*

Λ_f^+ (respectively Λ_f^-) is a lattice in $\mathbb{C}$ that is commensurable with the lattice Λ_E^+ (respectively Λ_E^-).

Let e_Γ be the exponent of Γ_{ab}, which is finite by [Darmon and Logan 03], and let $\tilde{\Lambda}_f^\pm = e_\Gamma^{-1}\Lambda_f^\pm$. The construction of Stark–Heegner points relies on the semidefinite integral

$$\mathfrak{H}^3 \to \mathbb{C}/\tilde{\Lambda}_f^\pm,$$
$$(\tau, x, y) \mapsto \int^\tau \int_x^y \omega_f^\pm,$$

which enjoys the following crucial properties:

(i) $\int^\tau \int_{x_1}^{x_2} \omega_f^\pm + \int^\tau \int_{x_2}^{x_3} \omega_f^\pm = \int^\tau \int_{x_1}^{x_3} \omega_f^\pm$.

(ii) $\int^{\tau_2} \int_{x_1}^{x_2} \omega_f^\pm - \int^{\tau_1} \int_{x_1}^{x_2} \omega_f^\pm = \int_{\tau_1}^{\tau_2} \int_{x_1}^{x_2} \omega_f^\pm \in \mathbb{C}/\Lambda_f^\pm$.

For more details on the construction of this semidefinite integral, we refer to [Darmon 04, Chapter 8], [Bertolini et al. 04], and [Darmon and Logan 03].

Let K/F be a quadratic extension that is complex at v_1 and real at v_2, and let $\mathcal{O}_K$ be the ring of integers of K. An *optimal embedding* of K into $M_2(F)$ is an F-algebra homomorphism $\mathbf{\Psi} : K \to M_2(F)$ such that $\mathbf{\Psi}(\mathcal{O}_K) = \mathbf{\Psi}(K) \cap M_2(\mathcal{O}_F)$. By making use of the Dirichlet units theorem, it can be shown that $\mathcal{O}_K^\times$ is a free rank-one abelian group modulo $\mathcal{O}_F^\times$. Also, it can be shown that the group $\mathbf{\Psi}(\mathcal{O}_K^\times) \cap \Gamma$ has a unique fixed point $\tau \in v_1(K) \cap \mathfrak{H}$.

Let γ_τ be a generator of that group. Choose $x \in \mathfrak{H}$ and put

$$J_\tau^\pm := \int^\tau \int_x^{\gamma_\tau x} \omega_f^\pm.$$

It is shown in [Darmon 04] that $J_\tau^\pm$ depends only on the orbit $\Gamma\tau$ and not on the choice of $x \in \mathfrak{H}$ in the definition. Let t denote the cardinality of the torsion of $E(K)$ and let

$$\eta^\pm : \mathbb{C}/\Lambda_E^\pm \to E(\mathbb{C})$$

be the Weierstrass uniformization attached to the lattice $\Lambda_E^\pm$. We choose nonzero integers $c^\pm$ such that $c^\pm \Lambda_f^\pm \subseteq \Lambda_E^\pm$ and set

$$P_\tau^\pm := t \cdot \eta^\pm(c^\pm \cdot J_\tau^\pm).$$

Let H be the ring class field of K, and $H^+ \supseteq H$ the narrow ring class field. The Galois group $\mathrm{Gal}(H^+/H)$ has cardinality at most 2, and we let σ be its generator. We recall Conjecture 2.3 from [Darmon 04].

Conjecture 4.2. [Darmon 04] *The point P_τ^+ (respectively P_τ^-) in $E(\mathbb{C})$ is a global point in $E(H)$ (respectively in $E(H^+)$), and we have*

$$\sigma \cdot P_\tau^+ = P_\tau^+ \quad \text{and} \quad \sigma \cdot P_\tau^- = -P_\tau^-.$$

It is very hard to compute the period lattices $\Lambda_f^\pm$ directly from their definition, since this requires a good understanding of the cohomology group $H^2(\Gamma, \mathbb{Z})$. Fortunately, by making use of Conjecture 4.2 we can circumvent that problem. Indeed, Conjecture 4.2 suggests that when $H^+ = H$, the point P_τ^- is trivial, meaning that cJ_τ^- is a period in Λ_f^- for some $c \in \mathbb{Q}$. Thus, in favorable circumstances, we can use the following proposition in order to compute the period lattice Λ_f^-.

Proposition 4.3. *Let K be a quadratic extension of F that is complex at v_1 and real at v_2. Let $\mathbf{\Psi} : K \to M_2(F)$ be an optimal embedding. Let u be a generator of the rank-one free group $\mathcal{O}_K^\times/(\mathcal{O}_F^\times)$ and let τ be the unique fixed point of $v_1(\mathbf{\Psi}(K^\times))$ in $\mathfrak{H}$. We assume that $H^+ = H$ and that*

$$\gamma_\tau := \mathbf{\Psi}(u) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is such that $a \in \mathcal{O}_F^\times$. Then

$$J_\tau^- = \int_{\frac{c}{a}-\frac{1}{\tau}}^{-\frac{1}{\tau}} \int_0^\infty \omega_f^- \text{or} J_\tau^- = \int_{\frac{c}{a}-\frac{1}{\tau}}^{\tau} \int_0^\infty \omega_f^-,$$

depending on whether $\varepsilon_N = 1$ or -1. Assuming Conjecture 4.2, the period J_τ^- belongs to $\alpha\Lambda_f^-$ for some $\alpha \in \mathbb{Q}^\times$.

Proof: Since $H^+ = H$, Conjecture 4.2 implies that P_τ^- is a torsion point in $E(H)$, which means that $J_\tau^- \in \alpha\Lambda_f^-$ for some $\alpha \in \mathbb{Q}^\times$. Now assume that $\varepsilon_N = -1$. Then the quantity J_τ^- is given by

$$\begin{aligned} J_\tau^- &= \int^\tau \int_\infty^{\gamma_\tau \infty} \omega_f^- = \int^\tau \int_\infty^0 \omega_f^- + \int^\tau \int_0^{\frac{a}{c}} \omega_f^- \\ &= \int^\tau \int_\infty^0 \omega_f^- - \int^{-\frac{1}{\tau}} \int_\infty^{-\frac{c}{a}} \omega_f^- \\ &= \int^\tau \int_\infty^0 \omega_f^- - \int^{\frac{c}{a}-\frac{1}{\tau}} \int_\infty^0 \omega_f^- = \int_{\frac{c}{a}-\frac{1}{\tau}}^{\tau} \int_\infty^0 \omega_f^-. \end{aligned}$$

A similar argument gives the second identity when $\varepsilon_N = 1$, and this completes the proof of the proposition. □

Remark 4.4. The aim of Conjecture 4.2 is to provide a way to construct infinite-order rational points on elliptic curves over real quadratic fields. Ironically, it is in its least interesting form that the conjecture has proven the most useful to us. Indeed, we use Conjecture 4.2 to compute lattice points in Λ_f^- that correspond to the trivial point on $E(H)$.

5. ALGORITHM AND EXAMPLES

Given a Hilbert eigenform f with integer Fourier coefficients, we need to find an elliptic curve E that shares the same L-series. When $F = \mathbb{Q}$, much information about the curve E can be obtained from the theory of modular symbols. (For example, we can determine the type of the period lattice of E and the sign of the functional equation.) In order to compensate for this lack of information, we will assume that we know the discriminant of E. In practice, this is not a very strong restriction, since the level of the modular form f and the discriminant Δ_E have the same set of prime divisors. Indeed, by incrementing the exponents of the prime divisors of $\mathrm{cond}(E)$ in a convenient way, we will eventually reach the discriminant Δ_E, and the algorithm will terminate.

Algorithm 5.1.

Step 1. Try several quadratic characters in order to determine the mixed periods $\Omega_E^s\Omega_{\bar{E}}^{s'}$, $s, s' \in \{-,+\}$, of the curve E and its Galois conjugate $\bar{E}$. We need to try characters χ whose conductors are as small as possible, since the size of the conductor of χ directly affects the speed of convergence of the series that determines $L(f,\chi,1)$. When $\mathfrak{n}$ is a square, we use Darmon's approach (see Section 4).

Step 2. Knowing the signs of $v_1(\Delta_E)$ and $v_2(\Delta_E)$, compute the types of the period lattices Λ_E and $\Lambda_{\bar{E}}$ and the pair $(\tau,\tau') \in \mathfrak{H}^2$ that determine E and $\bar{E}$.

Step 3. Compute the pair of j-invariants $(j(\tau), j(\tau'))$ and approximations to c_4 and its conjugate $\bar{c}_4$. With enough precision (see Remark 6.4), one should be able to recognize $c_4 - \bar{c}_4$ and $(c_4+\bar{c}_4)/\sqrt{D}$ as integers. If c_4 corresponds to an elliptic curve, the equation $c_4^3 - c_6^2 = 1728\Delta_E$ should have a solution $c_6 \in \mathcal{O}_F$.

Step 4. For each pair (c_4, c_6), find a minimal Weierstrass equation for E. As a check, one can verify that the traces of the Frobenius $a_{\mathfrak{p}}(E)$ agree with the Fourier coefficients of f up to a convenient bound.

Remark 5.2. In Step 1 of the algorithm, we sometimes use a trick of Cremona [Cremona 97, Section 2.11]. Namely, if χ_1 and χ_2 are two quadratic characters such that

$$\Omega_{f,\chi_i}^{ss'} = c_i\Omega_E^s\Omega_{\bar{E}}^{s'}, \quad c_i \in \mathbb{Z},$$

then we can determine the ratio $\frac{c_1}{c_2}$ if we compute it to enough precision. By trying several characters, we can determine the primes that divide, say, c_1, and then proceed as in [Cremona 97]. Alternatively, we can fix a range, and then try all the integers in that range as the possible multiples we are looking for. In practice, all the ranges we tried turned out to be very small.

We now give three examples, the first two of which are reconstructions from [Dembélé 05].

Example 5.3. Let $\mathfrak{n} = (5+2\omega)$ be one of the primes above 31 in $\mathbb{Q}(\sqrt{5})$, where $\omega = \frac{1+\sqrt{5}}{2}$. In [Dembélé 05], we found that there is a normalized eigenform with rational Fourier coefficients of weight 2 and level $\mathfrak{n}$. We want to find an elliptic curve E_f/F of conductor $\mathfrak{n}$. Let $\mathfrak{c}_1 = (3)$ be the unique prime above 3, and $\chi_1 : (\mathcal{O}_F/\mathfrak{c}_1)^\times \to \mathbb{C}^\times$ the unique quadratic character such that $\chi_1(\omega) = \chi_1(\bar{\omega}) = -1$. Next, we let $\mathfrak{c}_2 = (4-\omega)$ be one of the primes above 11, and $\chi_2 : (\mathcal{O}_F/\mathfrak{c}_2)^\times \to \mathbb{C}^\times$ the quadratic character given by $\chi_2(\bar{\omega}) = -1 = \chi_2(-1)$. Finally, let $\mathfrak{c}_3 = (4)$, and let $\chi_3 : (\mathcal{O}_F/\mathfrak{c}_3)^\times \to \mathbb{C}^\times$ be the unique quadratic character such that $\chi_3(\omega) = -1$ and $\chi_3(\bar{\omega}) = 1$.

By Conjecture 3.3, Ω_{f,χ_1}^{--} (respectively Ω_{f,χ_2}^{-+} and Ω_{f,χ_3}^{+-}) is an integral multiple of $\Omega_f^{-^-}$ (respectively $\Omega_f^{-^+}$ and $\Omega_f^{+^-}$). Using all the ideals $\mathfrak{a}$ of norm up to 300, we get

$$\begin{aligned}
\Omega_{f,\chi_1}^{--} &\approx 7.542829672311880211131042746 0,\\
\Omega_{f,\chi_2}^{-+} &\approx 20.241632560578134042430944 17i,\\
\Omega_{f,\chi_3}^{+-} &\approx 19.194856713798615637306615 53i.
\end{aligned}$$

Letting

$$\begin{aligned}
\Omega_f^{--} &= \Omega_{f,\chi_1}^{--},\\
\Omega_f^{-+} &= \Omega_{f,\chi_2}^{-+},\\
\Omega_f^{+-} &= \frac{\Omega_{f,\chi_3}^{+-}}{2} \approx 9.597428356899307818653307765 8i,
\end{aligned}$$

the Riemann–Hodge relations give

$$\Omega_f^{++} \approx 25.755270470967141659222210027 37.$$

For $\Delta_E = \omega^3(5+2\omega)$, we see that $v_1(\Delta_E) > 0$ and $v_2(\Delta_E) < 0$, which tell us the types of the period lattices of E and its Galois conjugate. Letting

$$\begin{aligned}
\tau &= 1.272390969151725829207221612644712687i,\\
\tau' &= 0.500000000000000000000000000\\
&\quad + 1.341779772310175064302580505990 13i,
\end{aligned}$$

we get the j-invariants

$$\begin{aligned}
j(\tau) &\approx 3777.985002370621477341703994762124999691 24,\\
j(\tau') &\approx -3883.407111798606702784264570911508861211 20.
\end{aligned}$$

From this, we obtain

$$\frac{c_4+\bar{c}_4}{2} \approx 33.006245461892707877380114669 3,$$
$$\frac{c_4-\bar{c}_4}{2\sqrt{5}} \approx 8.000786267244413771910591377 15,$$

which indicates that $c_4 = 25 + 8\omega$ (up to two-digit precision). We solve the discriminant relation for c_6. The only acceptable solution is $c_6 = -125 - 88\omega$.

By applying the Kraus–Laska algorithm to the curve with invariants c_4 and c_6, we obtain the minimal integral model

$$E_f : y^2 + xy + \omega y = x^3 - (1+\omega)x^2.$$

Its j-invariant is

$$j(E) = \frac{-54753 + 106208\omega}{31}.$$

Example 5.4. Let $\mathfrak{n} = (7)$ be the unique prime above 7 in $\mathbb{Q}(\sqrt{5})$. There is a unique normalized eigenform of weight 2 and level $\mathfrak{n}$ with rational Fourier coefficients. We want to find a modular elliptic curve E_f that corresponds to f. If such a curve exists, it should be isogenous to its Galois conjugate, since they would share the same eigenform. Using the characters of the previous example and the same set of ideals, we compute the periods

$$\Omega^{--}_{f,\chi_1} \approx 15.402502298890603186635516326 3049,$$
$$\Omega^{-+}_{f,\chi_2} \approx 20.064042467048509244375605730 4405i,$$
$$\Omega^{+-}_{f,\chi_3} \approx 20.059776894937158338082987854736 8i.$$

Although we do not have enough precision, the values of Ω^{-+}_{f,χ_2} and Ω^{+-}_{f,χ_3} suggest that E and $\bar{E}$ are isomorphic. Letting $\Delta_E = -7\bar{\omega}^6$ and

$$\Omega^{--}_f = \Omega^{--}_{f,\chi_1}, \quad \Omega^{-+}_f = \Omega^{-+}_{f,\chi_2}, \quad \Omega^{+-}_f = \Omega^{+-}_{f,\chi_3},$$

the Riemann–Hodge relations give

$$\Omega^{++}_f = -\frac{\Omega^{-+}_f \Omega^{+-}_f}{\Omega^{--}_f} \approx 26.130833009421273690206056313172786 64.$$

Then letting

$$\tau = 0.5000000000000000000000 + 0.651185648463821521543025019i,$$
$$\tau' = 0.5000000000000000000000 + 0.651324118565256213192808888i,$$

we get the approximate j-invariants

$$j(\tau) \approx 586.27333323579091250594341988173849743756738141,$$
$$j(\tau') \approx 585.16245084722668792737834819131243143882485,$$

and the approximate values

$$\frac{c_4+\bar{c}_4}{2} \approx -24.00220036102817748005777424316605240000,$$
$$\frac{c_4-\bar{c}_4}{2\sqrt{5}} \approx 7.99922506130012546104586105790357031762 50.$$

Then we determine that $c_4 = -32 + 16\omega$ and $c_6 = -280 + 160\omega$. The Kraus–Laska algorithm gives the minimal model $E : y^2 + y = x^3 + \omega x^2 + x$. It has j-invariant $j(E) = \frac{16^3}{7}$. This is the j-invariant of the curve E' listed as 175A1 in Cremona's tables. So, as suggested by the period lattices, the curve E is indeed a quadratic twist.

Example 5.5. Let $F = \mathbb{Q}(\sqrt{2})$, $\omega = \sqrt{2}$, $\varepsilon = 1 + \omega$, and $\mathfrak{n} = (5 + 2\omega)$. This is a prime above 17, the smallest norm for which there is a Hilbert modular form of weight 2 with rational Fourier coefficients and such that the corresponding curve is not a $\mathbb{Q}$-curve. Using a similar argument as in Example 5.3, we find the invariants $\Delta_E = \varepsilon^4(5 + 2\omega)$, $c_4 = 68 + 24\omega$, and $c_6 = 288 + 344\omega$. They correspond to the minimal model $E : y^2 + \omega xy + (1+\omega)y = x^3 + (1-\omega)x^2 - (1+2\omega)x - (1+\omega)$.

Remark 5.6. In principle, it is possible to use a shortcut to Steps 3 and 4. Indeed, we can instead find $j(E)$ from approximations to its real embeddings and use the algorithm in [Cremona and Lingham 08] in order to determine E from $j(E)$ and the prime divisors of $\mathrm{cond}(E)$. However, this approach requires a considerable number of Fourier coefficients and becomes quickly impracticable even in the case that $j(E)$ is an algebraic integer. For instance, in the simplest case of Example 5.3, this means using all the ideals of norm up to 10000 instead of up to 300 as we did.

6. APPLICATION: MODULAR ELLIPTIC CURVES WITH EVERYWHERE GOOD REDUCTION

In this section, we discuss several examples that illustrate how one can use our algorithm to compute modular elliptic curves with everywhere good reduction over real quadratic fields of narrow class number one, provided one can compute enough Fourier coefficients of the corresponding forms. Although all examples we discuss are

reconstructions, they clearly demonstrate that the algorithm works in principle. Each of them is interesting in its own way, since it explains how one can make the algorithm more efficient with some little variations depending on the situation at hand. To our knowledge, this is the first algorithm of its kind that proposes a systematic way of finding modular elliptic curves with everywhere good reduction over real quadratic fields in which one does not assume the curve to be a $\mathbb{Q}$-curve. We think that with reasonable computing capability, one should be able to implement it and create a database of such curves, and we hope to do so in the near future.

Example 6.1. Let $F = \mathbb{Q}(\sqrt{29})$, $\omega = \frac{1+\sqrt{29}}{2}$, and $\varepsilon = 2 + \omega$, and consider the elliptic curve $E : y^2 + xy + \varepsilon^2 x = x^3$. This is an elliptic curve with everywhere good reduction that was found by Tate and has been investigated in [Serre 72]. The curve E is isogenous to its Galois conjugate. We want to explain how this curve could have been computed from the corresponding modular form f.

Let $\mathfrak{c}_1 = (3 + \omega)$ be one of the primes above 5 and let $\mathfrak{c}_2 = (12 + 5\omega)$ be the unique prime above 29, and let χ_1 (respectively χ_2) be the unique quadratic character of conductor $\mathfrak{c}_1$ (respectively $\mathfrak{c}_2$) given by $\chi_1(\omega) = -1 = \chi_1(\bar{\omega})$, respectively $\chi_2(\varepsilon) = -1 = \chi_2(\bar{\varepsilon})$). Then by Conjecture 3.3, Ω^{++}_{f,χ_1} (respectively Ω^{--}_{f,χ_2}) is an integer multiple of $\Omega^{+}_{E}\Omega^{+}_{\bar{E}}$ (respectively $\Omega^{-}_{E}\Omega^{-}_{\bar{E}}$). Using all ideals of norm up to 3000, we compute

$$\Omega^{++}_{f,\chi_1} \approx 18.404772944969059323020956943708747040558325 0,$$
$$\Omega^{--}_{f,\chi_2} \approx 145.787495305335352280461347872169300862518970 4.$$

To compute the periods Ω^{-+}_{f} and Ω^{+-}_{f}, we will use Conjecture 4.2. Let us consider the quadratic extension $K = F(\beta) = F(\sqrt{-1+\omega})$. This is an extension that has been investigated in [Darmon 04]. It has narrow class number one and a relative discriminant of norm -7. The group of units is generated by

$$-1, \quad 2 + \omega, \quad \varepsilon_K := \frac{\beta^2 - \beta - 1}{2}.$$

Since the norm of ε_K is not a square, we replace it by its square

$$\varepsilon_K^2 = (-\beta^3 - \beta^2 + \beta + 4)/2.$$

In [Darmon 04], it is shown that the embedding $\mathbf{\Psi} : K \to M_2(F)$ that sends β to the matrix $\left(\begin{smallmatrix} \omega & -4 \\ 2 & -\omega \end{smallmatrix}\right)$ is an optimal embedding. The associated fixed point is

$$\tau \approx -1.096291201783626007812677622 88 + 0.893389948953878148512845864946 00i,$$

and we have

$$\gamma_\tau = \mathbf{\Psi}(\varepsilon_K^2) = \begin{pmatrix} -1 & -2\omega - 2 \\ 1 + \omega & 5 + \omega \end{pmatrix}.$$

From this, we get the period

$$J^-_\tau = \int_{\frac{c}{a} - \frac{1}{\tau}}^{-\frac{1}{\tau}} \int_0^\infty \omega_f^- \approx 3.860904680028850374927213764368053872893 2i.$$

By Conjecture 4.2, J^-_τ is a rational multiple of $\Omega^{-}_{E}\Omega^{+}_{\bar{E}}$ with denominator bounded by the torsion of $E(H)$. We now have a finite set of possibilities to try, and see which one gives us an elliptic curve E with everywhere good reduction. Letting

$$\Omega^{++}_f = \Omega^{++}_{f,\chi_1},$$
$$\Omega^{--}_f = \frac{\Omega^{--}_{f,\chi_2}}{4} \approx 11.582714040086551124781641293104161 61867972524,$$
$$\Omega^{-+}_f = 3J^-_\tau \approx 36.446873826333838070115336968042325215 6297426i,$$

the Riemann–Hodge relations give

$$\Omega^{+-}_f = \frac{\Omega^{++}_f \Omega^{--}_f}{\Omega^{-+}_f} \approx 57.913580099280209373380062589796100611331 93424i.$$

Letting

$$\tau = 0.500000000000000000000000 + 0.314666040019056129827812167971421i,$$
$$\tau' = 0.500000000000000000000000 + 1.573330469015942787905615202387094i,$$

we get

$$j(\tau) \approx 18.927148537157605478892686505143975711 + 5.753163429169375848462820272967378108478499 0E - 149i,$$
$$j(\tau') \approx -18909.960323280339329697876260358501691 2 + 3.408440282512242878319930553726397985245270 21E - 147i.$$

The approximate values

$$\frac{j(\tau)+j(\tau')}{2} \approx -9445.516587371590862109491786926678 85,$$
$$\frac{j(\tau)-j(\tau')}{2\sqrt{29}} \approx 1757.503080197255180934393434746729 18876,$$

suggest that the j-invariant is the algebraic integer $j(E) = -11203 + 3515\omega$. It is then easy to solve for the invariants c_4 and c_6 knowing that Δ_E is a unit. In fact, without loss of generality, we can assume that $\Delta_E \in \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^{12}$. Then, for $\Delta_E = -\varepsilon^{10}$, we get $c_4 = -263 - 120\omega$ and $c_6 = -63541 - 28980\omega$. From the Kraus–Laska algorithm, we get the minimal model $E : y^2 + xy + (1+\omega)y = x^3 + (5+2\omega)x + 72 + 33\omega$.

Example 6.2. Let $F = \mathbb{Q}(\sqrt{37})$, $\omega = \frac{1+\sqrt{37}}{2}$, and $\varepsilon = 5 + 2\omega$, and consider the elliptic curve $E : y^2 + y = x^3 + 2x^2 - (19+8\omega)x + (28+11\omega)$. This elliptic curve is a $\mathbb{Q}$-curve that has everywhere good reduction. Using the unique quadratic character $\chi_1 : (\mathcal{O}_F/(4))^\times \to \mathbb{C}^\times$ given by $\chi_1(\varepsilon) = -1 = \chi_1(\bar{\varepsilon})$ and all ideals of norm up to 5000, we get

$$\Omega^{--}_{f,\chi_1} \approx 40.896716499857408255229232168565264546863 3671446271.$$

From [Darmon 04], we know that

$$\int_0^{i\infty}\int_{i\varepsilon^{-1}}^{i\varepsilon} \omega_f^+ = -2\ell_F^2\Omega_f^{++} \approx -5.435612717661564008989987229775 2533601060720485821 0,$$

where $\ell_F = \frac{2}{5}$. To compute the period Ω_f^{-+}, we use the quadratic extension $K = F(\beta) = F(\sqrt{\omega-3})$ in [Darmon 04, Table 37.1]. This gives

$$J_\tau^- \approx 5.27137134740499202551815570143616819076263 467803850i.$$

For the choices

$$\Omega_f^{--} = \frac{\Omega^{--}_{f,\chi_1}}{4} \approx 10.22418835274925401000235971951991015757063,$$
$$\Omega_f^{-+} = \frac{5J_\tau^-}{2} \approx 13.17842836851248006379538925358782149017354i,$$

the Riemann–Hodge relations give

$$\Omega_f^{+-} \approx 13.17843227486942072481519660286609413879209 178530i.$$

The values of Ω_f^{-+} and Ω_f^{+-} suggest that the curve E and its Galois conjugate have the same j-invariant, and so $j(E) \in \mathbb{Z}$. Letting

$$\tau = \frac{\Omega_f^{-+}}{\Omega_f^{++}} \approx 0.77582736242809738798439577276944777299414217i,$$

we obtain

$$j(\tau) \approx 4096.00549431460286898419598571473654957 63358866118539269.$$

This suggests the rational integer $j(E) = 4096$, which is confirmed by computing the j-invariant to higher precision.

Now we can solve for c_4 and c_6 as in the previous example. For $\Delta_E = \varepsilon^6$, we get $c_4 = 384\omega + 976$ and $c_6 = -14112\omega - 35864$. From this, we get the minimal model $E : y^2 + y = x^3 - x^2 - (20+8\omega)x + 48 + 19\omega$.

Example 6.3. Let $F = \mathbb{Q}(\sqrt{509})$, $\omega = \frac{1+\sqrt{509}}{2}$, and $\varepsilon = 442 + 41\omega$, and consider the elliptic curve $E : y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + 71 + 34\omega$ constructed in [Pinch 82]. It is known to have everywhere good reduction and not to be isogenous to its Galois conjugate. This latter fact was proven by Socrates and Whitehouse [Socrates and Whitehouse 05], who also established Conjecture 1.1 in this case using a result of Faltings and Serre. We want to explain how the computations in their paper could have been used to produce the curve E. Using all the ideals of norm up to 50000, we compute

$$\int_0^{i\infty}\int_{i\varepsilon^{-1}}^{i\varepsilon} \omega_f^+ = -2\ell_F^2\Omega_f^{++} \approx -26.68782971866189788570328490568 81571758132970538273 0,$$

where $\ell_F = 1$.

For the computations of the periods Ω_f^{-+} and Ω_f^{+-}, we use the following optimal embedding. Let $K = F(\beta) = F(\sqrt{10-\omega})$. This is a quadratic extension of F with one complex place above v_1 and one real place above v_2. The

relative discriminant of K/F has norm -37, and an integral basis is given by $1, \beta, \beta^2, \beta^3$. The group of units is generated by $-1, \varepsilon, \varepsilon_K := \beta^3 - 21\beta + 1$. We obtain an optimal embedding by sending β to $\left(\begin{smallmatrix} -13\omega-137 & 166\omega+1806 \\ -\omega-11 & 13\omega+139 \end{smallmatrix}\right)$. We replace ε_K by its square, which gets sent to

$$\gamma_\tau := \mathbf{\Psi}(\varepsilon_K^2) = \begin{pmatrix} -67\omega - 716 & 332\omega + 3612 \\ -2\omega - 22 & -15\omega - 164 \end{pmatrix}.$$

The class number and narrow class number are equal, $h = h^+ = 10$, so by Conjecture 4.2, the periods J_τ^- up to rational multiples belong to Λ_f^-. Although the quadratic field F is not Euclidean, we were able to obtain the continued fraction

$$\gamma_\tau \infty = \frac{-67\omega - 716}{-2\omega - 22} = \frac{83 + 21\omega}{10} = [3\omega + 18, -18\omega + 212].$$

Using both the forms f_E and $f_{\bar{E}}$ that correspond to E and $\bar{E}$ respectively, we get

$$J^-_{E,\tau} \approx 61.700791384457270615297034803287313751157 68i,$$
$$J^-_{\bar{E},\tau} \approx 36.984361723493116902742772231796022395597 28i.$$

Letting

$$\Omega_f^{-+} = \frac{J^-_{E,\tau}}{10}, \quad \Omega_f^{+-} = J^-_{\bar{E},\tau},$$

we see that the curve E is given by one of the pairs $(\tau, \tau') \in \mathfrak{H}^2$, where

$$\tau \approx 0.46238897680999509129648i$$

or

$$\tau \approx 0.50000000000000000000 + 0.23119448840499754564824082213i;$$

and

$$\tau' \approx 2.77162752560813905168849256982296i$$

or

$$\tau' \approx 0.50000000000000000000 + 1.38581376280406952584424628i.$$

For

$$\tau = 0.46238897680999509129648i,$$
$$\tau' = 0.50000000000000000000 + 1.38581376280406952584424628i,$$

we get the j-invariants

$$j(\tau) \approx 797678.49665270609349821944419777263800674024 53$$
$$j(\tau') \approx -5335.01783180456397417573233141642224525341 3742.$$

By letting $\Delta_E = \varepsilon$, we get

$$\frac{c_4 + \bar{c}_4}{2} \approx 452.71105064565376692061875246 8514,$$
$$\frac{c_4 - \bar{c}_4}{2\sqrt{509}} \approx 19.986575782709166983812201386442 97.$$

We then try all the closest integers or half-integers to these two values that give an algebraic integer. For $c_4 = 433 + 40\omega$, we get $c_6 = -12977 - 1204\omega$. We recover the minimal model $E : y^2 + xy + y = x^3 - (1+\omega)x^2 + 33x + 37$ using Kraus–Laska's algorithm.

Remark 6.4. There is a precision analysis in [Darmon and Logan 03] that should carry over to our algorithm, although we haven't done so carefully. However, we would like to point out that the quantities we seek to identify are elements of $\mathcal{O}_F$ whose coordinates are rational integers or half-integers, and thus are much easier to recognize than those in [Darmon and Logan 03]. Therefore, our computations require less precision than theirs.

But in either case, the precision of the computations is hugely influenced by the size of the fundamental unit in $\mathcal{O}_F$. This explains the fact that despite using all the ideals of norm up to 50000 in Example 6.3, we were able to obtain only one-digit precision. In contrast, the previous examples required relatively fewer ideals.

Remark 6.5. The recent algorithm developed by Cremona and Lingham [Cremona and Lingham 08] can be used to find all the elliptic curves with everywhere good reduction over F. However, the merit of our approach is that by using a precise formulation of the conjectural Eichler–Shimura construction over F, we can recover those curves that are modular from their corresponding eigenforms.

ACKNOWLEDGMENTS

I first lectured on the results in this paper at the MSRI Graduate Summer Workshop "Computing with Modular Forms" in 2006. I would like to thank all the participants, especially William Stein, for helpful suggestions. I would like to thank Henri Darmon and Adam Logan for email exchanges that helped me better understand their construction of Stark–Heegner points together with the implementation of their algorithm. I would also like to thank Clifton Cunningham and

Hugh Williams for their constant support and encouragement. Finally, I would like to thank the Pacific Institute of Mathematical Sciences for their postdoctoral fellowship support.

REFERENCES

[Bertolini et al. 04] M. Bertolini, H. Darmon, and P. Green. "Periods and Points Attached to Quadratic Algebras." In *Proceedings of the MSRI Workshop on Special Values of Rankin L-Series*, edited by H. Darmon and S. Zhang, pp. 323–367. Cambridge, UK: Cambridge University Press, 2004.

[Cremona 92] J. E. Cremona. "Modular Symbols for $\Gamma_1(N)$ and Elliptic Curves with Everywhere Good Reduction." *Math. Proc. Cambridge Philos. Soc.* 111:2 (1992), 199–218.

[Cremona 97] J. E. Cremona. *Algorithms for Modular Elliptic Curves*, second edition. Cambridge: Cambridge University Press, 1997.

[Cremona and Lingham 08] J. E. Cremona and M. Lingham. "Finding All Elliptic Curves with Good Reduction outside a Given Set of Primes." To appear in *Experiment. Math.*, 2008.

[Darmon 04] H. Darmon. *Rational Points on Modular Elliptic Curves,* CBMS Regional Conference Series in Mathematics, 101. Providence: American Mathematical Society, 2004.

[Darmon and Logan 03] Henri Darmon and Adam Logan. "Periods of Hilbert Modular Forms and Rational Points on Elliptic Curves. *International Mathematics Research Notices* 2003:40 (2003) 2153–2180.

[Dembélé 05] Lassina Dembélé. "Explicit Computations of Hilbert Modular Forms on $\mathbb{Q}(\sqrt{5})$. *Experiment. Math.* 14:4 (2005), 457–466.

[Dimitrov 04] Mladen Dimitrov. "Compactifications arithmétiques des variétés de Hilbert et formes modulaires de Hilbert pour $\Gamma_1(\mathfrak{c}, \mathfrak{n})$." In *Geometric Aspects of Dwork Theory*, vols. I, II, pp. 527–554. Berlin: Walter de Gruyter, 2004.

[Oda 82] Takayuki Oda. *Periods of Hilbert Modular Surfaces*, Progress in Mathematics, 19. Bostin: Birkhäuser, 1982.

[Oda 83] Takayuki Oda. "Hodge Structures of Shimura Varieties Attached to the Unit Groups of Quaternion Algebras." In *Galois Groups and Their Representations (Nagoya, 1981)*, pp. 15–36, Adv. Stud. Pure Math., 2. Amsterdam: North-Holland, 1983.

[Pinch 82] R. G. E. Pinch. "Elliptic Curves over Number Fields." D.Phil. thesis, Oxford University, 1982.

[Serre 72] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Invent. Math.* 15:4 (1972), 259–331.

[Silverman 86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106. New York: Springer-Verlag, 1986.

[Socrates and Whitehouse 05] Jude Socrates and David Whitehouse. "Unramified Hilbert Modular Forms, with Examples Relating to Elliptic Curves." *Pacific J. Math.* 219:2 (2005), 333–364.

[Zhang 01] Shouwu Zhang. "Heights of Heegner Points on Shimura Curves. *Ann. of Math. (2)* 153:1 (2001), 27–147.

Lassina Dembélé, Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Ellernstrasse 29, 45326 Essen, Germany (lassina.dembele@gmail.com)

Received September 5, 2007; accepted December 29, 2007.